# Guidance on a safer life online for women and girls

Statement

**Statement**

Published 25 November 2025

For more information on this publication, please visit ofcom.org.uk

# Contents

## Section



## Annex

# 1. Overview

1.1 Ofcom is the UK's communications regulator, overseeing sectors including telecommunications, post, broadcast TV, radio, and online services. We were appointed the online safety regulator under the Online Safety Act 2023 (the 'Act') in October 2023.

1.2 The Act makes providers of regulated user-to-user and search services ('services') – including social media, search, and pornography services – legally responsible for keeping users safe online.[1] This includes clear requirements on services to address illegal harms such as intimate image abuse, and to protect children from harmful content, including pornographic and abusive content. To help companies meet their duties, we have published Codes of Practice ('Codes') and guidance on illegal content and protection of children. We are already enforcing these duties and have opened enforcement programmes, including investigations related to child sexual abuse material (CSAM) and children's exposure to pornographic content. For further information on our enforcement of the Act, see here.

1.3 In addition to these duties, the Act also states that Ofcom must produce dedicated guidance on how providers can address content and activity that disproportionately affects women and girls. This includes a wide range of harms that threaten, silence, abuse, coerce monitor, and otherwise target women and girls online, curtailing their safety and ability to express themselves freely. This statement follows our consultation published in February 2025 ("February 2025 Consultation") and sets out our decisions in the final Guidance on a Safer Life Online for Women and Girls ("the Guidance"). Our decisions today are the next steps in implementing the Act and creating a safer life online for women and girls.

1.4 In this Guidance, we draw on a safety-by-design approach to set out practical and ambitious steps providers can take to prevent and respond to harms across the entire design and operation of a service. We highlight relevant parts of the Codes, but we also include examples of good practice steps firms should take to improve the safety of women and girls. From embedding safety into their services at the outset to improving current systems, our good practice steps include:

a) 'Abusability' testing to identify potential misuse of services
b) Working with experts on gender-based harms when designing policies and features
c) Greater transparency, including on harms, user reports and outcomes
d) Prompts that ask users to reconsider before posting misogynistic abuse
e) Technology to detect and remove non-consensual intimate images
f) Stronger account security to protect user privacy
g) Allowing users to track and manage reports and tailor their reporting experience

1.5 We will work with service providers to encourage the use of this Guidance, and we plan to publish a follow-up report in 2027. This will include reviewing the uptake of the steps set out in the Guidance, and gathering feedback from women and girls in the UK about how their experiences have – or have not – changed. This report will shine a light on which services are prioritising women and girls' safety, helping users to make informed choices about how they use online services.

[1] Throughout this document, we refer to the online platforms themselves as 'services', and the legal entity that provides the service as a 'service provider' or 'provider'.

## What we have decided – in brief

- We are confirming the overall approach of highlighting existing Codes and guidance ('foundational steps') alongside ways providers can go further ('good practice steps') to improve the safety of women and girls. We have not changed which steps are foundational and which are good practice and we note that certain good practice steps might be included in future versions of the Codes.
- We have clarified our approach to the aims of the Guidance, including who the Guidance is intended to support. We have made changes throughout the Guidance to make it more explicit that while the focus – as required by the Act – is on content and activity that disproportionately affects women and girls, we expect that the foundational steps and good practice steps will improve safety outcomes for users more broadly.
- We are confirming the overall approach to encouraging providers to take up the good practice steps set out in the Guidance by publishing a follow-up report in 2027. We are considering stakeholder feedback on what this report should contain. We will continue to enforce duties in the Act which are linked to the foundational steps[2] through our wider supervision and enforcement programme.
- We have amended and clarified the scope of content and activity captured by the Guidance in light of stakeholder feedback. This includes clarified definitions and new evidence on the harm areas, how they manifest, and feedback from stakeholders on human rights, including freedom of expression:

> **Misogynistic abuse and sexual violence** *(replacing 'online misogyny').* This includes some forms of illegal content and some forms of abusive, hateful, pornographic and violent content that does not meet the threshold for illegality.

> **Pile-ons and coordinated harassment** *(replacing 'pile-ons and online harassment')*. This includes some forms of illegal content and some forms of abusive, hateful and violent content that does not meet the threshold for illegality.

> **Stalking and coercive control** *(replacing 'online domestic abuse').* We have retained the focus on illegal content, but have expanded this area to include stalking offences, and drawn out the differences between stalking and coercive control.

> **Image-based sexual abuse**. As set out at consultation, we are confirming that this covers illegal content captured by intimate image abuse and cyberflashing. We also cover self-generated indecent images.

- We have also amended and clarified the evidence on how these harms manifest, including new evidence on perpetrators and emerging harms. We still use the term online gender-based harms to refer collectively to the four harm areas listed above.
- We are confirming the overall approach of setting out nine actions for service providers to take to improve the safety of women and girls, drawing on a safety-by-design approach. These actions are still grouped into three chapters (Taking Responsibility,

[2] Foundational steps draw upon measures set out in our Codes of Practice and guidance on Illegal Content and Protection of Children. Codes of Practice describe measures recommended for the purpose of compliance with duties and cover issues such as content moderation, reporting and complaints, and user controls. For more information on the relationship between Codes of Practice and duties, see paragraph 3.13 in this Statement.

Preventing Harm, Providing Support), but we have made some minor changes to clarify the language:


- We have amended and clarified a range of the good practice steps. We have also added 14 new good practice steps to the Guidance based on stakeholder feedback, including:

> Ensure adequate resourcing for policy and risk expertise on an ongoing basis

> Clearly explain default settings, bundles and account access options to all users

> Design recommender systems that promote content diversity and variety, which might include content featuring diverse perspectives

> Use rate limits to prevent mass-posting in pile-ons

> Signpost to relevant supportive materials, including how to report a crime, when reports are made about image-based sexual abuse and stalking and coercive control

- We have amended the structure of the case studies throughout the Guidance to improve readability and applicability, including by focusing on a wider range of user journeys and service types.

The overview section in this document is a simplified high-level summary only. The decisions we have taken and our reasoning are set out in the full document.

# 2. Background

2.1 As the online safety regulator, Ofcom has a duty to ensure the safety of all people in the UK, including women and girls. This includes ensuring providers are addressing harms that disproportionately affect women and girls including intimate image abuse and coercive control. In addition, we have a duty to prepare guidance setting out practical ways services can be made safer and supporting women and girls to make informed decisions about the services they use.

2.2 On 2 July 2025, the Government's Statement of Strategic Priorities for online safety was designated after having been laid in draft before Parliament. This sets out the desired outcomes which Ofcom must have regard to when exercising its regulatory functions and outlines, as one of five priorities, the importance of 'safety-by-design' in tackling violence against women and girls ('VAWG'). Ofcom responded to this by way of letter dated 25 July 2025.[3] We have had regard to the Statement of Strategic Priorities when making our final decision concerning the Guidance.

2.3 We also understand that while we have an important role to play, securing women and girls' safety is a much wider societal challenge. We are aware of a significant number of global and domestic initiatives focusing on this issue. This includes governmental initiatives[4] and international partnerships.[5]

2.4 For example, the UK Government has announced a commitment to halve violence against women and girls in the next decade. Online experiences are a key aspect of this, and since the publication of the draft guidance we have already seen legislative changes to strengthen criminal laws related to online gender-based harms, including intimate image abuse. We will closely monitor the future strategy on VAWG as it develops and will respond to changes in the law that affect our powers under the Act to make women and girls safer online.

2.5 Technology is changing quickly, and with it, new types of harm are emerging, such as the misuse of generative artificial intelligence ('GenAI') for intimate image abuse. To address this, providers need to consider safety from the outset and continuously improve their systems. As digital tools evolve, there are significant risks, but there are also opportunities to go further to detect, reduce and respond to harms.

2.6 It is clear from talking to women and girls and experts in the field that there is more service providers can – and should – do to protect UK users. We intend to use the Guidance to drive forward change across industry and set a high standard of safety for online experiences of women and girls.

2.7 We expect to update the Guidance to reflect changes to Ofcom's implementation of the Act, such as any new Code measures we introduce or changes we make to existing ones, as well as to reflect emerging online gender-based harms and technologies. If changes are made to relevant legislation we may also update our Codes and guidance. We note the

[3] Ofcom, 25 July 2025, Letter to Government on the Statement of Strategic Priorities for Online Safety letter to Government.
[4] See for example, plans set out by the Northern Ireland, Welsh and Scottish Governments.
[5] See for example, the Global Partnership for Action on Gender-Based Online Harassment and Ofcom, which Ofcom is a member of.

recent announcements on making cyberflashing a priority offence and the introduction of a proposed new priority offence on depictions of strangulation and suffocation in pornography.

## Legal framework

2.8 Under section 54 of the Act, Ofcom is required to produce guidance for user-to-user and search service providers[6] which focuses on 'content and activity' that 'disproportionately affects women and girls'.

2.9 The Act sets out that the Guidance is to focus on content and activity in relation to which service providers have duties under Part 3 and Part 4 of the Act.[7] It goes on to set out two examples of things that the Guidance may, among other things, include. Those are: (a) that it may contain advice and examples of best practice for assessing risks of harm to women and girls from such content and activity, and reducing such risks; and (b) that it may refer to provisions contained in Ofcom's Codes that relate to the duties on Part 3 service providers and which are particularly relevant to the protection of women and girls from this type of content and activity.[8] Ofcom is therefore given a degree of flexibility as to how it frames the Guidance.

2.10 In **Annex A2**, we set out further details on the relevant legal context and explain our general duties and the matters we are required to have regard to in carrying out our functions, including media literacy duties. In **Annex A3**, we set out Ofcom's duty to carry out our functions compatibly with the Human Rights Act 1998 ('the HRA 1998'), including the right to freedom of expression and the right to respect for private and family life ('privacy'). We also explain our duties to carry out an impact assessment and equality and Welsh language impact assessments.

## Consultation and stakeholder engagement

2.11 We are committed to an ongoing and accessible dialogue and have conducted extensive stakeholder engagement throughout the development of this Guidance to support our interpretation of the available evidence and expand our evidence base further. We are grateful for the time and expertise of those who have shared their views throughout this process.

2.12 Prior to the publication of our draft guidance, we held two multistakeholder workshops with representatives from civil society, academia and industry. Over 40 organisations participated. This provided an opportunity to bring together a breadth of relevant specialists across the UK and beyond to ensure that we could consider these perspectives early in the process of developing the draft guidance.

[6] Section 54 of the Act requires Ofcom to produce guidance for providers of 'Part 3 services'. Section 4(3) of the Act sets out that a Part 3 service is a regulated user-to-user service or a regulated search service.
[7] Part 3 of the Act sets out 'duties of care' for providers of regulated user-to-user and search services, including duties relating to tackling illegal content and content that is harmful to children. Part 4 of the Act sets out other duties on providers of regulated user-to-user and search services, many of which apply only to a subset of these services known as 'Category 1 services'. These are services which meet particular threshold conditions set out in secondary legislation.
[8] The relevant Codes of Practice for this purpose are those under section 41 (see s.54(2)(b)) of the Act.

2.13 Following the publication of the draft guidance in February 2025, we received 111 consultation responses. Respondents included our statutory consultees,[9] over 40 responses from civil society organisations, 20 responses from industry and trade associations, and a number of responses from parliamentarians, governments, and other public bodies including law enforcement and academia. Most responses came from UK-based organisations, but we also received responses from international organisations.

2.14 In addition to the formal consultation process, we have also engaged with a wide range of stakeholders in different formats. We met with a group of survivors of domestic abuse to hear their views on our proposals, and hosted roundtables with men and boys' organisations and young people, as well as interactive workshops in Belfast, Cardiff and Edinburgh with over 80 stakeholders. We also hosted a webinar explaining the draft guidance which was attended by 60 stakeholders and attended a range of both domestic and international conferences to present our proposals. In international settings, we have also sought to gain feedback on regulatory coherence in line with our wider work with the Global Online Safety Regulator's Network.

2.15 We are committed to meaningful engagement and listening to those with lived experience of online gender-based harms and this is reflected in the Guidance. As we develop our work to drive take up of the Guidance, as well as our work under the Act more broadly, we will continue this valuable engagement.

## In this statement

2.16 The decisions explained in this statement set out our final decisions on the Guidance. To arrive at these final decisions, we have considered the consultation responses we received to the draft guidance and our stakeholder engagement. This statement covers:

a) **Section 3**: feedback and our decisions related to the overall aims of the Guidance, and how we intend to encourage providers to take action.
b) **Section 4**: feedback and our decisions related to the scope of harm in relation to 'content and activity that disproportionately affects women and girls'.
c) **Section 5**: feedback and our decisions in relation to the actions, good practice and case studies we have highlighted.
d) **Annex A1**: additional stakeholder feedback
e) **Annex A2**: the relevant legal framework, including Ofcom's wider duties
f) **Annex A3**: the impact assessments

2.17 We are confirming the broad structure of the Guidance, as set out in our February 2025 Consultation. We have made changes in a number of areas to amend, strengthen or clarify our positions, and to add additional evidence and good practice steps in light of the feedback we received.

2.18 Where stakeholders raised comments about Ofcom's approach to other online safety duties or wider concerns but did not make any specific comments about the proposed guidance itself, we have not responded directly or individually in all cases. For example, where these comments were outside the scope of the consultation.

[9] Before producing the Guidance, we are required to consult the Domestic Abuse Commissioner, the Commissioner for Victims and Witnesses and such other persons as we consider appropriate. We are also required to consult on revised or replacement guidance. See section 54(3) of the Act.

# 3. Aims of the Guidance

## Introduction

3.1 This section covers feedback and our decisions on overarching topics related to our duty under the Act and our aims for the Guidance:

a) **Topic 1:** Overall approach to scope and proportionality
b) **Topic 2:** Service in scope of the Guidance
c) **Topic 3:** Who the Guidance is intended to support
d) **Topic 4:** Encouraging take up among service providers, including the legal status of the Guidance and our proposed follow-up report.

## Overall approach to scope and proportionality

### What we proposed

3.2 In the draft guidance, we proposed providers take action to address four areas of online harm: online misogyny, pile-ons and online harassment, online domestic abuse and image-based sexual abuse. We used the term online gender-based harms to refer to these collectively.[10]

3.3 We highlighted a range of ways providers could intervene to tackle these harms. This includes both foundational steps (drawn from Ofcom's existing Illegal Content and Protection of Children Codes and statutory guidance on Risk Assessments and Transparency Reporting) as well as good practice steps (further mitigations for the four harm areas).

3.4 At consultation, we noted that two harm areas we proposed – online domestic abuse and image-based sexual abuse – only capture illegal content and activity. The other two harm areas – online misogyny and pile-ons and online harassment – could include both illegal content and content that does not meet the threshold for illegality but is harmful to children. This reflects the Act which sets out that the Guidance must cover content and activity where providers have specific duties under the Act – spanning both illegal content and content harmful to children.[11] We also explained that our evidence shows some harmful content and activity can negatively impact adults.

3.5 At consultation, we highlighted good practice steps that addressed harms areas spanning illegal content and content harmful to children (online misogyny and pile-ons and online harassment) in ways that support all users – adults as well as children. This was due to the dedicated and voluntary nature of the Guidance, and the evidence base on the risks and impacts of the harm.

[10] For detailed stakeholder feedback and our final decision in relation to this framing and terminology, see Section 4 in this statement.
[11] Section 54 says that the Guidance must cover content that disproportionately affects women and girls where providers have duties under Parts 3 and 4 of the Act – so this covers both illegal content and legal content harmful to children.

## Summary of stakeholder feedback

3.6 We received general feedback in support of the aims and scope of the Guidance, including how we highlighted good practice alongside existing expectations for providers.[12] For example, one industry stakeholder said they endorse Ofcom's recommendation encouraging providers to adopt relevant good practice steps in addition to fulfilling their statutory obligations.[13] Internet Matters said "we believe that Ofcom's approach to outlining the foundational steps and the good practice steps side-by-side is a helpful and clear way of conveying information to service providers on what they are required by law to do and what Ofcom, informed by a wide range of stakeholders and research, are recommending for further action."[14] Other stakeholders called for us to be more ambitious and go further with our good practice, as is discussed in detail in **Section 5** of this statement.

3.7 There was also support that many of our good practice steps contain sufficient safeguards against infringing on freedom of expression.[15] However, the Free Speech Union argued the decision to 'go beyond' the core requirements of the Act – e.g. including good practice – risked infringing upon freedom of expression where such proposals extended to legal speech. They argued that this "risks undermining core legal protections, such as the duty on providers to have particular regard for free speech." [16] Other organisations and individuals also raised concerns that the actions would require providers to monitor or police legal content, cutting into freedom of expression.[17] For example, one stakeholder said in response to the issue of good practice, "fairness will be near impossible, and the rights to freedom of expression will be lost."[18]

3.8 Although the majority of stakeholders supported our approach, some raised concerns about the potential administrative or regulatory burden for providers of taking up good practice alongside existing duties under the Act. This feedback is summarised in paragraphs 3.59 and our impact assessment (**Annex A3**) in this statement.

3.9 We also received feedback indicating that the harm areas required clearer descriptions of what content and activity is captured to clarify our expectations or mitigate risks of over moderation, takedown, enforcement or other impacts to users.[19]

3.10 However, other stakeholders argued that good practice steps targeting abusive and violent content that does not meet the threshold of illegality – including affording that good

---

[12] Response(s) to our February 2025 consultation: Age Check Certification Scheme, p.2; Barker, K.p.3; Jess Phillips, MP Minister for Safeguarding and Violence against Women & Girls, p.1; Online Dating and Discovery Association (ODDA), p.2; 5Rights Foundation, p.5; Women's Aid Federation of England, p.7; The four Welsh Office of Police and Crime Commissioners, p.1; Marie Collins Foundation, p.2-3; The Children's Commissioner for England's Office, p.5.

[13] Response(s) to our February 2025 consultation: Bumble, p.7

[14] Response(s) to our February 2025 consultation: Internet Matters, p.11.

[15] Response(s) to our February 2025 consultation: British and Irish Law, Education and Technology Association (BILETA) p.19; Barker, K.p.9.

[16] Response(s) to our February 2025 consultation: Free Speech Union, p.1-2.

[17] Response(s) to our February 2025 consultation: Name Withheld 2, p.2; Name Withheld 1, p.2; Parity, p.2

[18] Response(s) to our February 2025 consultation: Name Withheld 1, p.2.

[19] Response(s) to our February 2025 consultation: British and Irish Law, Education and Technology Association (BILETA), p.8; Barker, K, p.1; Free Speech Union, p.1; Parity, p.2; Evans, M.I., p.5; Office of the Derbyshire Police and Crime Commissioner, p.4; Centre for Protecting Women Online, p.5-6; Integrity Institute, Council on Technology & Social Cohesion, University of Southern California, Marshall School Neely Center, p.2-3; Welsh Government, p.1; [✂]; [✂];[✂];[✂].

practice to adults – helps prevent harm and protect the safety women and girls online.[20] For example, the Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales argued that "it is crucial that the guidance recognises how behaviours that are not explicitly illegal contribute to both a conducive context for illegal harms and the broader normalisation of violence against women and girls."[21] Similarly, the Commissioner Designate for Victims of Crime for Northern Ireland said, "if the sharp end of the wedge – criminal violence and abuse – is to be prevented, the behaviours and attitudes that lead to such behaviours must also be challenged as part of a comprehensive, collaborative and holistic approach."[22]

3.11 We also received feedback that the inclusion of content that does not meet the threshold of illegality is critical to protecting the rights of women and girls online, including their freedom of expression. For example, the Institute for Strategic Dialogue (ISD) argued such harms have "human rights implications of silencing and discrimination — particularly for women in public life. These harms can have chilling effects on political representation, freedom of expression, access to public life, the right to non-discrimination and participation in public affairs."[23] Similarly, Girlguiding's response cited their Girls Attitudes Survey of 14-21 year olds which found that "more than a third (36%) of girls and young women are put off certain jobs, like politics, because of the abuse high profile women get online."[24]

3.12 More generally, we received feedback that the Guidance should explicitly recognise the need to balance different rights or consider human rights principles. One stakeholder suggested we summarise the Rights Assessment in the Guidance itself.[25] Other stakeholders argued the Guidance should be more ambitious to protect the rights of women and girls, including freedom from torture / inhuman and degrading treatment and right to a private life of victims. [26] For example, the Online Safety Act Network said that "while freedom of expression should never be cavalierly dismissed, there is space here for Ofcom to be more courageous in its protection of the Article 8 rights of women and girls."[27] Similarly, stakeholders argued the draft guidance should elaborate on how it balances human rights implications — including Article 10 rights.[28] Stakeholders recommended considering models from the United Nations Human Rights principles, United Nations Convention on the Rights of the Child, and other intergovernmental principles.[29] We discuss the feedback and our decision in relation to rights further in our rights assessment (**Annex A3**) in this statement.

---

[20] Response(s) to our February 2025 consultation: The Cyber Helpline, p.1; End Violence Against Women Coalition (EVAW) Annex 2, p.5.
[21] Response(s) to our February 2025 consultation: Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.5.
[22] Response(s) to our February 2025 consultation: Commissioner Designate for Victims of Crime for Northern Ireland, p.3.
[23] Response(s) to our February 2025 consultation: Institute for Strategic Dialogue (ISD), p.3.
[24] Response(s) to our February 2025 consultation: Girlguiding, p.3.
[25] Response(s) to our February 2025 consultation: The Cyber Helpline, p.10.
[26] Response(s) to our February 2025 consultation: Online Safety Act Network, p.3; Commissioner for Children and Young People (NICCY), p.6-7.
[27] Response(s) to our February 2025 consultation: Online Safety Act Network (Annex), p.12.
[28] Response(s) to our February 2025 consultation: The Cyber Helpline, p.1; The Free Speech Union, p.4; Institute for Strategic Dialogue (ISD), p.2, End Violence Against Women Coalition (EVAW) Annex 2, p.5; [✂].
[29] Response(s) to our February 2025 consultation: Barker, K., p.6-7; Online Safety Act Network (Annex), p.10.

## Our final decision

3.13 We are confirming our position at consultation to include both steps linked to enforceable duties covered by the Codes of Practice and guidance we have already published (we call these 'foundational') on Illegal Harms, Protection of Children and Transparency, as well as further steps they could take (we call these 'good practice'). These are explained in **Table 1**.

| | Foundational steps | Good practice steps |
|---|---|---|
| **Summary** | Includes final Codes measures[30] and information from our risk assessment guidance[31] relevant to each action.<br>We also briefly refer to the Transparency Reporting duties under the Act. [32] | Includes additional steps that providers can take to do more to improve women and girls' online safety and experiences in line with the objectives of the action, beyond the foundational steps. |
| **Evidence base** | We have conducted rigorous evaluations, given they have been set out in final form as part of the wider regime. | These are generally less commonly used or our evidence base on efficacy is less established. |
| **Link to duties** | Included in the package of measures and guidance we have already set out to help providers comply with the corresponding duties in the Act as set out in the Legal Annex (**Annex A2**) in this statement. | We consider that taking these steps may assist providers to demonstrate their approach to user safety more broadly.[33] It is possible that certain good practice steps may ultimately become codes measures.[34] |

[30] Our Illegal Content Codes of Practice and Protection of Children Codes of Practice describe measures recommended for the purpose of compliance with illegal content and children's safety duties. These Codes cover safety measures on issues such as content moderation, reporting and complaints, and user controls. If service providers implement measures recommended in Codes, services will be treated as complying with the relevant duties. This means that Ofcom will not take enforcement action against them for breach of that duty if those measures have been implemented. However, the Act does not require that service providers must adopt the measures set out in the Codes, and service providers may choose to comply with their duties in an alternative way that is proportionate to their circumstances. Where providers do take alternative measures, they must keep a record of what they have done and explain how they think the relevant safety duties have been met.

[31] Our Illegal Harms and Children's Risk Assessment Guidance is intended to assist services in complying with their legal obligations. It does not represent a set of compulsory steps that services must take. We consider that following our risk assessment guidance will put services in a stronger position to comply with their duties.

[32] See section 77 of the Act. Duties around transparency reporting only apply to categorised services. Ofcom's Transparency Guidance is largely procedural in nature and primarily focuses on how Ofcom will request information for transparency reports. As explained in the Legal Annex (**Annex A2**) of this document, categorised service providers will be required to publish transparency reports based on requirements laid out in transparency notices issued by Ofcom. Ofcom must issue notices for categorised services once a year.

[33] While the good practice steps are not substitutes for the foundational steps, if service providers choose to implement these steps, this could assist providers to demonstrate compliance with the duties.

[34] We hope that, as more service providers implement good practice steps, it will improve our evidence base which may enable us to include some of these good practice recommendations in future iterations of Codes of Practice. Some of the good practice steps we recommend we may not be able to recommend as Codes. Sometimes this may be because there are legal restrictions which would prevent us from doing so - for example, we include good practice related to proactive technology (as defined in section 231 of the Act) but we would have to assess these measures against additional criteria in order to recommend these in Codes. We have not done so for the purposes of making these good practice recommendations in the Guidance. In addition, we can also only recommend proactive technology in our Codes on content communicated publicly – not on any content communicated privately. See our Guidance on content communicated 'publicly' and 'privately' for further details on how we understand these concepts under the Act. There may also be further restrictions under Schedule 4 to the Act which mean we cannot implement good practice as Codes measures.

| | Foundational steps | Good practice steps |
|---|---|---|
| **Further details** | Table 1 of our 'Guidance at a Glance' document provides a list of foundational steps with additional information on corresponding duties and which providers should implement the step.[35] | Table 2 of our 'Guidance at a Glance' document provides a list of the good practice steps set out in the draft guidance. |

**Table 1: Description of foundational steps and good practice steps in the Guidance**

3.14 Under the foundational steps, we have added reference to providers' duties about freedom of expression and privacy. When deciding on and implementing their safety measures and policies, user-to-user and search services will need to have particular regarding to the importance of protecting users' right to freedom of expression and protecting users from a breach of any statutory provision or rule of law concerning privacy (including, but not limited to, any such provision or rule concerning the processing of personal data).[36] Providers of Category 1 user-to-user services will need to carry out and publish an assessment of the impact that safety measures and policies would have on users' rights to freedom of expression and privacy and will also need to carry out and publish impact assessments of adopted safety measures and policies. They will have to keep impact assessments up to date and will also need to specify in publicly available statements the positive steps they have taken in response to impact assessments on these issues.[37]

3.15 With regards to the good practice steps, section 54 of the Act is permissive in terms of what we can include in the Guidance, and we retain our position from consultation that we intend for the Guidance to set out practical and ambitious recommendations that providers can take to improve women and girls' safety. We are clear that not all good practice steps will be relevant to all providers, and that ultimately it is up to service providers to determine what actions they take – or choose not to take – so long as they comply with their duties under the Act.

3.16 We are also confirming our approach at consultation to cover content that is illegal and content that is not illegal but is harmful to children as set out under the Act. However, we have made two changes to the Guidance in light of feedback provided by stakeholders.

3.17 First, we have tightened and clarified the scope of the harm areas for online misogyny and pile-ons and online harassment as these span illegal content and harms to children. For both online misogyny and pile-ons and online harassment, where content does not meet the threshold of illegality, we have explained these are only intended to capture content in relation to which providers have duties under the Act (i.e. in relation to the protection of

[35] We also indicate where the foundational step appears in other Ofcom documents, such as our Illegal Content Codes of Practice and our Protection of Children Codes of Practice. Where we refer in the 'Guidance at a Glance' document to measures being 'final', that means that these measures are included in Ofcom's Illegal Content Codes of Practice as issued on 24 February 2025 and in force since 17 March 2025 and in Ofcom's Protection of Children Codes of Practice as issued on 4 July 2025 and in force since 25 July 2025.

[36] Sections 22 and 33 of the Act.

[37] Section 22 of the Act. Category 1 service providers will have additional duties in relation to privacy and freedom of expression impact assessments of (1) contemplated and (2) adopted safety measures and policies designed to secure compliance with any of the duties set out in: (a) section 10 (illegal content), (b) section 12 (children's online safety), (c) section 15 (user empowerment), (d)section 20 (content reporting), or (e) section 21 (complaints procedures).

children[38] and, for Category 1 services, user empowerment for adults).[39] We have added references to our Illegal Content Judgements Guidance (ICJG) and, where relevant, the Guidance on Content Harmful to Children for each harm area to further clarify the scope of the content and activity captured. We have also changed the name of 'online misogyny' to 'misogynistic abuse and sexual violence' and the name of 'pile-ons and online harassment' to 'pile-ons and coordinated harassment' to reflect these amendments. Further details on changes we have made to both harm areas are detailed in paragraphs 4.43 and 4.89 in this statement.

3.18 Second, in response to stakeholder feedback, we have assessed which good practice steps should be applied to misogynistic abuse and sexual violence, and to pile-ons and coordinated harassment. We have made changes throughout **Chapters 3-5** to: (a) clarify if good practice applies to content that is not illegal, and (b) if so, explain how providers can apply this good practice in a way that mitigates impacts on freedom of expression and privacy rights through case studies and further clarification in the text. Where relevant, we also highlight where the Act sets additional duties for Category 1 providers to empower adult users to control their exposure to this type of content.[40] As explained in paragraph 3.14, providers also have specific duties under the Act about freedom of expression and privacy. Full details on the changes we have made are detailed in paragraphs 4.52-4.54 and 4.95 in this statement.

3.19 All good practice steps are voluntary, and it is ultimately up to service providers to decide what good practice steps they take, including what kinds of content they allow. The foundational steps reflect the relevant measures in our Codes and are connected to enforceable duties on providers. These steps have already been through rigorous assessment when we consulted on the Codes, including assessment of potential human rights impacts.

3.20 In making these final recommendations, we have had careful regard to the HRA 1998 and the rights protected under the European Convention on Human Rights ('ECHR'). In particular, as regards both users and providers, the right to freedom of expression, as set out in Article 10 ECHR and, with respect to users, the right to respect for private and family life in Article 8 ECHR, as well as other rights (see the rights assessment in **Annex A3** of this statement for more information). We consider that, given the evidence of harm to both adults and children in relation to the harm areas we have focused on in the Guidance, adults as well as children should have the opportunity to benefit from good practice in the Guidance relating to these harms, as they are also likely to be impacted by them.

---

[38] Primary priority content is defined in section 61 of the Act. In summary it comprises pornographic content and content which encourages, promotes or provides instructions for: (a) suicide; (b) an act of deliberate self-injury; and (c) an eating disorder or behaviours associated with an eating disorder. Priority content is defined at section 62 of the Act. In summary it comprises abusive content and content which incites hatred based on specified characteristics; violent content; bullying content; and content relating to dangerous stunts or challenges or physically harmful substances. It also includes 'non designated content' as defined in section 60(2)(c) of the Act which is content of a kind which presents a material risk of significant harm to an appreciable number of children in the UK (subject to certain exclusions). As is discussed in detail in **Section 4**, this Guidance mainly focuses on priority content falling under abuse, hate and violence.

[39] Section 15 of the Act.

[40] Section 14 of the Act. Providers will need to comply with these duties when we publish our register of categorised services and finalise Codes of Practice connected to these duties. For further information, see Ofcom's approach to implementing the Online Safety Act.

3.21 We recognise that our decision to cover content and activity which is not criminal in nature within the harm areas of misogynistic abuse, sexual violence and pile-ons and within our good practice recommendations has the potential to interfere with freedom of expression and privacy rights of other users where service providers choose to adopt these measures, as we go on to discuss. As expressly noted in the Guidance, the right to freedom of expression is not absolute and expression that promotes or justifies violence, hatred, is not normally protected under Article 10 (under Article 17 ECHR).[41] However, Article 17 will not be applicable to all content and activity covered by these areas and we have therefore considered the proportionality of any good practice steps given the pressing social need they are intended to address, and carefully balanced the rights of women and girls or other users who may be subjected to harms with the rights of others, including service providers and other users of online services. We recognise that even shocking or offensive content which contributes to democratic debate is protected by Article 10,[42] as we have sought to make clear in the Guidance. In line with what we have said in the Illegal Content Judgements Guidance and Guidance on Content Harmful to Children, we would not normally expect content falling within scope of these harm areas to include the type of content that would attract a high degree of protection under Article 10.

3.22 We consider it to be proportionate and in line with the Act for the Guidance to retain information about the impacts of these harms areas which span both illegal content and content harmful to children. This is in line with evidence that this content and activity disproportionately affects women and girls and evidence about the impacts on their human rights. Therefore, we consider that the inclusion of "legal" forms of misogynistic abuse, sexual violence and pile-ons in this Guidance (as defined in **Section 4**) is warranted to protect women and girls (as well as other groups targeted by these harms) from abuse and violence, and to facilitate their ability to participate in public debate or private communication, consistent with their own rights to freedom of expression and privacy. For more information on our approach, see our rights assessment (**Annex A3**) in this statement.

# Services in scope of the Guidance

## What we proposed

3.23 At consultation, we explained the Guidance applies to a range of regulated user-to-user and search services, including social media, gaming, discussion forums, pornography,[43] dating services and online marketplaces. We also noted that we expected a broader range of online and technology companies may find the Guidance useful.

---

[41] Perinçek v. Switzerland [GC], 2015, § 230; Zemmour v. France, 2022, § 49; European Court of Human Rights, Key Theme – Article 10 Hate Speech.

[42] See for example Handyside v UK: "Freedom of expression constitutes one of the essential foundations of such a [democratic] society, one of the basic conditions for its progress and for the development of every man. …. it is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no "democratic society."

[43] The Guidance does not apply to providers that publish or display pornographic content themselves, with no user-to-user interactions or search content. Part 5 of the Act sets out the duties of providers of regulated services in relation to certain pornographic content. Section 79 provides the definitions of 'provider pornographic content' and 'regulated provider pornographic content'. Ofcom has produced separate guidance for these services.

3.24 We set out that the various good practice steps would be more or less relevant to a service depending on the type of service. We recognised the ways that online gender-based harms manifest on these services can vary and the kinds of interventions available to address those harms evolve rapidly. In light of this, we proposed that providers use their discretion and understanding on their service to determine which good practice steps are most impactful for their users to improve their safety.

3.25 We also noted that our focus – both in terms of developing the Guidance and our future engagement – will be on those services with the highest reach or highest risk for online gender-based harms. We said that this is because we think this will have the most positive impact, however the Guidance is relevant to all providers and our consultation acknowledged that small services can be highly risky.

3.26 We also recognised that online gender-based harms are not isolated to specific services. There is a range of other technologies that can help facilitate or amplify these harms, including Internet of Things devices like smart technologies, which can be exploited by perpetrators of domestic abuse,[44] as well as Bluetooth,[45] which is commonly used for cyberflashing.[46] Where relevant, we referenced how these technologies are being used to facilitate or amplify online harm. We said that we expect that some of the information we provide in the Guidance may assist providers of these technologies to improve safety.

## Summary of stakeholder feedback

3.27 We received feedback calling for clarity on who the Guidance applies to, or that it should focus on different types of services including smaller services, dating, pornographic, end-to-end encrypted services or emerging services like metaverse and GenAI.[47] Some stakeholders also called for the expanding scope of Guidance or to clarify its role regarding Internet of Things devices, app stores or "out of scope services" flagging concerns that the latter promote and/or enable access to nudification apps."[48]

3.28 We also received feedback that the Guidance should acknowledge that there is no one-size-fits-all method and that services should have flexibility based on size, features, risks and

[44] Slupska, J. and Tanczer, L., 2021. Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things in The Emerald International Handbook of Technology-Facilitated Violence and Abuse. [accessed 13 November 2025]; eSafety Commissioner, 2024. Technology, gendered violence and Safety by Design. [accessed 13 November 2025].

[45] Bluetooth allows for wireless 'pairing' between two proximate devices using a peer-to-peer network. Bluetooth 'pairing' can be used to share files between devices, and perpetrators can use this to share unsolicited explicit images with nearby devices and cyberflash the device's user.

[46] Law Commission, 2021. Modernising Communications Offences: A final report. [accessed 19 November 2025]

[47] Response(s) to our February 2025 consultation: Suzy Lamplugh Trust, p.2; Centre for Protecting Women Online, p.21; Commissioner Designate for Victims of Crime for Northern Ireland, p.5; Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p. 5; Lucy Faithfull Foundation, p.3; Johnstone, E., p.1; End Violence Against Women Coalition (EVAW), p.12; CARE (Christian Action Research and Education), p.6; Welsh Women's Aid, p. 3; The Cyber Helpline, p.4; Children First, p.7; Institute for Strategic Dialogue (ISD), p. 4; [✂]; End Violence Against Women Coalition (EVAW) Annex 2, p.6; End Violence Against Women Coalition (EVAW) Annex 1, p. 21, 23; [✂]; Ukie, p.2-4; [✂]. Ofcom / Men and Boys Roundtable, 29 May 2025.

[48] Response(s) to our February 2025 consultation: Institute for Strategic Dialogue (ISD), p.8; [✂]; Name Withheld 3, p.1-2; Welsh Women's Aid, p.2; End Violence Against Women Coalition (EVAW) Annex 1, p.20; Centre to End All Sexual Exploitation (CEASE), p.6-9.

users.[49] One stakeholder said there is a risk service providers "cherry-picking" steps set out in the Guidance and not focus on safety improvements in other areas. .[50] The Cyber Helpline suggested we include tiers for good practice steps (basic, intermediate, advanced) so that all companies can do something regardless of size.[51]

## Our final decision

3.29 We are confirming our approach at consultation on the service types the Guidance applies to. We have made some small changes to clarify our approach.

3.30 The Act is clear that the Guidance applies to providers of all user-to-user and search services regulated under the Act. Services using emerging technologies, including many GenAI services, which fall under the definition of user-to-user services and search services in the Act are in scope of the duties in the Act and this Guidance. We have therefore explained that these are the services in scope of the Guidance. We remain of the view that the Guidance could be useful for a wider range of technology companies. This is because perpetrators of stalking or coercive control, for example, may exploit online services regulated under the Act and other digital technologies or telecommunication channels at the same time.[52]

3.31 We have clarified in **Chapter 1** (paragraph 1.20) in the Guidance that while the nine actions are designed to be achievable for all providers, we do not expect all services in scope to need to – or would be able to – take all of the steps under each action. We are retaining this position as this balances the need for the Guidance to apply to a range of service types while also ensuring we provide sufficient detail of what good looks like.

3.32 We recognise that smaller services can also be high risk for gender-based harms. Our Small but Risky Services Taskforce is a cross-Ofcom team, which targets services presenting a disproportionate level of harm to UK users due to their features, functionality, or harm-endorsing culture and the taskforce will continue to engage with high-risk services in 2026, including those associated with intimate image abuse, CSAM, and grooming.

3.33 We are also already using our enforcement powers where we have identified compliance issues. For example, we have opened cases on services' use of highly effective age assurance and safety measures to address child sexual abuse material.

3.34 We also recognise the diversity of services in scope of the Guidance, and have made changes to better reflect these differences. First, we have differentiated between good practice steps relevant to search services and good practice steps relevant to user-to-user services across **Chapters 3-5**. We have also used the case studies to showcase five new service types (messaging, image sharing, video sharing, and discussion forums), alongside the case studies on social media, gaming, dating, pornography, and search services from the draft guidance. Further details on changes to the case studies are explained in paragraphs 5.20-5.22 in this statement.

---

[49] Response(s) to our February 2025 consultation: The four Welsh Office of Police and Crime Commissioners, p.5; Barker, K, p.9; Popa-Wyatt, M, p2; Pinterest, p.7-8; Flux Digital Policy, p.3; Meta Platforms Inc, p.4; [✂]; LinkedIn, p.3; Online Dating and Discovery Association (ODDA), p. 1; [✂]; [✂]; Verifymy, p. 2; Popa-Wyatt, M, p.2; [✂]; [✂].

[50] Response(s) to our February 2025 consultation: Gender + Tech Research Lab Department of Computer Science, p. 6.

[51] Response(s) to our February 2025 consultation: The Cyber Helpline, p.8.

[52] Ofcom / Young People's Action Group Roundtable, 7 July 2025.

# Who the Guidance is intended to support

## What we proposed

3.35 At consultation, we framed the good practice steps as primarily aiming to help address the safety of women and girls online and noted that we expected that the good practice steps would improve safety of all users when taken effectively.

## Summary of stakeholder feedback

3.36 The vast majority of stakeholders acknowledged the need for dedicated consideration of safety features designed to improve the safety of women and girls. However, we received a wide range of feedback from stakeholders related to this framing.

3.37 Several stakeholders called on us to focus more on marginalised women's experience and/or intersectional risks, and provided evidence about how harms manifest in these contexts.[53] For example, End Violence Against Women and Girls Coalition (EVAW) and Glitch noted the distinct forms of abuse targeted at Black women[54] and others highlighted the experience of women and girls with disabilities.[55] Relatedly, some stakeholders called on us to focus more good practice steps on girls.[56] Some stakeholders highlighted the negative impact of harms such as cyberbullying have on children.[57] Conversely, one stakeholder raised concerns about the use of the term intersectionality as "divisive" and "unhelpful" and raised concerns that the draft guidance gave "'special' treatment" to those with several protected characteristics.[58]

3.38 We also received feedback from civil society organisations and individuals that the focus on women and girls was discriminatory or exclusionary to men and boys who can also experience the harms set out in the Guidance.[59] Several stakeholders noted Ofcom's responsibilities in relation to our role as a public authority, and our duties under the Equality Act 2010 ('the EA 2010') and HRA 1998 arguing this requires us to consider harms to men and boys.[60] One stakeholder argued the framing was inconsistent with the Government's position on violence against women and girls, which includes male victims.[61]

---

[53] Response(s) to our February 2025 consultation: Galop, p.1; Glitch, p.1; Equality Now, p.1; Office of the Derbyshire Police and Crime Commissioner, p.4; Women's Aid Federation of England, p.4; Antisemitism Policy Trust, p. 1-2; End Violence Against Women Coalition (EVAW), p.3; Girlguiding, p.4; End Violence Against Women Coalition (EVAW) Annex 2, p.4

[54] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (EVAW), p.3; Glitch, p.2.

[55] Response(s) to our February 2025 consultation: Equality Now, p.2; Girlguiding, p.8; End Violence Against Women Coalition (EVAW) Annex 2, p.4

[56] Response(s) to our February 2025 consultation: Barker, K. p.9; Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales p.6; NSPCC, p.13; Internet Matters, p.17; Plan International UK, p.15; British and Irish Law, Education and Technology Association (BILETA), p.2; Northern Ireland Commissioner for Children and Young People, p.11; Girlguiding, p.6-8.

[57] Response(s) to our February 2025 consultation: Galop, p.3; Plan International UK, p.7-8.

[58] Response(s) to our February 2025 consultation: Name Withheld 1, p.1.

[59] Response(s) to our February 2025 consultation: Name Withheld 1, p.1; [✂]; [✂]; Evans, M.I, p.2; Men and Boys Coalition Charity, p.1; Parity, p.1, p.5; Moxon, S.P, p.1; Name withheld 2, p.3; Ofcom / Men and Boys Roundtable, 29 May 2025.

[60] Response(s) to our February 2025 consultation: Name Withheld 2, p. 6; [✂]; Parity, p.4; Moxon, S.I., p.4; Evans, M.I., p,2; [✂].

[61] Response(s) to our February 2025 consultation: Men and Boys Coalition Charity, p.3.

3.39 Some individuals and organisations also provided evidence that men and boys experience gender-based harms and detailed the particular risks they face online. They argued this should be further explored in the Guidance, or that the harm areas should not be the focus of the Guidance because men and boys are affected (in some cases disproportionately).[62] For example, the Men and Boys Coalition Charity said that "tech companies should not believe that they do not have any responsibility, nor applicable guidance, to online harms against men and boys."[63]

3.40 A broad range of stakeholders noted that men and boys are disproportionately targeted by financially motivated sexual exploitation.[64] Other stakeholders provided evidence and recommendations for strengthening our positions on the impact of exposure to misogynistic content for men and boys,[65] and others noted links to extreme and dangerous misogynistic beliefs in gaming[66] and the role of algorithmic amplification[67] and influencers.[68] Further feedback related to misogynistic abuse is covered in paragraphs 4.35-4.42 in this statement.

3.41 Separately, we received feedback calling for the Guidance to be more explicitly inclusive of trans and non-binary people. For example, one stakeholder argued the draft guidance's "framing does not sufficiently acknowledge that gender-based harms can also affect non-binary, transgender, and intersex individuals, often in similar or intersecting ways."[69] Organisations and individuals also called for recognition of trans and/or non-binary people when designing and applying good practice.[70] Some also noted the disproportionate rates of online harm they experience, as well as specific kinds of abuse trans women and girls are targeted by.[71]

---

[62] Response(s) to our February 2025 consultation: Parity, p.2-3; Men and Boys Coalition Charity, p.2; Name Withheld 1, p.1; [✂]; [✂]; Moxon, S.P., p.1.
[63] Response(s) to our February 2025 consultation: Men and Boys Coalition Charity, p.3.
[64] Response(s) to our February 2025 consultation: [✂]; The four Welsh Office of Police and Crime Commissioners, p.7; Men and Boys Coalition Charity, p.4; Parity, p.2; Evans, M.I, p.1, p.9; Moxon, S.P., p.1; [✂]; [✂].
[65] Response(s) to our February 2025 consultation: White Ribbon UK, p.1; Northern Ireland Commissioner for Children and Young People, p.12; Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.5; Women's Aid Federation of England, p.2; Plan International UK, p.2-4; Ofcom / Men and Boys Roundtable, 29 May 2025.
[66] Response(s) to our February 2025 consultation: NSPCC, p.17
[67] Response(s) to our February 2025 consultation: White Ribbon UK, p.1; Integrity Institute Council on Technology & Social Cohesion; University of Southern California, Marshall School Neely Center p.7; Plan International, p.2-3; Ofcom / Men and Boys Roundtable, 29 May 2025.
[68] Response(s) to our February 2025 consultation: NSPCC, p.9; Integrity Institute Council on Technology & Social Cohesion; University of Southern California, Marshall School Neely Center p.4; Plan International UK, p.2; Ofcom / Men and Boys Roundtable, 29 May 2025.
[69] Response(s) to our February 2025 consultation: Institute for Strategic Dialogue, p.5.
[70] Response(s) to our February 2025 consultation: Galop, p.2-5; [✂]; Do-Ngoc, T., Carmel, E., p.1; [✂]; Institute for Strategic Dialogue, p.5; Cyber Helpline, p.1; Parity, p.11; NSPCC, p.7; Minderoo Centre for Democracy & Technology, p.2; Equality Now, p.1; Office of the Derbyshire Police and Crime Commissioner, p.4; Evans, M.I., p.6; [✂]; Ofcom / Translucent Meeting, 26 March 2025
[71] Response(s) to our February 2025 consultation: Galop, p.2-5; Do-Ngoc, T., Carmel, E., p.1; [✂]; Institute for Strategic Dialogue (ISD), p.5; The Cyber Helpline, p.1; NSPCC, p.7; The Minderoo Centre for Technology and Democracy at the University of Cambridge, p.2; Equality Now, p.1; Office of the Derbyshire Police and Crime Commissioner, p.4.

3.42 More generally, we received feedback on eradicating harm to all users or designing policies and systems that are 'gender-neutral' to support all users.[72] For example, Meta Platforms Inc., said "Policies, tools, resources, and outreach can take into account the online safety issues that may impact women and girls, while remaining gender neutral and relevant to all users".[73] Additionally, Pinterest said that "rather than establishing separate channels for different types of harms, we believe it is more efficient for platforms to ensure that their reporting channels are accessible and easy to use for everyone on their service."[74] This was echoed by other civil society stakeholders and individuals who expressed concern that providers would be punished for taking a 'gender-neutral' approach.[75] For example, one individual expressed concern that our approach "could result in reputational penalties for platforms that prioritise actual equality by taking a broader view of harm than gender exclusive focus."[76]

3.43 One stakeholder queried the definition of the terms 'gender' and 'gender identity.'[77] We also received feedback calling for Ofcom to "clarify what is meant by 'women and girls.'"[78] We received feedback that clear definitions for such terms were important for providers to ensure accurate reporting.[79]

3.44 We also received feedback related to the Supreme Court judgment in *For Women Scotland v Scottish Ministers* [2025] UKSC 16. A small number of stakeholders raised concerns that the Guidance might conflict or could cause confusion with the ruling,[80] and another said that it expected Ofcom "carefully reflect" on the ruling and incorporate implications into the Guidance.[81]

## Our final decision

3.45 The focus of the Guidance, as required by section 54 of the Act, is on content and activity "which disproportionately affects women and girls." More broadly, our statutory functions require us to consider impacts and risks to all users, taking account of all applicable ECHR rights under the HRA 1998, and our duties under the EA 2010.

3.46 We do not think it is necessary to further define user groups for the purposes of the Guidance. In line with the Act, both the foundational steps and the good practice steps are intended specifically to target content and activity that disproportionately affects women and girls. However, as we explained in the February 2025 Consultation, we are not proposing that the good practice steps are only aimed at women and girls. Rather, they were designed to apply more widely and we remain of the view that the good practices in the Guidance will benefit, and should be afforded to, anyone experiencing these harms.

---

[72] Response(s) to our February 2025 consultation: Name Withheld 1, p.2; Parity, p.6, p.10; Evans, M.I., p.5; [✂]; [✂]; [✂].
[73] Response(s) to our February 2025 consultation: Meta Platforms Inc., p.4;
[74] Response(s) to our February 2025 consultation: Pinterest, p.7.
[75] Response(s) to our February 2025 consultation: Name Withheld 1, p.2; Name Withheld 2, p.5;
[76] Response(s) to our February 2025 consultation: Evans, M.I., p.6-7.
[77] Response(s) to our February 2025 consultation: LGB Alliance, p.2. Ofcom / Translucent Meeting, 26 March 2025, also asked for the definition of 'gender' and 'sex.'
[78] Response(s) to our February 2025 consultation: LGB Alliance, p.3. The Free Speech Union, p.5, also asked for clarity on "the definition of 'woman' for the purposes of assessing misogyny."
[79] Response(s) to our February 2025 consultation: LGB Alliance, p.3.
[80] Response(s) to our February 2025 consultation: Free Speech Union, p.5; LGB Alliance. p.3.
[81] Response(s) to our February 2025 consultation: British and Irish Law, Education and Technology Association (BILETA), p.22.

3.47 We have made some changes to clarify how we expect the Guidance to support the safety of different groups in light of stakeholder feedback.

3.48 We have explicitly noted in **Chapter 1** (paragraph 1.8) of the Guidance that, while the Guidance focuses on harms disproportionately affecting women and girls, we expect the Guidance to help raise safety outcomes for anyone who may be affected by the harms.

3.49 We agree with stakeholders that different people can experience the harms we focus on in the Guidance, and that a wide range of factors can impact risk and vulnerability. We have, therefore, added additional evidence across **Chapter 2** of the Guidance to reflect this. We draw out more examples of the additional risks of harm to those based on demographic factors like race and ethnicity, sexuality, gender identity,[82] and age as well as and how dynamics like isolation and mental health contribute to risk.

3.50 We have also made several changes to the case studies across the Guidance to better reflect the broader impacts the good practice could have on different groups, for case studies covering the experiences of marginalised women (**Case study 3** and **Case study 14**), and girls (**Case study 5**). See **Section 5** in this statement for further details on these changes.

3.51 We agree with stakeholders that engaging with men and boys is an important aspect of tackling gender-based harms. We have updated a case study on harm prevention (**Case study 10**) focusing on the risks to boys from recommender systems promoting misogynistic abuse and sexual violence. We have also added evidence across **Chapter 2** of the Guidance on the risk of harm to men and boys. We have incorporated new evidence from stakeholders about, for example, the particular risk of sextortion and exposure to misogynistic abuse. We also note men and boys can also face specific barriers to reporting these harms.

3.52 We consider these changes to address concerns from stakeholders about applying the good practice more widely and clarify that our work on encouraging the take up of the Guidance takes into account our expectation that providers will deploy features to support all users. More information on the impacts and risks to users are detailed in the equality impact assessment and rights assessment in **Annex A3** in this statement.

3.53 We also acknowledge that stakeholders wanted us to comment on the implications of the Supreme Court's judgment in *For Women Scotland v Scottish Ministers* [2025] UKSC 16. This judgment was concerned with establishing the correct interpretation of the EA 2010 and, in particular, the meaning of the terms "sex", "man", "male", "woman" and "female" as used in the EA 2010 to define the parameters of sex-based discrimination and sex-based harassment for the purposes of that statute.[83] We do not consider that the Supreme Court

[82] We use the terms 'sexuality' and 'gender identity' here and within the Guidance as these are widely used and accessible terms used to describe groups and characteristics relevant to intersecting risks of harm. Where we are referring to specific protected characteristics set out in law, for example in our equality impact assessment (**Annex A3**), we use the terms 'sexual orientation' and 'gender reassignment' in line with the legislation. This is consistent with our approach in our Illegal Register of Risks and Children's Register of Risks.

[83] In this context, the Supreme Court examined the effect, if any, of the Gender Recognition Act 2004 on the interpretation of those terms in the EA 2010. The central question on appeal was whether the EA 2010 treats a trans woman with a Gender Recognition Certificate as a woman for its statutory purposes, or when the EA 2010 speaks of a "woman" and "sex" it is referring to a biological woman and biological sex [paragraph 8]. The Supreme Court concluded that it was only by adopting the latter approach that the provisions of the EA 2010

judgment has any direct implications for this Guidance as it does not comment on the interpretation of the words used in section 54 of the Act. The Guidance does not depend on the meaning of 'sex,' 'woman' and 'female' within the EA 2010.

# Encouraging take up among service providers

## Legal status of the Guidance

### What we proposed

3.54 We proposed this approach as it set out the foundations, or equivalent measures, that we have recommended providers take to comply with their duties under the Act, while also encouraging providers to take more ambitious action where relevant and feasible.

### Summary of stakeholder feedback

3.55 We received a range of stakeholder feedback on how we explained the status of the Guidance and on the links between foundational steps and good practice steps.

3.56 Many stakeholders gave feedback that the Guidance should be clearer with regards to the distinction between foundational and good practice steps, or called on us to explain the link between foundational steps and how Ofcom will enforce against providers found to not be in compliance.[84] For example, the Information Commissioner's Office (ICO) said that ambiguity about good practice steps "creates an uncertainty about whether legal obligation could be an appropriate lawful basis for personal information processing that is carried out when following the good practice steps."[85]

3.57 Similarly, several stakeholders called on us to be stronger in our language across the Guidance that companies have a clear responsibility to take action, including on safety-by-design approaches.[86] For example, the Institute for Strategic Dialogue (ISD) called for the framing to be reconsidered as it risks being seen as aspirational and could undermine the urgency and seriousness of the harms addressed.[87]

3.58 A small number of stakeholders said we should emphasise that the Guidance is "statutory guidance" meaning companies are expected to engage with it and have a reason for not following recommendations.[88]

---

could be interpreted and applied in a coherent and workable manner [paragraph 264]. The Supreme Court did not determine the appropriate meaning, usage and effect of "woman "and "sex" in all contexts outside the scope of the EA 2010, with the Supreme Court emphasising at the outset that "*it is not the role of the court to adjudicate on the arguments in the public domain on the meaning of gender or sex, nor is it to define the meaning of the word "woman" other than when it is used in the provisions of the EA 2010.*" [paragraph 2].

[84] Response(s) to our February 2025 consultation: Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p. 3; Women in Tech Policy Network, p.3; Welsh Government, p.2; LinkedIn, p.3; The Information Commissioner's Office (ICO), p.2-3; End Violence Against Women (EVAW) Annex 2, p.6; p.3; Institute for Strategic Dialogue (ISD), p.2; Johnstone, E., p. 8; End Violence Against Women Coalition, p. 2; Kira, B., Asser, Z., Ruiz, J., p.2.; Verifymy, p.1; LinkedIn, p.3; Refuge, p. 2; Thelwall, S. p.4; [✂].

[85] Response(s) to our February 2025 consultation: Information Commissioner's Office (ICO), p.3.

[86] Response(s) to our February 2025 consultation: Kira, B., Asser, Z., Ruiz, J., p.3; Plan International UK, p.9; [✂].

[87] Response(s) to our February 2025 consultation: Institute for Strategic Dialogue (ISD), p.1.

[88] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (Annex 2), p.6.. Online Safety Act Network, p.3-4 and End Violence Against Women Coalition (Annex 1), p.26 made similar points.

3.59 One stakeholder raised concerns about the "above and beyond approach" of good practice, saying this was "explicitly non-binding but framed as moral obligations" and arguing this framing imposed "a moral expectation that goes beyond the law".[89] techUK and the Mid-Size Platform Group (Middle Tech Coalition) raised concerns about the administrative burden or duplication in relation to completing various assessments or other obligations required under the Act.[90] Meta Platforms Inc. said that the foundational steps lay out "very comprehensive measures", including for women and girls, and noted that "while Ofcom is tasked to provide additional guidance for women and girls, and the clear split between foundational measures and good practice steps is helpful, the added nine proposed measures encompass significant additional measures where Ofcom itself sets out in this guidance that it would not be able to implement some as Code measures. "[91] Further comments on impact on providers are discussed in our impact assessment (**Annex A3**) of this statement.

3.60 We also received concerns that providers will not implement the Guidance because the good practice steps are voluntary, or that the voluntary nature will limit impact of the Guidance.[92] One stakeholder challenged our analysis that service providers have been slow to address online gender-based harms mainly because of a lack of diverse perspectives in leadership, particularly from women and marginalised groups, arguing that, while this is important, slowness to address online gender-based harms was due to the lack of mandatory Codes for violence against women and girls.[93] Relatedly, many stakeholders called on Ofcom to make good practice steps an "enforceable Code" or for there to be a Code of Practice on violence against women and girls.[94] One stakeholder urged Ofcom to "avoid making further 'good practice steps' into mandatory measures included in future Code iterations," suggesting the need for a stabilisation period "to allow the current online safety regime bed-in and take effect."[95]

3.61 We also received feedback on our chosen terminology. Some stakeholders wanted us to change 'foundational' to 'minimum' steps[96] or 'current expected practices.'[97] For example, one stakeholder said, "the framing of these steps as 'foundational' could be interpreted as aspirational for tech platforms."[98]

---

[89] Response(s) to our February 2025 consultation: Free Speech Union, p.1.
[90] Response(s) to our February 2025 consultation: Mid-Size Platform Group (Middle Tech Coalition), p.3; techUK, p.10
[91] Response(s) to our February 2025 consultation: Meta Platforms Inc, p.2.
[92] Response(s) to our February 2025 consultation: Clean Up the Internet, p.5; Office of the Derbyshire Police and Crime Commissioner, p.3; Internet Matters, p.18; Centre for Protecting Women Online, p.1-2
[93] Response(s) to our February 2025 consultation: Commissioner for Children and Young People (NICCY), p.9.
[94] Response(s) to our February 2025 consultation: 5Rights Foundation, p.2, p.10; Internet Matters, p.18; Centre for Protecting Women Online, p.2; Institute for Strategic Dialogue (ISD), p.2; Chayn, p.7; Galop, p.5; Plan International UK, p.16-17; End Violence Against Women Coalition (Annex 2), p.1, p.6; Glitch, p.7-8; [✂]; Women's Aid Federation of England, p.7.
[95] Response(s) to our February 2025 consultation: Mid-Size Platform Group (Middle Tech Coalition) p.5.
[96] Response(s) to our February 2025 consultation: Johnstone, E. p.8; 5Rights Foundation, p. 6; End Violence Against Women Coalition (EVAW) Annex 2, p. 3, p. 6; Glitch, p.9; End Violence Against Women Coalition, p.5; Women's Aid Federation of England, p.4; Suzy Lamplugh Trust, p. 12; Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p. 2-3; Plan International UK, p.17.
[97] Response(s) to our February 2025 consultation: Institute for Strategic Dialogue (ISD), p.6.
[98] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (Annex 1), p.5.

3.62 Respondents also asked us to reconsider the framing of 'good practice steps' to highlight that these are existing industry standards and practices,[99] or "future standards." [100] Several stakeholders argued this better reflected that many of these steps are already deployed by tech companies.[101]

## Our final decision

3.63 We are confirming our approach to having foundational steps drawn from the Codes and guidance we have published to aid compliance with the statutory duties, and the additional good practice steps which are intended to build on these.

3.64 We have amended the Guidance in **Chapters 1 and 3-5** to clarify how we are ensuring compliance with foundational steps.

3.65 We have clarified the difference between foundational steps and good practice steps, and have added information about the link between foundational steps and our compliance and enforcement programmes, and providers' duties under the Act. We have strengthened the language on the role of foundational steps compared to good practice steps at the beginning of **Chapters 3-5.**

3.66 We have also reminded providers of their responsibilities to comply with data protection law in **Chapter 1,** and where relevant, have signposted to Information Commissioner's Office guidance and resources in **Chapters 3-5**. This is discussed further in this statement in **Section 5** and our rights assessment (**Annex A3**).

3.67 We agree with stakeholders that the Codes play a crucial role in driving change across industry and will continue to update the Guidance, as appropriate, to reflect further iterations of Codes measures. We have also made changes following recent Code updates:

a) Since the February 2025 Consultation, we have updated some of the good practice in the Guidance to reflect measures that we are proposing in Consultation Additional Safety Measures, which was published in June 2025.[102] These draft Codes build on our initial package of measures, and include a range of relevant proposals, including hash matching for intimate image abuse, crisis response, and the use of automated content moderation and automated search moderation. As they are not final positions, we have included them as good practice steps, and we will update the Guidance to incorporate them as foundational steps once our position on these Codes is final.
b) We have updated relevant sections of the Guidance to reflect the final positions, as set out in Ofcom's Protection of Children Codes and Guidance (published April 2025) and the Transparency Reporting guidance (published July 2025), which were subject to consultation when we published the draft guidance.

3.68 Beyond this, we are unable to amend or introduce foundational steps through the Guidance, as the foundational steps reflect measures in the Codes and risk assessment guidance which we have already consulted on and published through separate processes.

---

[99] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (Annex 1), p.6; Glitch, p.9; End Violence Against Women Coalition (EVAW), p.18.
[100] Response(s) to our February 2025 consultation: Institute for Strategic Dialogue (ISD), p.5.
[101] Response(s) to our February 2025 consultation: 5Rights Foundation, p.8; End Violence Against Women Coalition (EVAW) Annex 1, p.6; End Violence Against Women Coalition (EVAW), p.18.
[102] These are currently good practice because we have not yet set out our final positions. We will update the Guidance where relevant as we finalise the Codes.

3.69 In line with our position at consultation, we consider that good practice steps are an opportunity to include recommendations that go further than the measures in our Codes. This may be because a recommendation reflects a measure that is still being consulted on (as in relation to the Additional Safety Measures Consultation referred to above) or we currently do not have the evidence base that would be needed to include it in our Codes. Through the good practice steps, we have been able to highlight a broader range of steps at this stage, such as algorithmic evaluations, improvements to reporting, and abusability testing. These good practice steps are not currently specifically recommended for compliance with enforceable duties, and as discussed in paragraph 3.19 in this statement, we intend to allow flexibility for providers to apply the Guidance proportionately (see impact assessment in **Annex A3**) using a range of alternative tools to encourage providers to take up this good practice.

3.70 **We are also confirming our terminology for foundational and good practice steps.** We consider the term 'foundational steps' better reflects the status of Codes measures as a safe harbour than the terms 'minimum steps' or 'current expected practice', as the Codes measures themselves are not binding and providers can take alternative measures to comply. We do not consider alternative names such as 'industry standard' to accurately describe the state of play – for example, our evidence suggests that voluntary transparency reports and hash matching for intimate image abuse are not widely adopted by services, and we believe the suggested terminology risks overstating what companies are already doing. We share the concern about ensuring we are pushing providers towards higher safety standards. While we do draw on industry, we also draw on prototypes including those co-designed by survivors and civil society, such as the case study on a reporting dashboard illustrated under Action 8 (**Case study 20**). In addition, while we do expect some of the good practice steps could be incorporated in the Codes in the future, the use of "future standards" across the board would pre-empt policy we have not yet consulted on, and flattens the nuanced considerations as to why some of these good practice steps may not be appropriate to include as Codes measures recommended for compliance with enforceable duties.

3.71 Finally, we considered using 'best practice' as set out in section 54 of the Act as an example of what the Guidance could contain. However, we remain of the view that it is not appropriate to label these as 'best practice' steps. This is to account for the rapid pace of innovation and the emergence of new evidence on effective harm mitigation strategies. We aim to be responsive to evolving practices, including those addressing emerging harms.

## Follow-up report 2027

### What we proposed

3.72 In the draft guidance, as explained in the previous section, we noted that the foundational steps are linked to services' legal duties under the Act and their take up will be monitored through existing supervisory and enforcement programmes.

3.73 We also urged providers to go further and take the good practice steps we have set out in order to make their services safer for women and girls. As part of our effort to encourage take up, we proposed to publish a report 18 months after we finalise the Guidance. We proposed that this report would look at how providers are using the Guidance and seek evidence from experts, as well as feedback from women and girls across the UK to understand how their online experience has changed.

## Summary of stakeholder feedback

3.74 Many stakeholders supported the proposal for the 2027 follow-up report.[103] Some noted that services may be incentivised to react due to risk of negative coverage[104] while others argued that the report could lead to premature positive coverage without showing "established and consistent progress over a significant period of time."[105]

3.75 Some stakeholders expressed concerns with the proposal, noting that the report may lead to reputational pressure on services or paint an inaccurate impression of services' trust and safety efforts.[106] Some said that section 54 of the Act does not include powers for Ofcom to publish the report.[107]

3.76 Some stakeholders called on Ofcom to clarify what effective implementation of the good practice steps means and how services will be monitored and evaluated.[108] One stakeholder emphasised the need to specify that companies must address harms across all nine actions in order to be considered to have to adopted a safety by design approach.[109] Clean Up the Internet suggested a benchmark for services for what level of reduction in online gender-based harms services are expected to deliver.[110] Several stakeholders suggested services should be assessed on overall effectiveness,[111] and others noted the report should take into account differences between business models, moderation frameworks, and content types.[112] One stakeholder suggested that the report should analyse how many enforcement cases Ofcom would have been entitled to begin if they had powers to enforce the Guidance.[113]

3.77 We also received feedback that the report should name services, [114] while one stakeholder raised concerns that naming services in the assessment could act as "some sort of prelude

---

[103] Response(s) to our February 2025 consultation: Barker, K, p.12; The four Welsh Office of Police and Crime Commissioners, p.6; Harrison, J., p.10; Flux Digital Policy, p.4; Children's Commissioner for England's Office, p.6; Marie Collins Foundation, p.4; Suzy Lamplugh Trust, p.11; British and Irish Law, Education, and Technology Association (BILETA), p.20; [✂]; Do-Ngoc, T., Carmel, E, p.5; Popa-Wyatt, M., p.2; Clean Up The Internet, p.5; Gender + Tech Research Lab Department of Computer Science, p.7; Bumble, p.9; Verifmy, p.4; Pinterest, p.7; Baroness Morgan of Cotes, p.2; Are, C., p.5; The Cyber Helpline, p.10; Image Angel, p.10; South West Grid for Learning (SWGfL), p.14; Age Check Certification Scheme, p. 2; Equality Now, p. 5; Commissioner for Children and Young People (NICCY), p.13; Welsh Women's Aid, p.4; Women's Aid Federation Northern Ireland, p.8; Institute for Strategic Dialogue (ISD), p. 11.

[104] Response(s) to our February 2025 consultation: Are, C, p.5.

[105] Response(s) to our February 2025 consultation: CyberSafe Scotland, p.2.

[106] Response(s) to our February 2025 consultation: [✂]; [✂]; Moxon, S..P, p.6; Name Withheld 2, p.5; Evans, M. I, p.6; Parity, p.11; [✂]; Free Speech Union, p.13.

[107] Response(s) to our February 2025 consultation: [✂]; Evans, M.I., p.6; Parity, p.11; [✂].

[108] Response(s) to our February 2025 consultation: Office of Derbyshire Police and Crime Commissioner, p.5; Harrison, J, p.12; Heriot-Watt University - University of Edinburgh, p.5; Gender + Tech Research Lab Department of Computer Science, p.2; [✂]; Meta Platforms Inc, p.12; Bumble, p.9; Verifymy, p.4; Flux Digital Policy, p.5; Thelwall, S., p.9-10; Kira, B. Asser, Z. Ruiz, J, p.14.

[109] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (EVAW), p.7.

[110] Response(s) to our February 2025 consultation: Clean Up The Internet, p.5.

[111] Response(s) to our February 2025 consultation: [✂]; Parity, p.12; Pinterest, p.8; Meta Platforms Inc, p.12; [✂]; Evans, M. I, p.7.

[112] Response(s) to our February 2025 consultation: [✂]; British and Irish Law, Education, and Technology Association (BILETA), p.20; [✂]; Bumble, p.9; Meta Platforms Inc, p.12; Pinterest, p.8; Equality Now, p.5.

[113] Response(s) to our February 2025 consultation: Baroness Morgan of Cotes, p,2.

[114] Response(s) to our February 2025 consultation: Are, C, p.5; The Cyber Helpline, p.10; Image Angel, p.10; Popa-Wyatt, M., p.3; Bolt Burden Kemp LLP, p.6.

to the possibility of more official enforcement."[115] Relatedly, many stakeholders argued that the report should include a framework to evaluate services, and recommended a range of evaluations such as rating, ranking, score cards, as well as methods to endorse services through certification, accreditation, badge, recognition programmes and a charter.[116] One stakeholder called for Ofcom to publish a dashboard for each service with metrics related specifically to women and girls' online safety.[117]

3.78 Two stakeholders said that the report should be informed by independent audits, user feedback, or self-reporting.[118] A range of stakeholders argued for the need to include children, young people, survivors, civil society, public bodies and partner agencies in the development of the report.[119] Equality Now said Ofcom should convene an independent panel of experts to advise on future iterations of the Guidance[120] and several stakeholders suggested a forum for providers to share practices and challenges.[121]

3.79 We received feedback that the report should be published before mid-2027 to limit the delay of the implementation of the Guidance by services.[122] Stakeholders also recommended that Ofcom publish a baseline survey before the 2027 follow up report.[123] A variety of stakeholders suggested continuous reporting and reviews of the Guidance to build accountability and responsibility and to consider emerging technologies and harms.[124]

## Our final decision

3.80 We are confirming our approach as set out at consultation and we plan to publish a report in the first half of 2027.

3.81 We do not agree that publishing a report as envisaged undermines the voluntary nature of the Guidance. As set out in paragraph 3.13 in this statement, we have made changes to the Guidance to further clarify that the foundational steps within the Guidance are tied to compliance with enforceable duties, while the good practice steps represent ways in which

---

[115] Response(s) to our February 2025 consultation: ACT | The App Association, p.4

[116] Responses to our February 2025 Consultation: University of Portsmouth, p.11; Barker, K, p.12; Gender + Tech Research Lab Department of Computer Science, p.7; Verifymy, p.4; Age Check Certification Scheme, p.3; British and Irish Law, Education, and Technology Association (BILETA), p.21; Equality Now, p.5; Harrison, J., p.11; Welsh Women's Aid, p.4; South West Grid for Learning (SWGfL), p.17; Commissioner for Children and Young People (NICCY), p.13; [✂]; Women's Aid Federation Northern Ireland, p.8; NSPCC, p.25; Bolt Burden Kemp LLP, p.6; Engendering Change, p.2; Scottish Government, p.5; Institute for Strategic Dialogue (ISD), p. 11; Internet Matters, p,19; Do-Ngoc, T., Carmel, E, p.5.

[117] Response(s) to our February 2025 Consultation: Harrison, J., p.10.

[118] Response(s) to our February 2025 Consultation: Gender + Tech Research Lab Department of Computer Science, p.7; Do-Ngoc, T., Carmel, E, p.4.

[119] Response(s) to our February 2025 Consultation: The Cyber Helpline, p.10; Harrison, J., p.13; Commissioner for Children and Young People (NICCY), p. 13; University of York, p. 10; Cybersafe Scotland, p.6; The four Welsh Office of Police and Crime Commissioners, p.6; The Jo Cox Foundation, p. 3; Lucy Faithfull Foundation, p.5; Thelwall, S., p. 13; [✂]; Do-Ngoc, T., Carmel, E, p.6; Verifymy, p.4; Image Angel, p.11; University of Portsmouth, p.11; Mayor of London, p.12.

[120] Response(s) to our February 2025 Consultation: Equality Now, p.5.

[121] Response(s) to our February 2025 Consultation: Parity, p.13; Evans, M. I, p. 8; [✂]; [✂].

[122] Response(s) to our February 2025 Consultation: Marie Collins Foundation, p.5; Women in Tech Policy Network, p.2; Welsh Government, p. 6; Verifymy, p.5; [✂].

[123] Response(s) to our February 2025 Consultation: Gender + Tech Research Lab Department of Computer Science, p.6; 5Rights Foundation, p. 9; NSPCC, p.25.

[124] Response(s) to our February 2025 Consultation: Bolt Burden Kemp LLP, p.6; Equality Now, p.5; Verifymy, p.5; NSPCC, p.26; Marie Collins Foundation, p.4; Children First, p.9; 5Rights Foundation, p.10; Bumble, p.4; Clean Up The Internet, p.1; Flux Digital Policy, p.4; Internet Matters, p.19; Scottish Government, p.2; [✂].

services can go further. Our expectation is that service providers can use their discretion to determine which good practice will be most relevant to their service and most impactful for their users, and we will make this clear in the report.

3.82 We have a broad power under section 164 of the Act to produce and publish reports about online safety matters. Also, in accordance with section 1(3) of the Communications Act 2003, we consider the preparation and publication of such a report is incidental or conducive to the carrying out of Ofcom's online safety functions.

3.83 In response to the feedback about how much detail the report should include, we are not able to confirm the specific structure or scope of the report at this stage. However:

a) The purpose of the report is to share information with the public and the wider sector to increase awareness and understanding about what services are doing to address online gender-based harms and the progress they are making in introducing good practice steps. Our aim is to empower users to make informed choices about the services they use and to build up our shared understanding on what works to address online gender-based harms.
b) Our expectation is that providers take the good practice steps that are relevant and applicable to their services, taking into consideration size, risk, functionalities, business models, and user base. For this reason, we will not be able to include comparative metrics on take up of individual good practice steps across services.
c) The report will be informed by evidence from a wide range of stakeholders including service providers, civil society organisations, academia, and expert public bodies. We also intend to engage with users and people with lived experience to understand how their online experience has changed.

3.84 With regards to feedback that Ofcom should convene a panel to advise on future iterations of the Guidance or a forum for services to share good practice, we will continue to engage with key stakeholders, including services, civil society, academia, those with lived experience and public bodies, to build our evidence and consider a variety of perspectives.

# 4. Scope of online gender-based harms

## Introduction

4.1 The Act sets out that the Guidance should focus on "*content and activity"* that *"disproportionately affects women and girls"* and in relation to which service providers have duties under Part 3 and Part 4 of the Act.[125]

4.2 This section covers feedback and our final decisions on topics related to how we have identified and framed the scope of such content and activity for the purposes of the Guidance. Specifically, we cover:

a) **Topic 1:** Our approach and framing
b) **Topic 2:** Misogynistic abuse and sexual violence
c) **Topic 3:** Pile-ons and coordinated harassment
d) **Topic 4:** Stalking and coercive control
e) **Topic 5:** Image-based sexual abuse
f) **Topic 6:** Other harms

## Our approach and framing

### Our approach: 'Disproportionately affects'

#### What we proposed

4.3 At consultation, we acknowledged that all online harms may have a gendered dynamic in terms of how they manifest, and therefore, we narrowed in on content and activity that represents, enables or reinforces misogyny, sexism and gender-based violence. We proposed that such content and activity has either a disproportionate or a distinct effect on women and girls online. Specifically, we identified the following key harm areas, which we referred to collectively as online gender-based harms:

**a) Online misogyny**
**b) Pile-ons and online harassment**
**c) Online domestic abuse**
**d) Image-based sexual abuse**

4.4 This approach aimed to capture both the greater likelihood of women and girls experiencing certain harms, and the distinct effect of certain harms on women and girls. We took this holistic view to identify areas most relevant to the safety of women and girls online, noting that robust quantitative and comparative data on online harms is limited.

[125] Part 3 of the Act sets out 'duties of care' for providers of regulated user-to-user and search services, including duties relating to tackling illegal content and content that is harmful to children. Part 4 of the Act sets out other duties on providers of regulated user-to-user and search services, many of which apply only to a subset of these services known as 'Category 1 services'. These are services which meet particular threshold conditions set out in secondary legislation.

4.5 We drew on a range of evidence sources and stakeholder engagement to arrive at this proposal, including Ofcom's own research, academic papers, reports from governmental and non-governmental organisations, as well as bilateral engagement with industry and civil society, including frontline organisations.

## Summary of stakeholder responses

4.6 We received a range of feedback on our approach to identifying the harm areas set out under the Act. A significant number of stakeholders were supportive of the four key harm areas and/or provided additional feedback and evidence outlining how these harm areas disproportionately or distinctly affect women and girls.[126] For example, the British and Irish Law, Education and Technology Association (BILETA) suggested the "framing of the 'content and activity' of concern is appropriately expansive and evidence-based" although BILETA also noted there are aspects not captured.[127] Another respondent said the four areas are "too restrictive and do not appropriately capture the full range of harmful behaviours that women experience online".[128] We address the detailed of this feedback for each harm area under the relevant sections in this statement.

4.7 Several civil society stakeholders and individuals questioned whether Ofcom had sufficiently established that women and girls experience certain online harms disproportionately.[129] These stakeholders raised concerns about the robustness of the evidence used to identify disproportionate effect, and the definitions used to understand online gender-based harms, which they said may not be representative.[130] They recommended the use of comparative, disaggregated data to better understand how online harms affect different groups, including men and boys.[131] These stakeholders also highlighted that under-reporting—including among men survivors and victims—may distort available data and should be considered.[132]

4.8 Many of these stakeholders shared evidence across the different harm areas questioning whether the effect on women and girls is disproportionate to men and boys.[133] This included research from the Pew Research Online Harassment Survey,[134] Office of National

[126] Response(s) to our February 2025 consultation: 5Rights Foundation, p.3; Age Check Certification Scheme, p.2; Are, C., p.2; Association of Police and Crime Commissioners, p.1; Barker, K., p.1; Bolt Burden Kemp, p.1; Children's Commissioner for England's Office, p.4-5; The Cyber Helpline, p.1; Flux Digital Policy, p.2; Match Group, p.1; Online Dating and Discovery Association (ODDA), p.1; TikTok, p.1; Verifymy, p.1; Women's Aid Federation of England, p.1.
[127] Response(s) to our February 2025 consultation: British and Irish Law, Education and Technology Association (BILETA), p.2.
[128] Response(s) to our February 2025 consultation: Centre for Protecting Women Online, p.5.
[129] Response(s) to our February 2025 consultation: Evans, M.I., p.1; Moxon, S.P., p.1; Name Withheld 2, p.1; Parity, p.1; [✂]; [✂].
[130] Response(s) to our February 2025 consultation: Evans, M.I., p.4; Moxon, S.P., p.3; Name Withheld 2, p.1; Parity, p.8; [✂]; [✂].
[131] Response(s) to our February 2025 consultation: Evans; M.I., p.6; Name Withheld 2, p.1; Parity, p.4; [✂]; [✂].
[132] Response(s) to our February 2025 consultation: Evans, M.I., p.1,5,9; Moxon, S.P., p.2; Parity, p.3,5,14; [✂]; [✂].
[133] Response(s) to our February 2025 consultation: Evans, M.I., p.1; Men and Boys Coalition Charity, p.1; Moxon, S.P., p.1; Parity, p1; [✂]; [✂].
[134] Pew Research Center, 2017. Online Harassment 2017. [accessed 3 November 2025]; Pew Research Center, 2021. The State of Online Harassment. [accessed 3 November 2025].

Statistics information on domestic abuse,[135] and UNESCO data[136] on rates of homicide of journalists.

4.9 Some stakeholders called for greater clarity on how harms are categorised and assessed (including how we assessed whether they disproportionately affect women and girls).[137] The Integrity Institute, Council on Technology & Social Cohesion, University of Southern California, Marshall School Neely Center ('Integrity Institute') said that harms should be defined and measured in a comparable way across platforms.[138]

4.10 We also received feedback on how we referred to the four harm areas collectively. Several stakeholders used or preferred alternative terms such as 'tech(nology) facilitated gender-based violence (TFGBV)'[139] and 'violence against women and girls (VAWG)'.[140] One stakeholder called for us to use 'sex-based' rather than 'gender-based' harms, in particular raising concerns that our proposed terminology could lead to the suppression of gender critical content.[141]

4.11 Further, the Online Safety Act Network asked that Ofcom consider the substance and recommendations of the Online VAWG coalition and amend and improve the Guidance accordingly.[142]

## Our final decision

4.12 We are confirming our approach set out at consultation to group content and activity that disproportionately affects women and girls into four key harm areas to outline the different ways harms manifest.

4.13 In line with our position at consultation, we use these key harm areas to describe common typologies of harm, not as a comprehensive view of all online gender-based harms. We recognise that these harm areas often overlap, however we have kept them distinct to help services understand specific tactics, dynamics and risks.

4.14 We have decided to continue referring to these collectively as 'online gender-based harms'. We use 'harm' to reflect the wide spectrum of content and activity we focus on, which has severe and enduring physical and psychological impacts.[143] We use 'gender-based' because it is a widely used term, and reflects that services need to consider how their users' gender affects the risks they face.

---

[135] ONS Centre for Crime and Justice, 2025. Redevelopment of domestic abuse statistics: research update May 2025. [accessed 3 November 2025].
[136] UNESCO, n.d. Statistics on Killed Journalists. [accessed 3 November 2025].
[137] Response(s) to our February 2025 consultation: Integrity Institute, Council on Technology and Social Cohesion, University of Southern California, Marshall School Neely Centre, p.1; Kira, B., Asser, Z. and Ruiz, J., p.1; Name Withheld 2, p.1.
[138] Response(s) to our February 2025 consultation: Integrity Institute, Council on Technology and Social Cohesion, University of Southern California, Marshall School Neely Centre, p.1.
[139] Response(s) to our February 2025 consultation: British and Irish Law, Education and Technology Association (BILETA), p.1; Integrity Institute, Council on Technology & Social Cohesion, University of Southern California, Marshall School Neely Center, p.3; The Young Women's Movement, p.3.
[140] Response(s) to our February 2025 consultation: British and Irish Law, Education and Technology Association (BILETA), p.1; Institute for Strategic Dialogue (ISD), p.6.
[141] Response(s) to our February 2025 consultation: Free Speech Union, p. 5.
[142] Response(s) to our February 2025 consultation: Online Safety Act Network, p.1.
[143] The Act sets out that 'harm' means physical or psychological harm.

4.15 As explained further below, at the start of each key harm area, we set out clearly how it relates to illegal content and content harmful to children under the Act. We signpost to the Illegal Content Judgements Guidance and Guidance on Content Harmful to Children to support service providers to identify relevant content, and ensure that providers following the Guidance are taking action on content and activity in scope of the Act. We recognise it can be challenging for providers to identify online gender-based harms and encourage providers to consider additional context available about relevant content and activity and how it is presented on the service.

4.16 We have made changes regarding the scope and terminology for three of the four key harm areas considering stakeholder feedback, evidence base and related matters:

a) Misogynistic abuse and sexual violence *(replacing 'Online misogyny')*
b) Pile-ons and coordinated harassment *(replacing 'Pile-ons and online harassment')*
c) Stalking and coercive control *(replacing 'Online domestic abuse')*
d) Image-based sexual abuse (*terminology unchanged from the draft guidance, expanded to include self-generated indecent imagery)*

4.17 Further details on the specific feedback and decisions we have made to each key harm area, including in relation to new evidence provided, are discussed in detail in **Section 4** in this statement.

4.18 We have also added a section in the Guidance setting out our approach to how we have identified harms that 'disproportionately affect' women and girls.

4.19 This is in response to stakeholder feedback querying our approach and evidence base. This section:

a) Clarifies our position that 'disproportionately affects' can mean that women and girls are more likely to experience online-gender based harms or that the effect on women and girls is distinct.
b) Clarifies that while certain harms may disproportionately affect women and girls, they do not affect women and girls exclusively. The Guidance explicitly recognises that anyone may experience these harms, and we include examples in **Chapter 2** of the Guidance about how, for example, men and boys are affected by certain types of image-based sexual abuse.
c) Explains the limitations of comparative data in the context of online gender-based harms. Evidence suggests that inconsistent definitions, lack of disaggregation, and structural barriers to disclosure all impact the quality of data available.[144] For example, we note that under-reporting— including among men and boys —may impact our understanding of who experiences online gender-based harms and to what extent. This reinforces our commitment to ongoing engagement with stakeholders and researchers to improve the evidence base.
d) Acknowledges that multiple characteristics can increase people's vulnerability. This includes adding evidence throughout **Chapter 2** of the Guidance on the risk of harm from, for example, misogynistic abuse targeting trans and non-binary people.

4.20 Across **Chapter 2** of the Guidance, we have made changes to better explain how each of the harm areas 'disproportionately affects' women and girls. We have drawn on both

[144] King's Global Institute for Women's Leadership (Schmid, C., Fearnside, H. and Rohregger, N.), 2024. *Measuring Gender Equality in the UK: Data on Violence Against Women and Girls*. [accessed 10 October 2025]. This report analyses both online and offline harm areas.

quantitative and qualitative evidence, where available, and have incorporated a range of new evidence provided by stakeholders to the Guidance. Changes we have made for each of the harm areas are set out, starting at paragraph 4.32 in this statement.

4.21 Where relevant, we have also updated our evidence base to reflect the final positions set out in the Children's Register of Risks.

## Framing: How online gender-based harms manifest

### What we proposed

4.22 At consultation, we used **Chapter 2** of the draft guidance to summarise the risks and impacts of online gender-based harms. We set out that such harms were intersectional, that they overlap and co-occur with other online and offline harms, and that they are exacerbated by societal norms.

4.23 We also provided an in-depth view of the risks and impacts to individuals from each of the four key harm areas. This broadly drew on evidence from the Illegal Harms Register of Risks, and the draft Children's Register of Risks.

### Summary of stakeholder responses

4.24 Many stakeholders were supportive of the framing of online gender-based harms, but as noted at 3.37 in this statement, several stakeholders called for more information on intersectional impacts.[145] Many other stakeholders provided feedback and evidence on how these harms overlap, including with offline harms.[146]

4.25 Another stakeholder noted that gender-based harms are "deeply rooted in the inequality between men and women that persists worldwide".[147] Several stakeholders called for the Guidance to go further in recognising new and emerging risks and forms of harms[148] such as virtual harassment and assault in the metaverse,[149] chatbots,[150] and the exploitation of facial recognition technology.[151]

4.26 One stakeholder argued that the draft guidance lacked evidence and discussion on perpetrators.[152] Many stakeholders provided us with feedback and evidence about the tactics used by perpetrators, and how gender-based harms are reinforced and enabled by particular business models, features and functionalities.[153] Relatedly, two stakeholders

---

[145] Response(s) to our February 2025 consultation: Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.4; Glitch, p.1; [✂]; South West Grid for Learning (SWGfL), p.2; NSPCC, p.5-8; Women's Aid Federation of England, p.4-5.

[146] Response(s) to our February 2025 consultation: Bolt Burden Kemp, p.1; Children First, p.5; Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.5-6; Mayor of London, p.1; [✂]; [✂]; Tranchese, A., p.1; Women's Aid Federation of England, p.1-2.

[147] Response(s) to our February 2025 consultation: The Young Women's Movement, p.4.

[148] Response(s) to our February 2025 consultation: Bumble, p.5; Children's Commissioner for England's Office, p.5.

[149] Response(s) to our February 2025 consultation: Association of Police and Crime Commissioners, p.2; Mayor of London, p.8; Women's Aid Federation of England, p.7.

[150] Response(s) to our February 2025 consultation: Women's Aid Federation of England, p.7.

[151] Response(s) to our February 2025 consultation: Mayor of London, p.8.

[152] Response(s) to our February 2025 consultation: Clean Up The Internet, p.3; Ending Violence Against Women Coalition (EVAW) Annex 2, p.5.

[153] Further details on the specific evidence provided and how we have addressed it are included under each harm area in the relevant sections in this statement.

called for the Guidance to go further in recognising that platform design[154] and business models themselves can be harmful.[155] Stakeholders also highlighted specific service features including algorithms[156] and "accounts which use concealed or deceptive identities to perpetrate harm".[157]

4.27 Some stakeholders noted that in places, the draft guidance used the passive voice to describe the actions of perpetrators.[158] One stakeholder noted that this "masks the action and responsibility of the perpetrator".[159] Many stakeholders noted that men are the main perpetrators of illegal gender-based harms.[160] One stakeholder argued that "acknowledging the role of male perpetration… could help inform better platform interventions, such as early detection of radicalisation pathways and risk factors in male-dominated user ecosystems".[161] Other stakeholders said that women also perpetrate harms such as intimate image abuse and domestic abuse.[162]

## Our final decision

4.28 We have amended **Chapter 2** of the Guidance in response to feedback on the framing of the key harm areas.

4.29 Across all sections in **Chapter 2** of the Guidance, we have integrated more evidence on how perpetrators exploit service features to target women and girls, seeking to provide relevant information for service providers about how service design enables harm. We have added references to specific actions or good practice steps which we expect to have particular relevance to, or challenges for, each key harm area. For example, we note that **Action 6** is particularly relevant for reducing the circulation of misogynistic abuse and sexual violence. However, we also note that **Action 8**, on enabling user reports, is likely to be less effective in communities dedicated to the sharing of misogynistic abuse and sexual violence. More information on these changes is outlined in the following sections.

4.30 We are alive to the risks and perpetrator tactics enabled by new and emerging technologies. Where such content and activity falls under the four key harm areas, we have incorporated the evidence in **Chapter 2** of the Guidance, and we have made changes at 2.9 in the Guidance recognising that online gender-based harms are constantly evolving alongside technology. We also have several good practice steps focused on identifying and responding to emerging risks, for example see paragraph 4.47 in the Guidance.

---

[154] Response(s) to our February 2025 consultation: Institute for Strategic Dialogue (ISD), p.3

[155] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (EVAW) Annex 2, p.3.

[156] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (EVAW), p.4.

[157] Response(s) to our February 2025 consultation: Clean Up The Internet, p.2.

[158] Response(s) to our February 2025 consultation: Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.3; End Violence Against Women Coalition (EVAW) Annex 1, p.28; End Violence Against Women Coalition (EVAW) Annex 2, p.5; Refuge, p.4.

[159] Response(s) to our February 2025 consultation: Refuge, p.4.

[160] Response(s) to our February 2025 consultation: CARE (Christian Action Research and Education), p.3; End Violence Against Women Coalition (EVAW) Annex 1, p.28; End Violence Against Women Coalition (EVAW) Annex 2, p.5; Engendering Change, p.1; Institute for Strategic Dialogue (ISD), p.4; Refuge, p.5; Women's Aid Federation of England, p.2.

[161] Response(s) to our February 2025 consultation: Institute for Strategic Dialogue (ISD), p.5.

[162] Response(s) to our February 2025 consultation: Institute for Strategic Dialogue (ISD), p.4. Ofcom / Refuge's Survivor Panel, 10 June 2025.

4.31 We have also added evidence on how online gender-based harms are perpetrated where relevant. We have adjusted the Guidance to draw out a more active voice when discussing perpetrators of illegal harms in the Guidance. We have, however, retained the use of some passive language such as 'those doing harm' in the Guidance when describing children sharing misogynistic abuse, as we have received feedback from stakeholders previously indicating the importance of not labelling children as perpetrators.

# Misogynistic abuse and sexual violence

## Misogynistic abuse

### What we proposed

4.32 At consultation we used the term 'online misogyny' to describe a wide range of content and behaviour online which engages in, normalises or encourages misogynistic attitudes and ideas. We explained that illegal online misogyny (such as harassment, threats and abuse, or hate) is covered in the Illegal Harms Register of Risks and online misogyny that is harmful to children (such as abuse and hate content, violent content and pornographic content) in the draft Children's Register of Risks.

4.33 We explained that online misogyny occurs in a variety of online spaces and on services of different sizes. We included evidence on the role of 'misogynistic influencers', recommender feeds and dedicated communities in promoting online misogyny content. We also noted the effects on girls and boys from such content.

4.34 We included a subsection on overlaps between misogyny and sexually explicit content – we cover stakeholder feedback and our final decision on this from paragraph 4.59 in this statement.

### Summary of stakeholder responses

4.35 We received a significant amount of feedback on the inclusion of online misogyny in the draft guidance.

4.36 Several stakeholders indicated broad support for the inclusion of online misogyny in the draft guidance and emphasised the importance of addressing this content.[163] Stakeholders provided additional feedback and evidence that misogynistic abuse which may not – or does not – meet the threshold of illegality can:

a) Have a harmful impact on adults, including men and boys. One stakeholder provided evidence that young fathers are particularly susceptible to misogynistic content,[164] and White Ribbon UK argued "Such content reinforces rigid, harmful ideas about masculinity, limits emotional expression, harms men and boys' mental health and distorts perceptions of healthy relationships".[165] White Ribbon UK also pointed out that men and boys who may want to act as allies can be targeted themselves.[166]

[163] Response(s) to our February 2025 consultation: Cybersafe Scotland, p.4; Engendering Change, p.1; Commissioner for Children and Young People (NICCY), p.14; White Ribbon UK, p.1; Women's Aid Federation of England, p.2.
[164] Response(s) to our February 2025 consultation: Internet Matters, p.2.
[165] Response(s) to our February 2025 consultation: White Ribbon UK, p.1.
[166] Response(s) to our February 2025 consultation: White Ribbon UK, p.1.

b) Be connected to illegal harms.[167] For example, the Domestic Abuse and Victim's Commissioners for England and Wales argued that "behaviours that are not explicitly illegal contribute to both a conducive context for illegal harms and the broader normalisation of violence against women and girls".[168] Another stakeholder emphasised that "Online misogyny exists on a spectrum. While some extreme forms are clearly illegal…many other expressions may be legal yet harmful".[169]
c) Overlap with intersectional dynamics. Stakeholders highlighted misogynoir,[170] transmisogyny[171] and misgendering[172] and links between sexism and antisemitism.[173]
d) Overlap with wider structures. One academic argued misogyny should be understood "as a system of coercion – i.e. a set of ideological, behavioural, and institutional mechanisms that uphold patriarchal power and male dominance through harassment, punishment, intimidation, exclusion and violence".[174]

4.37 Some stakeholders commented on the terminology of 'misogyny'. One civil society stakeholder specifically welcomed the use of the term misogyny.[175] However, one individual said that misogyny is ideological and/or with no scientific basis.[176] Another individual argued we should use "gender based hatred, contempt or prejudice" rather than misogyny to avoid excluding men[177] and several stakeholders called for the inclusion of misandry in the Guidance.[178] One stakeholder argued we should not use the term violence to describe harm that is not physical.[179]

4.38 We also received feedback from a range of stakeholders arguing that our description of online misogyny was overly broad or imprecise, and therefore introduced risks around the application of good practice steps to such content.[180] For example, one stakeholder argued that misogyny is "an umbrella term that is not universally understood […]" and "a pervasive high level cultural concept that affects both online and offline communities".[181] Another stakeholder noted that the complexity of defining what is 'harmful' content may pose a challenge to effective enforcement and oversight.[182] Several stakeholders called for more information or raised concerns about how good practice steps, particularly relating to

[167] Response(s) to our February 2025 consultation: Centre for Protecting Women Online, p.5-6; Ending Violence Against Women and Girls (EVAW), p.14; Kira, B., Asser, Z. and Ruiz, J., p.4.
[168] Response(s) to our February 2025 consultation: Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.5.
[169] Response(s) to our February 2025 consultation: Kira, B., Asser, Z. and Ruiz, J., p.4-5.
[170] Response(s) to our February 2025 consultation: Ending Violence Against Women and Girls (EVAW), p.5-6; Glitch, p.1; Women's Aid Federation, p.4.
[171] Response(s) to our February 2025 consultation: Galop, p.1.
[172] Response(s) to our February 2025 consultation: [✂]; Galop p.4.
[173] Response(s) to our February 2025 consultation: Antisemitism Policy Trust p.2.
[174] Response(s) to our February 2025 consultation: Popa-Wyatt, M. (Annex), p.1.
[175] Response(s) to our February 2025 consultation: Refuge, p.2.
[176] Response(s) to our February 2025 consultation: Moxon, S.P., p.3
[177] Response(s) to our February 2025 consultation: Name Withheld 1, p.1.
[178] Response(s) to our February 2025 consultation: Evans, M.I., p.2; Moxon, S.P., p.4; Parity, p.2; [✂]; [✂].
[179] Response(s) to our February 2025 consultation: Name Withheld 1, p.1.
[180] Response(s) to our February 2025 consultation: Centre for Protecting Women Online, p.5; Free Speech Union, p.2; [✂]; Integrity Institute, Council on Technology & Social Cohesion, University of Southern California, Marshall School Neely Center, p.1; Office of the Derbyshire Police and Crime Commissioner, p.3.
[181] Response(s) to our February 2025 consultation: Meta Platforms Inc., p.2.
[182] Response(s) to our February 2025 consultation: Welsh Government, p.1.

content moderation, should be proportionately applied when addressing harm areas that cover content and activity that is not illegal.[183]

4.39 Stakeholders argued that we should broaden our definition of online misogyny to include more kinds of content and activity that may not meet the threshold of illegality. For example, stakeholders called for the Guidance to recognise content 'normalis[ing] misogyny,' and misogynistic 'prank videos'.[184] One stakeholder argued that "online misogyny is often experienced by children and young people in more indirect forms, such as in the context of jokes and memes about gendered violence or harmful gendered stereotypes".[185] Another stakeholder argued online abuse includes belittlement, criticism of appearance, emotional harm, and defamation.[186]

4.40 Other stakeholders argued this section should only include content and activity that meets the threshold of illegality to protect freedom of expression. Several civil society organisations and individuals argued that the good practice steps to address online misogyny should be removed because this infringes the right to freedom of expression.[187] These respondents cited concerns about the potential for service providers to engage in take down of a wide range of content and activity as a result, including 'laddish or immature banter,'[188] 'criticisms of feminism,'[189] and gender-critical views.[190] At the same time, many civil society stakeholders and academics argued women's freedom of expression and other human rights are compromised when perpetrators are able to send them gendered abusive, violent, and hateful content – including content that is not illegal.[191] One academic indicated that "Recent scholarship and regulatory commentary highlight that while some of these harms may not meet criminal thresholds, they still result in exclusionary and chilling effects on women's speech and participation online".[192]

4.41 We also received a range of stakeholder feedback about how misogynistic abuse manifests and its impact. One stakeholder noted the importance of understanding content that "encourages and normalises abusive behaviours".[193] Other stakeholders raised the role of emerging technologies such as AI chatbots[194] and avatars,[195] as well as recommender

[183] Response(s) to our February 2025 consultation: British and Irish Law, Education and Technology Association (BILETA), p.5,8,14; Centre for Protection Women Online, p.5-6,8; [✂]; Kira, B. Asser, Z. and Ruiz, J., p.9; Office of the Derbyshire Police and Crime Commissioner p.3.
[184] Response(s) to our February 2025 consultation: Engendering Change, p.2; Institute for Strategic Dialogue (ISD), p.4.
[185] Response(s) to our February 2025 consultation: CyberSafe Scotland, p.1.
[186] Response(s) to our February 2025 consultation: University of York, p.1.
[187] Response(s) to our February 2025 consultation: Evans, M. I., p.3; Free Speech Union, p.1-4; Parity, p.2; [✂]; [✂].
[188] Response(s) to our February 2025 consultation: Free Speech Union, p.3.
[189] Response(s) to our February 2025 consultation: Parity, p.2.
[190] Response(s) to our February 2025 consultation: Free Speech Union, p.5-7.
[191] Response(s) to our February 2025 consultation: Centre for Protecting Women Online, p.3-4; The Cyber Helpline, p.1; Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.3-4; End Violence Against Women Coalition (EVAW), p.6; Institute for Strategic Dialogue (ISD), p.2; Online Safety Act Network, p.3; Plan International, p.9-10; Popa-Wyatt, M., p.3; Women's Aid Federation of England, p.14-16.
[192] Response(s) to our February 2025 consultation: Barker, K., p.5.
[193] Response(s) to our February 2025 consultation: University of Portsmouth, p.2.
[194] Ofcom / Men and Boys Roundtable, 29 May 2025.
[195] Response(s) to our February 2025 consultation: Ending Violence Against Women (EVAW) Annex 1, p.21.

systems, in promoting misogynistic content online[196] - especially to young men and boys.[197] Women's Aid Federation of England also suggested the Guidance should consider the impact of autoplay functionalities.[198] Some stakeholders argued specifically that there should be greater recognition of 'incel culture' under this harm area,[199] including calls to recognise the "coded language of incel culture".[200] The Commissioner for Children and Young People also set out the "challenges that boys and young men face in being drawn into misogynistic online cultures such as the 'incel culture'"[201] and one stakeholder highlighted the negative impacts of misogynistic content on men and boys.[202] Further, stakeholders highlighted overlaps between misogynistic content and other forms of extremist content or radicalisation.[203] One stakeholder referred to a report which identified "online misogyny as a key tenant of extremism".[204] Children First expressed concerns about the risk of violent actions stemming from misogynistic cultures online[205] and the Domestic Abuse and Victims' Commissioners for England and Wales called for the Guidance to "go further in exploring the consequences of online misogyny and emphasising the importance of early interventions to prevent illegal harm".[206]

4.42 As noted in paragraphs 4.59-4.67 in this statement, we also received additional evidence about harm from sexually explicit content, including pornography.

## Our final decision

4.43 We are confirming our position at consultation to focus on misogynistic content and activity. However, we have made several amendments to the Guidance.

4.44 These changes are in line with our position on scope and proportionality outlined in paragraphs 3.13-3.22 in this statement.

4.45 We have clarified that the harm addressed is 'misogynistic abuse and sexual violence'. This is in line with stakeholder feedback that the term online misogyny was imprecise and overly broad and could lead to over-moderation or action taken on content beyond what is intended by our policy (such as legitimate debates about gender roles or non-abusive banter). We have retained the use of 'misogyny' given its specificity to the issue of gender-based harm and stakeholder feedback in support of the term.

4.46 We have set out a more precise definition and explanation of how this harm area relates to illegal content and content harmful to children.[207] The new description in the Guidance

---

[196] Response(s) to our February 2025 consultation: Internet Matters, p.2-3; Women's Aid Federation of England, p.2.
[197] Response(s) to our February 2025 consultation: 5Rights Foundation, p.3; Clean Up The Internet, p.2.
[198] Response(s) to our February 2025 consultation: Women's Aid Federation of England, p.11.
[199] Response(s) to our February 2025 consultation: Mayor of London, p.8; [✂].
[200] Response(s) to our February 2025 consultation: The Minderoo Centre for Technology and Democracy at the University of Cambridge, p.1.
[201] Response(s) to our February 2025 consultation: Commissioner for Children and Young People (NICCY), p.8.
[202] Response(s) to our February 2025 consultation: White Ribbon UK, p.1.
[203] Response(s) to our February 2025 consultation: Classification Office, p.2; [✂]; Popa-Wyatt, M. (Annex), p.4.
[204] Response(s) to our February 2025 consultation: Crest Advisory, p.3
[205] Response(s) to our February 2025 consultation: Children First, p.5.
[206] Response(s) to our February 2025 consultation: Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.5-6.
[207] Providers of category 1 services also have additional responsibilities related to empowering adult users to control their exposure to certain types of content that do not meet the threshold for illegality, including hateful and abusive content. We will be publishing a Code of Practice and Guidance for these providers to help

focuses on misogynistic content and activity that is abusive and hateful towards women and girls and/or depicts, invokes, encourages or normalises gender-based violence, including sexual violence. This definition ties directly to the types of content and activity we are intending to capture, as set out under the Act.

4.47 In line with our decision, set out in paragraph 4.15 in this statement, we explain that misogynistic abuse and sexual violence covers certain types of illegal content (threats and abuse[208]) and content harmful to children (abuse and hate content[209] and violent content[210]). We also explain that the harm area covers content depicting, invoking, encouraging or normalising sexual violence, including certain types of pornographic content.

4.48 Under a new subsection called 'misogynistic abuse', we discuss abusive content and content that incites hatred against women and girls as a group, including some forms of abuse directed towards individual women and girls[211] as well as content which glorifies gender-based violence such as controlling or coercive behaviour.

4.49 Under a new subsection called 'sexual violence', we cover content which depicts, invokes, encourages or normalises sexual violence. As noted above, the next section of this statement provides a detailed overview of our position on sexually explicit content.

4.50 We have decided not to narrow the scope of the Guidance to only include illegal harms in relation to misogynistic abuse and sexual violence. We acknowledge the concerns from stakeholders related to freedom of expression. However, we consider it to be proportionate and in line with the policy objective of the Guidance to retain information about the impacts of misogynistic abuse and sexual violence which spans both illegal content and content harmful to children. This is in line with evidence that this content disproportionately affects women and girls, including its impacts on the human rights of women and girls. In addition, there is evidence of links between such content and illegal harms, see **Chapter 2** in the Guidance.

4.51 We have decided not to expand this harm area to include examples of content outside of that captured by illegal content or content harmful to children, such as prank videos which do not meet the threshold of abusive and/or violent content. We consider that broadening our definition would introduce significant complexity by incorporating content and activity not set out under the Act. Where this complexity leads to uncertainty, this could result in over-moderation of content which is in turn likely to have a disproportionate impact on freedom of expression. However, it is important for service providers to be aware that content purporting to be memes or jokes could amount to misogynistic abuse[212] and be in scope of the Guidance (and relevant duties).

---

them comply with their user empowerment duties in due course. For more information see: Ofcom, 2025. Ofcom's approach to implementing the Online Safety Act.

[208] More information is set out in Section 4 of the Illegal Harms Register of Risks and Section 3 the Illegal Content Judgements Guidance.

[209] More information is set out in Section 5 of the Children's Register of Risks and Section 6 of the Guidance on Content Harmful to Children.

[210] More information is set out in Section 7 of the Children's Register of Risks and Section 8 of the Guidance on Content Harmful to Children.

[211] This includes some types of image-based content that does not meet the threshold of intimate image abuse but is abusive, for example 'semen images.' For more information, see paragraph 4.93 in this statement.

[212] This could include "a derogatory meme or caricature of a person, with threatening, abusive, hurtful or harmful commentary." For more detail see Section 6 of the Guidance on Content Harmful to Children.

4.52 In line with the position set out on scope in paragraph 3.18 in this statement, we have made changes to ensure the good practice steps for misogynistic abuse and sexual violence are proportionate and to explain how these can be taken. For example, we set out that service providers could afford all users the good practice steps related to user controls (Action 7) to address misogynistic abuse and sexual violence. We consider this proportionate because it enables adults to choose the kind of content and activity they are exposed to and to restrict their exposure to this content if they wish.[213] This is also in line with the user empowerment duties for Category 1 services in section 15 of the Act.

4.53 On the other hand, we do not recommend deploying good practice steps that proactively identify and remove misogynistic abuse and sexual violence (Action 6), instead limiting these mitigations only to illegal content. Further details about our approach to applying the good practice steps to misogynistic abuse and sexual violence can be found under each action in **Section 5**, and in the rights assessment (**Annex A3**), in this statement.

4.54 We consider that these changes provide clarity and address stakeholder concerns. We also consider that these clarified definitions, alongside the changes outlined in paragraph 3.18 in this statement on the good practice steps, ensure that service providers following the Guidance are only taking action on content and activity in scope of the Act, mitigating the risk of unduly restricting the right to freedom of expression (for example, as a result of over-moderation caused by a lack of clarity over definitions of content).

4.55 We have made several changes to the Guidance to incorporate additional evidence, including evidence provided by respondents, about how misogynistic abuse manifests.

4.56 In line with our overall approach set out in paragraph 4.20 in this statement, we draw on quantitative evidence to set out the distinct and disproportionate effect misogynistic abuse has on women and girls. We also recognise that this harm affects men and boys.

4.57 We have added more evidence in paragraph 2.24 in the Guidance on how services, and individual content creators, benefit from recommender systems which reward shocking content. We have also explained that this can be reinforced by endless feeds and autoplay functionalities. We have also added evidence in paragraph 2.26-2.29 in the Guidance on misogynistic communities, such as 'incel' communities. We recognise that these communities can contain extremist views. We set out that these communities promote user anonymity and use coded symbols and language that are not widely understood.

4.58 We have also added new evidence in the Guidance on overlaps between relevant harms. We have included this evidence to help service providers understand and address this content. This also incorporates stakeholder feedback on how misogynistic abuse intersects with other forms of discrimination, including homophobia and transphobia.

## Sexually explicit content, pornography and sexual violence

### What we proposed

4.59 At consultation, we included evidence on sexually explicit content including some kinds of pornography as a subsection within 'online misogyny'.

[213] Providers must comply with duties to protect children from primary priority content (e.g. pornography) and priority content (e.g. abuse, hate and violence).

4.60 In this section, we noted the relationship between some forms of pornography and misogynistic and sexual violence. We noted that regardless of the expectations set out in the draft guidance, all pornography is primary priority content, and children must be prevented from encountering it.

4.61 This position predated the recommendations from Creating a safer world: the challenge of regulating online pornography, the Independent Pornography Review, which was not published in time for the evidence and findings to be reflected within our draft guidance.

## Summary of stakeholder responses

4.62 We received a significant amount of feedback on this issue. Some stakeholders were supportive of our approach.[214] A range of stakeholders called for us to strengthen our position on pornography in the Guidance, for example two stakeholders argued that there should be a standalone section on pornography in the Guidance.[215]

4.63 Many stakeholders argued there needed to be more acknowledgement of how mainstream pornography normalises violence against women and girls, for example through misogynistic tropes that dehumanise women.[216] In addition, civil society and public bodies argued there needed to be more acknowledgement in the Guidance of the link between consumption of pornography and harmful or violent sexual behaviour,[217] including links to sexual exploitation,[218] domestic abuse[219] and the sexualisation of children.[220] The British Board of Film Classification (BBFC) noted that content excluded from their standards represents a credible risk of harm, for example "promoting dangerous emulation or by encouraging unhealthy fantasies relating to violence, sadism, abuse and non-consensual behaviour".[221] Some stakeholders called for us to create parity between what is barred online and offline – for example, Baroness Bertin and other stakeholders noted that some content allowed online may not be allowed to be distributed offline if it is unclassifiable by the BBFC,[222] including step-incest,[223] and age based role -play content.[224]

---

[214] Response(s) to our February 2025 consultation: [✂]; Gallop, C., p.1; Internet Matters, p.3.
[215] Response(s) to our February 2025 consultation: Baroness Bertin, p.1; CARE (Christian Action Research and Education), p.1.
[216] Response(s) to our February 2025 consultation: Baroness Bertin, p.1-2; British Board of Film Classification (BBFC), p.2; CARE (Christian Action Research and Education), p.3; Centre to End All Sexual Exploitation (CEASE), p.1; Collective Shout, p.7-9; Ending Violence Against Women Coalition (EVAW) Annex 2, p.4-5; Institute for Strategic Dialogue (ISD), p.5; Internet Matters, p.4-5; [✂]; Tranchese, A., p.1.
[217] Response(s) to our February 2025 consultation: Baroness Bertin, p.1-2; British Board of Film Classification (BBFC), p.2; CARE (Christian Action Research and Education), p.3; Centre to End All Sexual Exploitation (CEASE), p.1; Children's Commissioner for England's Office, p.2-3; Collective Shout, p.7-9; Common Sense Media, p.4; Internet Matters, p.4-5.
[218] Response(s) to our February 2025 consultation: Centre to End All Sexual Exploitation (CEASE), p.3-4; Collective Shout, p.4.
[219] Response(s) to our February 2025 consultation: Centre to End All Sexual Exploitation (CEASE), p.1; Collective Shout, p.3.
[220] Response(s) to our February 2025 consultation: Collective Shout, p.4-7.
[221] Response(s) to our February 2025 consultation: British Board of Film Classification (BBFC), p.1.
[222] Response(s) to our February 2025 consultation: Baroness Bertin, p.2; The British Board of Film Classification (BBFC), p.2; Internet Matters, p.2-3.
[223] Response(s) to our February 2025 consultation: CARE (Christian Action Research and Education), p.4-5; Centre to End All Sexual Exploitation (CEASE), p.4.
[224] Response(s) to our February 2025 consultation: CARE (Christian Action Research and Education), p.5.

4.64 Stakeholders called for the Guidance to make explicit reference to deepfake intimate image abuse,[225] sexual exploitation,[226] strangulation[227] and the use of non-consensual 'nudification' tools.[228] CARE (Christian Action Research and Education) and the Centre to End All Sexual Exploitation (CEASE) argued the Guidance needed to make more references to the risks of AI-generated pornography.[229]

4.65 Some stakeholders argued that not all pornography is violent or harmful.[230] For example, one academic stakeholder noted that this positioning "pathologises sex and sex workers."[231] Relatedly, one industry stakeholder said that "while intimate image abuse and coercive sexual content must be tackled forcefully, consensual depictions of sexuality - including commercial pornography featuring adult performers under formal release agreements - should not be implicitly categorised as harmful to women and girls."[232]

4.66 Separately, two stakeholders raised concerns about how educational, promotional or testimonial content related to women's health issues or women's experiences of abuse can be restricted by blanket bans on terms related to sexual violence, women's bodies and sexual health.[233]

4.67 In addition, we also received feedback recommending we include specific good practice steps targeted at pornographic and sexually explicit content, or pornography services. We summarise this feedback and our decisions in **Section 5** of this statement.

## Our final decision

4.68 We are confirming our position at consultation to include some forms of sexually explicit content within the scope of the Guidance. However, we have made several changes to amend and clarify our position.

4.69 In response to feedback, we have clarified that the harm addressed is 'sexual violence' and this section has been restructured to emphasise our focus on this form of misogynistic abuse. We cover content depicting, invoking, encouraging or normalising sexual violence as this is a common, and widely available, type of violent content targeting women and girls.

4.70 We set out that sexual violence covers some forms of extreme pornography,[234] such as content depicting rape and injury and life-threatening content, which is illegal content. This can include realistic synthetic images, such as those generated by AI (for more information

[225] Response(s) to our February 2025 consultation: The Four Welsh Office of Police and Crime Commissioners, p.4.
[226] Response(s) to our February 2025 consultation: Collective Shout, p.4.
[227] Response(s) to our February 2025 consultation: CARE (Christian Action Research and Education), p.4.
[228] Response(s) to our February 2025 consultation: Baroness Bertin, p.1; Centre to End All Sexual Exploitation (CEASE), p.3; End Violence Against Women Coalition (EVAW), p.5; Welsh Women's Aid, p.1.
[229] Response(s) to our February 2025 consultation: CARE (Christian Action Research and Education), p.6; Centre to End All Sexual Exploitation (CEASE), p.2.
[230] Response(s) to our February 2025 consultation: Image Angel, p.1-2.
[231] Response(s) to our February 2025 consultation: Are, C., p.1.
[232] Response(s) to our February 2025 consultation: Hammy Media Ltd / xHamster, p.2.
[233] Response(s) to our February 2025 consultation: British and Irish Law, Education and Technology Association (BILETA), p.8; Essity, p.1-2.
[234] Extreme pornography has a specific definition in UK law. It refers to pornographic content that is grossly offensive or obscene and portrays certain acts such as rape, sexual violence, necrophilia and bestiality. For a more detailed overview see Section 7 of the Illegal Harms Register of Risks and Section 10 of the Illegal Content Judgements Guidance.

see the Illegal Content Judgements Guidance). It also includes illegal threats that are sexually violent.

4.71 Furthermore, sexual violence covers sexually violent pornography (including where it is AI-generated), which is legal content. It also covers content that is not sexually explicit but encourages or normalises sexual violence, for example, content which degrades survivors and victims of sexual violence.

4.72 This approach clarifies and refocuses the section to capture content that depicts, invokes, encourages or normalises sexual violence, including some types of pornography and extreme pornography. In line with feedback on the risk of pathologising sex workers by presenting pornography as inherently violent or harmful, our approach intentionally does not capture all forms of pornography. In taking this approach, we have also had regard to the right to freedom of expression under Article 10 ECHR, both in terms of adult users generating, uploading or sharing legal pornographic content and adult users being able to access such content.

4.73 Furthermore, there is not a consensus in the research that adults consuming non-violent pornography are harmed by it.[235] However, there is clear evidence of significant harm from content and activity which is sexually violent.[236] As noted in paragraph 4.60 in this statement, service providers also have duties to ensure all children must be prevented from encountering pornographic content.

4.74 We have decided not to create a standalone section on pornography. It is our view that the ways in which sexual violence is leveraged online in pornographic content is deeply intertwined with violence and abuse, and it therefore sits best within the framing of misogynistic abuse and sexual violence.

4.75 We have decided not to focus on step incest and role-play (where it is not explicitly sexually violent). While we recognise that this would align with offline standards, we do not have any role in classifying pornographic content that is not illegal – this is a matter for the BBFC where it falls within their remit and any future changes to the law are a matter for Parliament. All pornographic content is primary priority content harmful to children under the Act, and therefore providers of user-to-user services, including many online

[235] This refers to the contested nature of existing research and the methodological issues (for further information on methodological issues please see the Government Equalities Office Literature review) in researching the impact of pornography on adults. These methodological challenges include variation in what is being measured—such as sexual scripts, attitudes towards women and girls, or sexual aggression—and the diversity of content types, ranging from non-violent to violent pornography. The evidence around the impact of *any* type of pornography use was contested. Stakeholders referenced several pieces of work, a recent meta-analysis which found no link between sexual aggression and non-violent pornography, the Government Equalities Office Literature review which found *"substantial evidence of an association between the use of pornography and harmful sexual attitudes and behaviours towards women"* and Baroness Bertin's review into the Challenge of Regulating Online Pornography which further highlighted the influence of legal but harmful pornographic content.

[236] 'Sexually violent content' is more consistently linked to harm despite the methodological limitations outlined above. The Government Equalities Office literature review (2020) found stronger associations between violent pornography and harmful sexual attitudes and behaviours, particularly those that support violence against women and girls. Baroness Bertin's review (2025) provides further detail on the impact of violent and misogynistic pornography. Baroness Bertin's review (2025) finds that "there is clear evidence that pornography, especially that which promotes violent and misogynistic ideals, plays a part in influencing sexual behaviours and attitudes towards women and girls".

pornography services, have duties to use highly effective age assurance to prevent children from accessing it.

4.76 As discussed in the previous section, misogynistic abuse and sexual violence includes both illegal content and content harmful to children. Given this, we have taken care to ensure the recommended good practice steps for such content are proportionate, in particular with regard to freedom of expression. Further details can be found under each action in **Section 5,** and in the rights assessment (**Annex A3**) of this statement.

4.77 We have made several changes to our Guidance to incorporate additional evidence provided by respondents about how sexual violence manifests.

4.78 In line with our overall approach set out in paragraph 4.20 in this statement, we draw on quantitative evidence to highlight that sexual violence disproportionately targets women and online depictions of sexual violence are a manifestation, and reinforcement, of existing patterns of offline violence.

4.79 We have added relevant evidence related to sexual violence, including new evidence on the role of recommender systems in promoting pornographic content depicting sexual violence and how GenAI chatbots can normalise sexual violence through harmful sexual stereotypes associated with 'AI girlfriends' and 'AI boyfriends'.[237] In line with our broader approach to **Chapter 2** of the Guidance, we have added examples of which actions and good practice steps are most relevant to address sexual violence in paragraph 2.37 in the Guidance, including good practice steps specific to pornography services and other services that allow sexually explicit content.

# Pile-ons and coordinated harassment

## What we proposed

4.80 At consultation we used the term 'pile-ons and online harassment' to describe behaviours where many users target an individual victim or group of victims with abusive, hateful or threatening content, often repetitively or at scale.

4.81 We considered pile-ons and online harassment to include both illegal content such as illegal threats and harassment, and abuse and hate content harmful to children. We further explained that in the context of gender-based harms, such behaviours are often misogynistic, involving sexualisation, threats, descriptions of rape and the sharing of deepfake intimate image abuse content.

4.82 We also set out evidence of the disproportionate effect that content and activity related to pile-ons and online harassment have on women and girls from marginalised groups, as well as the risks to women and girls in public life, such as journalists, celebrities, politicians and influencers. In addition, we explained how this harm area can overlap with other online gender-based harms, such as intimate image abuse.

4.83 Further, we set out that pile-ons and online harassment involve a group of perpetrators carrying out repetitive or widescale abuse, and that this can be coordinated on dedicated sites. We also set out the impact of pile-ons and online harassment, highlighting for

[237] The Act applies to certain types of GenAI content, chatbots and services. See Ofcom's open letter to online service providers which outlines how the UK's Online Safety Act will apply to Generative AI and chatbots.

example how women in public life, such as journalists, are threatened, discredited and demeaned.

## Summary of stakeholder responses

4.84 We received feedback from several stakeholders who supported our inclusion of content and activity related to pile-ons and online harassment in the draft guidance.[238] One stakeholder noted how abuse and intimidation are leveraged against women in public life.[239] Some stakeholders also provided evidence on the impact of pile-ons on women and girls outside of public life, noting it can have a "systemic silencing"[240] effect or chilling effect, discouraging women from participating in politics due to fear of gendered disinformation".[241]

4.85 We also received feedback that women in public life are disproportionately affected by pile-ons and online harassment, but outside of public life both men and women face online harassment. One stakeholder noted that women in public life face unique risks,[242] while another stakeholder highlighted that it is not only women in public life targeted as "women are at risk of pile-ons simply by having an online presence".[243] Internet Matters set out that their research shows "girls are significantly more likely than boys to experience online harassment".[244] However, other stakeholders provided evidence that in some circumstances men are more likely than women to experience harassment.[245]

4.86 We received feedback from stakeholders on the tactics deployed by perpetrators of pile-ons and online harassment, including on the use of deepfakes to target women in public life,[246] with one stakeholder explaining deepfake intimate image abuse frequently forms part of pile-ons on women in public life, especially those involved in the entertainment industry.[247]

4.87 We also received feedback from stakeholders calling for us to include doxing in this harm area.[248] One industry stakeholder noted that from a technology perspective, pile ons are understood as coordinated mass posting and that the Guidance should acknowledge that not all mass posting is intended to be harmful or constitutes harassment. They said that activists could use mass posting to raise awareness about issues.[249]

4.88 One stakeholder also recommended that we include specific good practice steps for women in public life, for example that service providers engage with women politicians and provide

[238] Response(s) to our February 2025 consultation: Barker, K., p.5; Centre for Protecting Women Online, p.8-9; The Jo Cox Foundation, p.1.
[239] Response(s) to our February 2025 consultation: The Jo Cox Foundation, p.1.
[240] Response(s) to our February 2025 consultation: Institute for Strategic Dialogue (ISD), p.2.
[241] Response(s) to our February 2025 consultation: Moonshot, p.2.
[242] Response(s) to our February 2025 consultation: Institute for Strategic Dialogue (ISD), p.2.
[243] Response(s) to our February 2025 consultation: Centre for Protecting Women Online, p.9.
[244] Response(s) to our February 2025 consultation: Internet Matters, p.5.
[245] Response(s) to our February 2025 consultation: Evans, M.I., p.1; Moxon, S.P., p.1; Parity, p.3; [✂]; [✂].
[246] Response(s) to our February 2025 consultation: The Jo Cox Foundation, p.1. Ofcom Stakeholder Roundtable, Belfast, 8 May 2025.
[247] Response(s) to our February 2025 consultation: Crest Advisory, p.4.
[248] Response(s) to our February 2025 consultation: The Cyber Helpline, p.2; Mayor of London, p.7; Name Withheld 3, p.1; Welsh Women's Aid, p.3.
[249] Response(s) to our February 2025 consultation: Meta Platforms Inc, p.3.

routes for politicians to report abuse online.[250] We explain our response to these suggestions in **Section 5** in this statement.

## Our final decision

4.89 We are broadly confirming the scope of this harm area as set out at consultation. However, we have made some changes to the framing and terminology in line with stakeholder feedback.

4.90 We have clarified that the harm addressed is 'pile-ons and coordinated harassment'. This reflects more clearly the focus of this key harm area on the particular dynamic of a group of perpetrators targeting an individual woman or girl, or a small group of women and girls.

4.91 In line with our decision set out in paragraph 4.15 in this statement, we explain that pile-ons and coordinated harassment covers certain types of illegal content and activity (harassment, threats and abuse[251] and hate[252]) and content harmful to children (abuse and hate content[253] and violent content[254]).

4.92 We note that critical or potentially offensive speech and expression is protected by human rights law, and is vital to maintaining a free and democratic society.[255] For example, people have the right to criticise women politicians or other women in public life because they disagree with their political actions or views, or their policies, and may do so in a way that shocks or offends. However, we also note the right to freedom of expression is not absolute. Expression that promotes or justifies violence, hatred, xenophobia or another form of intolerance is not normally protected.[256] Illegal harassment, threats or abuse impact on other people's rights, and Parliament has determined that these offences give rise to priority illegal content under the Act.

4.93 As with misogynistic abuse and sexual violence above, we have made these changes to clarify that the scope is not intended to capture broader forms of content that are not illegal or harmful to children under the Act. This is to ensure that service providers following the Guidance are taking action on content and activity in scope of the Act, mitigating the risk of undue restriction on the right to freedom of expression (for example, by way of over-moderation of content).

4.94 We have reframed this harm area to focus primarily on women in public life, and the chilling effect this has on women and girls' participation more broadly. As noted in

---

[250] Response(s) to our February 2025 consultation: The Jo Cox Foundation, p.2.
[251] For a more detailed overview see Section 4 of the Illegal Harms Register of Risks and Section 3 of the Illegal Content Judgements Guidance.
[252] For a more detailed overview see Section 3 of the Illegal Harms Register of Risks and Section 3 of the Illegal Content Judgements Guidance.
[253] For a more detailed overview see Section 5 of the Children's Register of Risks and Section 6 of the Guidance on Content Harmful to Children.
[254] For a more detailed overview see Section 7 of the Children's Register of Risks and Section 8 of the Guidance on Content Harmful to Children.
[255] See for example Handyside v UK: "Freedom of expression constitutes one of the essential foundations of such a [democratic] society, one of the basic conditions for its progress and for the development of every man. …. it is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no 'democratic society'".
[256] Perinçek v. Switzerland [GC], 2015, § 230; Zemmour v. France, 2022, § 49; European Court of Human Rights, Key Theme – Article 10 Hate Speech. [accessed 10 November 2025].

paragraph 2.41-2.45 in the Guidance, the evidence shows that this harm disproportionately affects women in public life, for example journalists, politicians, influencers and athletes, as well as women and girls who end up in the public eye for other reasons.

4.95 In line with the position set out on scope in paragraph 3.18 in this statement, we have made changes to ensure the good practice steps for pile-ons and coordinated harassment are proportionate and to explain how these can be taken. Further details about our approach to applying the good practice steps to pile-ons and coordinated harassment can be found under each action in **Section 5** and in the rights assessment (**Annex A3**), in this statement.

4.96 Men and boys can also experience pile-ons and coordinated harassment and we have noted this in the Guidance.[257] In line with our position in paragraph 3.46 in this statement, we would expect the good practice steps to address pile-ons and coordinated harassment we have outlined in the Guidance to support anyone at risk of experiencing a pile-on.

4.97 We have made several changes to our Guidance to incorporate additional evidence, including evidence provided by stakeholders, about how pile-ons and coordinated harassment manifest.

4.98 In line with our overall approach set out in paragraph 4.20 in this statement, we draw on quantitative and qualitative evidence to highlight the disproportionate and distinct effect that pile-ons and coordinated harassment have on women in public life. We also recognise that pile-ons and coordinated harassment can be perpetrated against men and boys and can have a chilling effect on women and girls more broadly.

4.99 In paragraphs 2.43-2.45 in the Guidance, we have added evidence on the heighted risk of pile-ons and coordinated harassment experienced by women in public life, including to reflect Ofcom's own research on women politicians.[258] We also recognise the impact on women in public life beyond politics, including on women in sport and women journalists. In paragraph 2.46 in the Guidance, we have reflected the evidence on the chilling effect pile-ons and coordinated harassment targeted at women in public life can have on women and girls' participation more broadly.

4.100 We have also added evidence on perpetrator tactics and behaviour in paragraphs 2.47-2.48 in the Guidance. We recognise that perpetrators can use doxing to target an individual as part of a pile-on. We have also expanded our explanation in paragraph 2.49 in the Guidance to consider how particular functionalities and business models can contribute to pile-ons and coordinated harassment. In paragraph 2.48 in the Guidance, we set out the overlaps between pile-ons and intimate image abuse, including perpetrators targeting women in public life with deepfake intimate image abuse. In line with our broader approach to **Chapter 2**, we have added examples of which good practice steps and actions are most relevant to pile-ons and coordinated harassment in paragraph 2.50 in the Guidance.

[257] Ofcom, 2025. Online hate and abuse in sport: a report by Ofcom in partnership with Kick it Out.
[258] Ofcom, 2025. Experiences of online hate and abuse among women in politics.

# Stalking and coercive control

## What we proposed

4.101 At consultation we used the term 'online domestic abuse' to describe illegal content that amounts to controlling or coercive behaviour (which can include stalking and harassment). We explained that this harm occurs in the context of an intimate relationship.

4.102 In **Chapter 2** of the draft guidance, we explained how online domestic abuse can overlap with other forms of online gender-based harms including intimate image abuse and harassment. We also considered how online domestic abuse can overlap with harms such as human trafficking and sexual exploitation and honour-based abuse. We set out that controlling or coercive behaviour is heavily under-reported, to both services and the police.

4.103 Further, we set out a range of behaviours which can be perpetrated as part of a pattern of online domestic abuse. We explained that controlling or coercive behaviour can be especially difficult for service providers to identify, and emphasised the importance of providers engaging with relevant support services to understand this harm area

## Summary of stakeholder responses

4.104 We received support from stakeholders for the inclusion of domestic abuse as a key harm area.[259] Stakeholders echoed our proposals, highlighting the challenges for service providers in identifying harms such as domestic abuse. Two stakeholders set out that services are not always aware of relevant offline context, including relationships between users.[260] Several stakeholders also raised concerns that domestic abuse is not adequately covered by services' user reporting processes (see Action 8 in this statement).

4.105 We received a significant amount of feedback on stalking. Stakeholders called for stalking to be included as a standalone key harm area[261] and expressed concerns that "the lack of specific reference to cyberstalking in the guidance deprioritises this harm type".[262] Suzy Lamplugh Trust defined stalking as "a pattern of fixated and obsessive behaviour which is repeated, persistent, intrusive and causes fear of violence or engenders alarm and distress in the victim"[263] and noted that "Stalking is a unique and highly complex crime".[264] Other stakeholders also provided feedback and evidence about the significant and distinct harm caused by stalking. Several stakeholders called for us to recognise that stalking can occur outside of intimate relationships, domestic abuse and cases of coercive control.[265] Two respondents provided evidence that a significant number of survivors and victims of

[259] Response(s) to our February 2025 consultation: Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.4; [✂]; Refuge, p.1; Women's Aid Federation of England, p.1.
[260] Response(s) to our February 2025 consultation: LinkedIn, p.2; [✂].
[261] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (EVAW), p.2; Refuge, p.3; Suzy Lamplugh, p.2.
[262] Response(s) to our February 2025 consultation: Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.5.
[263] Response(s) to our February 2025 consultation: Suzy Lamplugh, p.1.
[264] Response(s) to our February 2025 consultation: Suzy Lamplugh, p.1.
[265] Response(s) to our February 2025 consultation: Association of Police and Crime Commissioners, p.1; The four Welsh Office of Police and Crime Commissioners, p.2; [✂]; Suzy Lamplugh, p.1. Ofcom Stakeholder Roundtable, Cardiff, 1 May 2025.

stalking are stalked by someone they did not know.[266] The Scottish Government suggested amending this key harm area to 'domestic abuse and stalking'.[267]

4.106 Some stakeholders noted that individual incidents which may not meet the threshold of 'illegality' could still contribute to a pattern of stalking or coercive control, or that individual instances can culminate in greater harm.[268] For example, two stakeholders gave the example of fake accounts which can be used to target survivors and victims of domestic abuse.[269] Another stakeholder expressed concern that "incidents of abuse are frequently viewed in isolation which risk mis-categorisation, mis-recording, minimisation and ultimately inaction".[270] Other stakeholders noted the importance of acknowledging that stalking and coercive control are patterns of repeated behaviour or ongoing actions.[271]

4.107 We received feedback on the terminology 'online domestic abuse'. One stakeholder argued the term "fails to acknowledge the comorbidity of online and offline harms".[272] Stakeholders called for this category of harm to be named technology-facilitated abuse[273] or tech-facilitated gender-based violence,[274] with one stakeholder explaining that "this terminology [is] more widely recognised".[275]

4.108 We also received stakeholder feedback around our decision to refer to controlling or coercive behaviour in the context of an intimate relationship. Two stakeholders argued that the term 'intimate' may detract from abuse perpetrated outside of intimate partner relationships.[276] Another stakeholder set out that perpetrators of domestic abuse may recruit others, including "family members, friends or associates, or people they meet online", to abuse the survivor and victim.[277] Further, several stakeholders expressed concerns that our proposals did not address children's, and specifically girls', experiences of domestic abuse.[278] One stakeholder set out that children of survivors and victims can also be affected by domestic abuse[279] and the NSPCC set out that domestic abuse "within intimate relationships can and does happen to girls".[280]

---

[266] Response(s) to our February 2025 consultation: Scottish Government, p.2; Suzy Lamplugh, p.1.
[267] Response(s) to our February 2025 consultation: Scottish Government, p.2.
[268] Response(s) to our February 2025 consultation: Children First, p.4; Mayor of London, p.5.
[269] Response(s) to our February 2025 consultation: Mayor of London, p.6; University of Portsmouth, p.2.
[270] Response(s) to our February 2025 consultation: Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.5.
[271] Response(s) to our February 2025 consultation: Children First, p.4; End Violence Against Women Coalition (EVAW), p.2.
[272] Response(s) to our February 2025 consultation: The Cyber Helpline, p.2.
[273] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (EVAW) Annex 2, p.5; Gender + Tech Research Lab Department of Computer Science, p.1; Women's Aid Federation of England, p.1.
[274] Response(s) to our February 2025 consultation: The Young Women's Movement, p.3.
[275] Response(s) to our February 2025 consultation: Gender + Tech Research Lab Department of Computer Science, p.1.
[276] Response(s) to our February 2025 consultation: The Cyber Helpline, p.2; Gender + Tech Research Lab Department of Computer Science, p.2.
[277] Response(s) to our February 2025 consultation: Centre for Protecting Women Online, p.10.
[278] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (EVAW), p.3; Plan International UK, p.5-6.
[279] Response(s) to our February 2025 consultation: Children First, p.4. Ofcom / Refuge's Survivor Panel, 10 June 2025.
[280] Response(s) to our February 2025 consultation: NSPCC, p.6.

4.109 A small number of stakeholders recommended that we include financial abuse[281] or economic abuse[282] within this harm area. Other stakeholders recommended we include abuse perpetrated through device-based technology.[283] The four Welsh Office of Police and Crime Commissioners called for more inclusion of honour-based abuse.[284]

## Our final decision

4.110 We are confirming our position at consultation to focus on coercive control. We have made several changes to the section on domestic abuse and have expanded this key harm area to cover stalking.

4.111 We focus on a single perpetrator (or very small number of perpetrators) targeting a single survivor and victim, in contrast to pile-ons and coordinated harassment. Therefore, we have chosen to keep stalking and coercive control within the same harm area, rather than as two standalone areas, to draw out the overlapping dynamics and perpetrator tactics involved in both stalking and coercive control.

4.112 However, we have included separate subsections on 'stalking' and 'coercive control'. This is to explicitly recognise the offence of stalking, and to ensure we sufficiently differentiate the two harms.

4.113 In line with these changes, we have renamed this harm area from 'online domestic abuse' to 'stalking and coercive control'. The change also aims to reflect that coercive control can occur outside of domestic contexts and recognise overlaps between online and offline abuse.

4.114 In line with our decision, as set out in paragraph 4.15 in this statement, stalking and coercive control covers two types of illegal content and activity (stalking[285] and controlling or coercive behaviour[286]) and we set out clear definitions for both types and signpost to the Illegal Content Judgements Guidance and the Illegal Harms Register of Risks.

4.115 We have made several changes to our Guidance to incorporate additional evidence, including evidence provided by respondents about how stalking and coercive control manifest.

4.116 In line with our overall approach, set out in paragraph 4.20 in this statement, we draw on quantitative evidence to highlight the disproportionate effect of stalking and coercive control on women.

4.117 In the stalking subsection, we have incorporated additional evidence, including evidence provided by stakeholders. This includes evidence about the impact and nature of this harm, distinct from coercive control. We note that stalking is a form of harassment characterised by a pattern of fixated, obsessive, unwanted and repeated behaviour which is intrusive. We recognise that perpetrators of stalking can include friends, family members, colleagues and strangers. In paragraphs 2.55-2.56 in the Guidance, we note the impact stalking has on

[281] Response(s) to our February 2025 consultation: The Cyber Helpline, p.2.
[282] Response(s) to our February 2025 consultation: Scottish Government, p.2.
[283] Response(s) to our February 2025 consultation: [✂]; Welsh Women's Aid, p.2-3.
[284] Response(s) to our February 2025 consultation: The four Welsh Office of Police and Crime Commissioners, p.2.
[285] For a more detailed overview see Section 4 of the Illegal Harms Register of Risks.
[286] For a more detailed overview see Section 5 of the Illegal Harms Register of Risks.

survivors and victims and acknowledge that stalking co-occurs across both online and offline spaces.

4.118 We have also added additional evidence on coercive control, recognising it as the repeated or continuous perpetration of behaviour that is controlling or coercive in paragraph 2.60 in the Guidance. We have also removed our reference to intimate relationships and set out that coercive control can be perpetrated in the context of an intimate or family relationship. We also recognise that perpetrators may target the children of survivors and victims. We have also set out that coercive control that is perpetrated online may overlap with other forms of abuse, such as physical, financial, and device-based abuse in paragraph 2.61 in the Guidance.[287] In paragraph 2.63 in the Guidance, we acknowledge that business profiles run by survivors and victims can be targeted by perpetrators of abuse.

4.119 We recognise the challenges for service providers in identifying these behaviours but also emphasise the risks that stalking and coercive control present for offline escalation. We have added evidence in paragraph 2.57 in the Guidance on the range of behaviours that may be perpetrated as part of stalking, in line with evidence provided by respondents. In paragraphs 2.59 and 2.66 in the Guidance highlight relevant good practice steps and actions from the Guidance, such as enabling the reporting of offline behaviour and the importance of providers working with specialist services to support survivors and victims.

# Image-based sexual abuse

## What we proposed

4.120 At consultation we used the term 'image-based sexual abuse' to describe this category of content and explained that we considered it to cover illegal content that amounts to either intimate image abuse or cyberflashing. We recognised that while intimate images are often sexually explicit, they can include intimate scenarios based on specific cultural and religious contexts.

4.121 We explained the profound negative impact intimate image abuse has on survivors and victims, including the distinct impact on sex workers. We also set out how intimate image abuse can overlap with other online gender-based harms, including 'pile-ons and online harassment' and 'online misogyny'.

4.122 Further, we explained what cyberflashing is and provided evidence about the negative impacts of this harm on survivors and victims, and the higher risk faced by women in minority ethnic groups and LGBTQ+ groups.

4.123 We set out that intimate image abuse can be perpetrated as part of a pattern of controlling or coercive behaviour or as part of 'collector culture'. We provided evidence on how re-shares cause re-victimisation and re-traumatisation for survivors and victims. We also covered the growing risk of deepfake intimate image abuse, including how 'nudification' apps and search engines make it easier to access this illegal content.

[287] We do not go into detail about the impact of device-based abuse given our powers under the Act relate to user-to-user and search services. For further information, see Section 3 in this statement.

## Summary of stakeholder responses

4.124 Broadly, stakeholders were supportive of the focus on intimate image abuse and cyberflashing in the draft guidance.[288] Some stakeholders called for us to strengthen or clarify specific types of intimate image abuse or overlaps with other harms. For example, two stakeholders noted the overlaps between honour-based abuse and image-based sexual abuse.[289] Another two stakeholders noted the growing impact of deepfake intimate image abuse, in particular on women in public life.[290]

4.125 Some stakeholders argued this harm area should include sextortion.[291] Many stakeholders noted that sextortion disproportionately affects men.[292]

4.126 Other stakeholders recommended expanding this harm area to include other harms. End Violence Against Women Coalition (EVAW) recommended the inclusion of 'semen images'.[293] One stakeholder said "while we find the categorisation of image-based sexual abuse to be comprehensive, there are other forms of content that should be highlighted as part of this category" and also said they had "identified an increasing trend in individuals uploading videos of themselves committing sexual acts to printed out pictures or videos of individuals".[294]

4.127 Some stakeholders supported Ofcom's recognition of intimate scenarios based on specific cultural and religious contexts.[295] One stakeholder called for Ofcom to "emphasise that cultural differences and attitudes towards women's bodies will have an impact on what images are considered intimate"[296] and another stakeholder emphasised that "Intimacy is contextual".[297] A different stakeholder raised the exploitation of avatars depicting non-consensual acts as a new form of abuse, noting the lack of legal clarity around this as the avatars are not photorealistic but represent individuals.[298] The Free Speech Union expressed concerns about recognising contextual understandings of intimacy and its potential impact on freedom of expression, arguing that "the same photograph could be lawful or unlawful depending on the ethnicity, religion, or gender identity of the subject".[299]

4.128 We received a range of stakeholder feedback on deepfake and 'nudification' tools and their connection to intimate image abuse.[300] One stakeholder told us it had identified a "vast landscape of tools, website[s], accounts, and forums dedicated to creating and sharing non-

---

[288] Response(s) to our February 2025 consultation: Age Check Certification Scheme, p.1; Centre for Protecting Women Online, p.10-11; Institute of Strategic Dialogue (ISD), p.8; [✂]; South West Grid for Learning (SWGfL), p.2.
[289] Response(s) to our February 2025 consultation: Mayor of London, p.6; Name Withheld 3, p.2.
[290] Response(s) to our February 2025 consultation: [✂]; The Jo Cox Foundation, p.1.
[291] Response(s) to our February 2025 consultation: Centre for Protecting Women Online, p.9; Mayor of London, p.8; Scottish Government, p.3.
[292] Response(s) to our February 2025 consultation: The Cyber Helpline, p.2; Evans, M.I., p.9; The four Welsh Office of Police and Crime Commissioners, p.7; Moxon, S.P., p.1; Parity, p.3; [✂]; [✂].
[293] 'Semen images' refer to images where semen is depicted on top of a non-intimate image. Response(s) to our February 2025 consultation: End Violence Against Women Coalition (EVAW), p.3.
[294] Response(s) to our February 2025 consultation: Moonshot, p.4
[295] Response(s) to our February 2025 consultation: Scottish Government, p.4.
[296] Response(s) to our February 2025 consultation: Centre for Protecting Women Online, p.12.
[297] Response(s) to our February 2025 consultation: Chayn, p.6.
[298] Response(s) to our February 2025 consultation: Ending Violence Against Women (EVAW) Annex 1, p.21.
[299] Response(s) to our February 2025 consultation: Free Speech Union, p.11.
[300] Response(s) to our February 2025 consultation: [✂]; End Violence Against Women Coalition (EVAW), p.4; Institute for Strategic Dialogue (ISD), p.8; Internet Matters, p.8; Name Withheld 3, p.1.

consensual intimate images."[301] Another stakeholder called for Ofcom to address how algorithms promote 'nudification' apps[302] and one civil society organisation noted that some of these 'nudification' tools only work on women.[303]

4.129 Further, one stakeholder set out that "Women and marginalised gendered – particularly sex workers – face disproportionate risk of image-based abuse".[304] Another stakeholder noted that in the context of some deepfake intimate images the "image and likeness of a sex worker has been unconsensually taken for the purposes of victimising another woman."[305]

## Our final decision

4.130 We are confirming our position at consultation to focus on intimate image abuse and cyberflashing. However, we have also extended the section to include self-generated indecent imagery. We have clarified the scope excludes content that does not meet the criminal threshold for these harms.

4.131 In response to stakeholder feedback, we have added in a subsection on self-generated indecent imagery. We explain our reasoning for adding this section and our approach to self-generated indecent imagery in paragraphs 4.148-4.150 in this statement.

4.132 In line with our overall decision, as set out in paragraph 4.15 in this statement, 'image-based sexual abuse' covers three types of illegal content and activity (intimate image abuse,[306] self-generated indecent imagery,[307] and cyberflashing[308]). We set out clear definitions for all three types of illegal content and signpost to the Illegal Content Judgements Guidance and the Illegal Harms Register of Risks.

4.133 We have decided not to include within the scope of this harm area the taking, creating, sharing, or threatening to share of images understood as 'intimate' in specific cultural and religious contexts, 'semen images' or images depicting non-photorealistic images and videos of adults. These images can cause significant harm, and we have, therefore, acknowledged that these kinds of images can be a form of misogynistic abuse and sexual violence in paragraph 2.27 in the Guidance, under the 'misogynistic abuse and sexual violence' harm area. We consider that these kinds of images are better covered under this harm area than under intimate image abuse, as we are focusing specifically on illegal content and activity that amounts to intimate image abuse.[309] These images can amount to illegal content where they meet, for example, the legal definition of harassment.

---

[301] Response(s) to our February 2025 consultation: Moonshot, p.3.
[302] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (EVAW) Annex 2, p.5.
[303] Response(s) to our February 2025 consultation: Internet Matters, p.8.
[304] Response(s) to our February 2025 consultation: Image Angel, p.9.
[305] Response(s) to our February 2025 consultation: Crest Advisory, p.4.
[306] For a more detailed overview see Section 6 of the Illegal Harms Register of Risks and Section 10 of the Illegal Content Judgements Guidance.
[307] For a more detailed overview see Section 2B of the Illegal Harms Register of Risks and Section 4 of the Illegal Content Judgements Guidance.
[308] For a more detailed overview see Section 19 of the Illegal Harms Register of Risks and Section 16 of the Illegal Content Judgements Guidance.
[309] Most commonly, an 'intimate image' is a photograph or video where the person or people are depicted engaging in, participating in, or are present during a sexual act and/or where their genitals, buttocks or breasts are exposed or covered only with underwear. An 'intimate image' also covers a photograph or video where the person or people are depicted in an act of, or carrying out personal care associated with, urination, defecation or genital or anal discharge. For more information see sections 66B – 66H of the Sexual Offences Act 2003.

4.134 We have made several changes to the Guidance to incorporate feedback provided by respondents about how intimate image abuse manifests.

4.135 In line with our overall approach, set out in paragraph 4.20 in this statement, we draw on quantitative evidence to set out the disproportionate effect that intimate image abuse and cyberflashing have on women. We also recognise sextortion as a form of intimate image abuse and note that it disproportionately affects men.

4.136 We have added additional detail about the business models and ecosystem of 'nudification' apps, websites and forums in paragraph 2.79 in the Guidance. We have given examples of which good practice steps from the Guidance would be especially relevant for service providers in tackling deepfake intimate image abuse. We have also added a specific acknowledgment in paragraph 2.48 in the Guidance of the role of intimate image abuse (and specifically deepfake intimate image abuse) in pile-ons and coordinated harassment targeting women in public life.

### Legislation on online gender-based harms

In the UK, several legislative changes have been announced since the UK Parliament passed the Act in 2023. This is part of the Government's commitment to halving violence against women and girls in a decade.[310] We will continue to pay close attention to these changes and where necessary we will update our Codes and Guidance to reflect them. Recent changes include:

**Intimate image abuse**

- Intimate image abuse has been made a 'priority offence' under the Online Safety Act.[311]
- Creating, and requesting the creation of, deepfake intimate images without the consent of the individual depicted has been criminalised.[312]
- The Home Office and Ministry of Justice are in the process of criminalising the taking of intimate images without consent and the installation of equipment for this purpose.[313]

**Cyberflashing**

- The Department for Science, Innovation and Technology has announced that cyberflashing will be made a 'priority offence' under the Act.[314]

**Sexual violence**

- The Ministry of Justice has announced that the depiction of strangulation in pornography will be criminalised.[315]

---

[310] Home Office and Jess Phillips MP, 2025. Government pledges to protect more women from violence. [accessed 19 November 2025].
[311] Department for Science, Innovation and Technology, Home Office, Ministry of Justice, Peter Kyle MP, Jess Philips MP, and Alex Davies-Jones MP, 2024. Crackdown on intimate image abuse as government strengthens online safety laws. [accessed 14 November 2025].
[312] See sections 66E – 66H of the Sexual Offences Act 2003. The provisions have not yet been commenced.
[313] Ministry of Justice and Alex Davies-Jones MP, 2025. Government cracks down on explicit deepfakes. [accessed 13 October 2025].
[314] Department for Science, Innovation and Technology and Liz Kendall MP, 2025. Tech firms to prevent unwanted nudes under tougher laws to protect women and girls online. [accessed 13 October 2025].
[315] Ministry of Justice and Alex Davies-Jones MP, 2025. Strangulation in pornography to be made illegal. [accessed 13 October 2025].

# Other harms

## What we proposed

4.137 At consultation, we made clear that our four key harm areas do not cover all types of content and activity that affect women and girls online. We specifically recognised illegal harms such as child sexual exploitation and abuse (CSEA) and modern slavery and human trafficking, as well as eating disorder content and bullying content harmful to children in the draft guidance.

4.138 We included information on those harms where they overlapped with the four key harm areas. For example, we recognised that techniques used for online domestic abuse may overlap with methods used for human trafficking and sexual exploitation. We also acknowledged the distinct risk of intimate image abuse faced by sex workers.

4.139 We included foundational steps related to the prevention of CSEA throughout the draft guidance.

## Summary of stakeholder responses

4.140 Many stakeholders raised concerns about our approach to CSEA.[316] For example, several stakeholders called for CSEA to be a standalone harm area in recognition of the disproportionate effect of this harm on girls.[317] Some stakeholders called specifically for grooming for the purposes of CSEA to be included as a standalone harm area.[318] The NSPCC argued that including CSEA as a harm area would allow the Guidance to include best practice targeted at CSEA.[319] Some other stakeholders highlighted the overlaps between CSEA and image-based sexual abuse.[320] The NSPCC called for the Guidance to "address non-consensual peer-to-peer image sharing as a distinct and separate risk to adult-perpetrated CSA"[321] and Internet Matters explained that the "dynamics, impact and types of harm associated with child-on-child abuse differ from adult offending".[322]

4.141 In addition, several stakeholders suggested the Guidance should address modern slavery and human trafficking[323] and sexual exploitation[324] more extensively. A stakeholder noted that "Digital technologies have created significant additional risks for women in the sex trade".[325] Stakeholders also identified links between sexual exploitation and the key harm areas set out in the draft guidance, including image-based sexual abuse.[326]

---

[316] Response(s) to our February 2025 consultation: Clean Up The Internet, p.2.
[317] Response(s) to our February 2025 consultation: Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.6; End Violence Against Women Coalition (EVAW) Annex 2, p.4; Lucy Faithfull Foundation, p.2; NSPCC, p.3-5; Plan International UK, p.6.
[318] Response(s) to our February 2025 consultation: Bolt Burdon Kemp LLP, p.2; Plan International UK, p.6; [✂].
[319] Response(s) to our February 2025 consultation: NSPCC, p.3.
[320] Response(s) to our February 2025 consultation: Internet Matters, p.7-9; NSPCC, p.4-5; Plan International UK, p.6-7.
[321] Response to our February 2025 consultation: NSPCC, p.24.
[322] Response to our February 2025 consultation: Internet Matters, p.10-11.
[323] Response(s) to our February 2025 consultation: Clean Up The Internet, p.2; Heriot-Watt University – University of Edinburgh, p.4; [✂]; Scottish Government, p.2.
[324] Response(s) to our February 2025 consultation: Centre to End All Sexual Exploitation (CEASE), p.4; [✂]; Tranchese, A., p.2.
[325] Response(s) to our February 2025 consultation: Tranchese, A., p.1.
[326] Response(s) to our February 2025 consultation: Centre to End All Sexual Exploitation, p.4; [✂].

4.142 We received feedback and evidence on the impact on women and girls from content harmful to children such as eating disorder and bullying content.[327] Some stakeholders called for us to include eating disorder content in the Guidance.[328] One stakeholder argued that young people who have experienced cyber-bullying are almost twice as likely to attempt suicide compared to those who have not.[329] Another stakeholder called for us to recognise that exposure to content that encourages self-harm, body dissatisfaction, disordered eating, and self-silencing shape gendered self-concepts and reinforce inequality.[330]

4.143 One stakeholder argued eating disorder content should be included in the Guidance as they are not convinced our illegal content and children's safety codes will significantly reduce the risk of harm.[331] Another stakeholder said that excluding these harms runs contrary to Parliament's intent that the Guidance should bring together all the measures that can tackle abuse which disproportionately affects women and girls online.[332]

4.144 We also received feedback from one stakeholder who suggested we embed, rather than highlight, the experiences of trans women and girls. They referenced a survey of trans girls and gender diverse children and found that almost half (48%) had experienced cyber bullying, 66% of which was directly due to their gender identity.[333]

## Our final decision

4.145 We are broadly confirming our approach to the harm areas we are focusing on in the Guidance and are not expanding our focus to CSEA or modern slavery and human trafficking. However, we have expanded the image-based sexual abuse harm area to cover self-generated indecent imagery.

4.146 CSEA is a top priority area of Ofcom's work on online safety. We have developed more Codes measures aimed at tackling CSEA than any other harm area and we are currently consulting on additional measures to strengthen restrictions on interactions with livestreams and recommending the use of proactive technologies to detect grooming and CSAM.[334]

4.147 We have a range of ongoing enforcement cases looking specifically at providers' compliance with duties for CSEA and we are prioritising a range of work on protecting children. For example, in July we announced the launch of an extensive monitoring and impact programme, primarily focused on the biggest services where children spend most time, including Facebook, Instagram, Roblox, Snap, TikTok and YouTube. This includes scrutinising the measures they are taking to reduce the risk of grooming on their services.

---

[327] Response(s) to our February 2025 consultation: Plan International UK, p.7; Welsh Government, p.2.
[328] Response(s) to our February 2025 consultation: Clean Up The Internet, p.1; NSPCC, p.2; Plan International UK, p.8; Welsh Government, p.2.
[329] Response(s) to our February 2025 consultation: Galop, p.3.
[330] Response(s) to our February 2025 consultation: Institute for Strategic Dialogue (ISD), p.5.
[331] Response(s) to our February 2025 consultation: Clean Up the Internet, p.1.
[332] Response(s) to our February 2025 consultation: NSPCC, p.2.
[333] Response(s) to our February 2025 consultation: NSPCC, p.7 (evidence referenced is Herrmann, L., Bindt, C., Hohmann, S. and Becker-Hebly, I., 2023. Social media use and experiences among transgender and gender diverse adolescents. Int J Transgender Health, 25(1)).
[334] For more information, see our Consultation: Online Safety - Additional Safety Measures which was published in June 2025.

4.148 Intimate image abuse and CSEA are distinct harms which have different impacts, different offending behaviours and are addressed by different legal frameworks. It is illegal to take, make, distribute, possess or publish any image of a child in a sexual or indecent context, whereas for an intimate image of an adult, it is illegal to take, create, share, or threaten to share the image without the consent of the person depicted. Establishing consent is crucial in preventing intimate image abuse and the focus of some of the good practice steps set out in the Guidance. Despite the distinct differences between intimate image abuse and CSEA, there are some similarities in how the harms manifest online, for example the risk of the non-consensual sharing of an image created by the individual depicted in it (including under coercion). Therefore, where the good practice steps set out in the Guidance are focused on creating friction points for image sharing, these may help address the risks associated with both harms.

4.149 In recognition of this, as noted in paragraph 4.130-4.131 in this statement, we have added a subsection on 'self-generated indecent imagery'[335] under the image-based sexual abuse harm area. This section sets out evidence on how the harm manifests, the impact on survivors and victims and the disproportionate effect on girls.[336] In line with our overall approach to **Chapter 2**, we have also added examples of which good practice steps are most relevant to self-generated indecent imagery.

4.150 As part of our changes to the case studies, we have removed the case studies on grooming and CSEA to focus on mitigations specifically covered by the Guidance. See paragraph in 5.22 in this statement for further information.

4.151 As set out in paragraphs 4.12-4.13 in this statement, we are confirming our position at consultation to use the key harm areas to describe common typologies of harm, not provide a comprehensive overview. While we acknowledge that many online harms are likely to have a gendered dynamic in terms of how they manifest, including modern slavery and human trafficking and eating disorder content harmful to children, we have focused the key harm areas on content and activity that represents, enables or reinforces misogyny and gender-based violence.

[335] We recognise the challenges associated with this terminology and how it may fail to capture the nature of the abuse suffered and unintentionally imply that a child is responsible for their own abuse. However, in the absence of a more appropriate and widely adopted alternative, we have chosen to use this wording to ensure clarity.

[336] We recognise that there is a growing trend of SGII being used as a method of financially motivated sexual extortion. Financially motivated sexual extortion disproportionately affects boys. For more information see Section 2 of the Illegal Harms Register of Risks.

# 5. Actions for services

## Introduction

5.1 In this section, we explain our decisions regarding the steps we have set out – both foundational and good practice – for service providers to follow in meeting the actions set out in the Guidance. This includes detailing what we proposed in our February 2025 consultation, the stakeholder feedback on the draft guidance, and our final decisions and reasoning. Specifically, we cover:

a) Topic 1: Overall approach: Safety-by-design and case studies
b) Topic 2: Taking responsibility (**Actions 1-3**)
c) Topic 3: Preventing harm (**Actions 4-6**)
d) Topic 4: Providing support (**Actions 7-9**)

5.2 We received detailed feedback on the actions. While we have carefully considered all feedback, the following sections summarise key issues raised by stakeholders and the decisions we have made in response. We have considered potential impacts on fundamental rights, including the rights to freedom of expression and privacy, as noted in stakeholder responses. We consider the recommendations set out will benefit the safety of women and girls,' as well as other groups affected by these harms. See our rights assessment (**Annex A3**) for further details.

5.3 Unless specified in this section, we have not made changes to our proposals suggested by stakeholders, for example to add further good practice steps. The reasoning for this varies depending on the feedback, but includes lack of evidence, proportionality concerns, exceeding the scope of the Guidance or Ofcom's remit, and overlap or duplicate with existing decisions.

5.4 Further, as explained in **Section 3** of this document, many stakeholders called on us to make various draft good practice steps foundational (e.g. include them within Codes of Practice). While we may include certain good practice steps in future iterations of our Codes, the consultation process for this Guidance is separate to us consulting on any future Codes. Given this, we have not included feedback from stakeholders calling for good practice to become foundational under each action. We have addressed this issue in the round in **Section 3.**

## Overall approach

### Safety-by-design

#### What we proposed

5.5 At consultation, we set out nine high level actions for providers to take to address online gender-based harms. Under each action, we included both foundational and good practice steps to showcase the actions providers could take. The nine actions are illustrated at **Figure 1.**

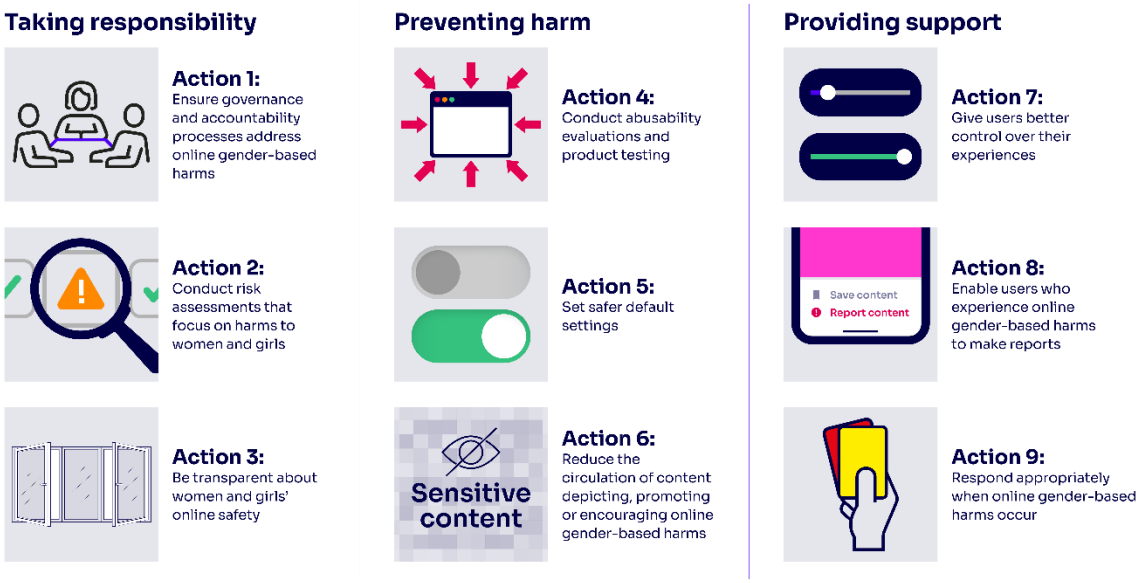


**Figure 1: Nine action areas in Chapters 3-5**

5.6 At consultation, we set out that these actions were intentionally high-level to ensure they were relevant for all providers. We also explained that the actions, taken together, represented a safety-by-design approach focused on prevention and on embedding the safety of women and girls throughout the operation and design of their services.

## Summary of stakeholder responses

5.7 Many stakeholders supported the nine actions.[337] For example, one stakeholder said the nine actions demonstrate "a meaningful commitment to prevent online harm against women and girls, ensure companies and providers are accountable, and support women and girls who may be affected."[338] Another noted the actions represent a "significant step forward in recognising that platform design and governance decisions shape the online experience."[339]

5.8 Several stakeholders raised concerns about many of the actions being exclusionary or discriminatory towards men and boys, and some emphasised the need for actions to be gender-neutral or extended to all users who are at risk of experiencing online gender-based harms. We summarise this feedback and our decisions on this issue in **Section 3** in this statement.

5.9 A small number of stakeholders expressed concern that the nine actions did not adequately capture the impact of business models,[340] or focused too heavily on safety work for

[337] Response(s) to our February 2025 consultation: Age Check Certification Scheme, p.1; Engendering Change, p.1; Refuge, p.2; Baroness Morgan of Cotes, p.1; Barker, K. p.7; Ofcom Advisory Committee for Scotland, p.2; Image Angel, p.3, Online Dating and Discovery Association (ODDA), p.2; [✂]; [✂]; The Cyber Helpline, p.3; Popa-Wyatt, M. p.1; 5Rights Foundation, p.4; Chayn, p.2.

[338] Response(s) to our February 2025 consultation: Belfast Area Domestic & Sexual Violence and Abuse Partnership, p.1.

[339] Response(s) to our February 2025 consultation: Institute for Strategic Dialogue (ISD), p.6.

[340] Response(s) to our February 2025 consultation: Clean Up the Internet, p.1; Domestic Abuse Commissioner for England and Victim's Commissioner for England and Wales, p.8-9.

survivors and victims, and/or not enough on prevention.[341] The Scottish Government suggested combining actions (e.g., Transparency and Governance).[342]

5.10 More generally, stakeholders including industry, civil society, and public sector supported the focus on a safety-by-design approach underpinning the nine actions.[343] Some stakeholders noted different models of safety-by-design, or related models such as privacy-by-design and equality-by-design, and called for clarity.[344] We also received feedback on alternative approaches to safety-by-design, for example, calls to prioritise a focus on the design of a product to eliminate or reduce risk of harm followed by introducing features and processes to mitigate risks of harm, and finally remediating.[345] A small number of stakeholders said the description of safety-by-design should be strengthened to emphasise "that safety by design requires platforms to eliminate risks at the outset rather than relying on mitigation."[346]

## Our final decision

5.11 We are confirming our approach at consultation and retaining the nine actions and the safety-by-design approach. We have made some minor changes to clarify our approach.

5.12 Based on feedback on the actions at a high level and on individual good practice, we consider the actions provide a helpful guide for services to take a safety-by-design approach that considers the safety of women and girls online.

5.13 We agree with respondents that a priority of safety-by-design should be designing out risks, as is addressed in **Actions 1, 2**, and **4**, and that this should be followed by introducing safety features and processes to prevent harm (**Actions 5 – 7**), as well as taking remedial action (**Action 8** and **9**). We consider our overall approach captures this dynamic, as well as the influence of business models over such decisions. We have amended the wording in **Chapter 1** to emphasise reducing risk at the outset as a priority. We also note that this can be done on new and existing features, and explore this across relevant Actions.

5.14 As explained in **Section 3**, while these actions focus on addressing content and activity that disproportionately affects women and girls, they are designed to take a preventative approach to harm and improve safety outcomes more generally across the service. This means, for example, that all default settings and user tools should be made available to all users of a service, even though they may have been developed specifically to address gender-based harms. In line with this approach, we have made changes to **Chapter 1** and

---

[341] Response(s) to our February 2025 consultation: Children First, p.6; Heriot Watt University – University of Edinburgh, p.1; South West Grid for Learning (SWGfL), p.8; Welsh Government, p.5.
[342] Response(s) to our February 2025 consultation: Scottish Government, p.4.
[343] Response(s) to our February 2025 consultation: NSPCC, p.8-9; The Young Women's Movement, p.5; Bumble, p.5; Gender + Tech Research Lab Department of Computer Science, p.2; British and Irish Law, Education, and Technology Association (BILETA), p.3, p.6; Baroness Morgan of Cotes, p.1; Refuge, p.2; [✂]; Flux Digital Policy, p.2; Mayor of London, p.2; Equality Now, p.4; 5Rights Foundation, p.4; Do-Ngoc, T., Carmel, E., p.1-2.
[344] Response(s) to our 2025 consultation: Ending Violence Against Women (EVAW), p.7; Equality Now, p.3; British and Irish Law, Education, and Technology Association (BILETA), p.7; The Young Women's Movement, p.5-6.
[345] Response(s) to our February 2025 consultation: Online Safety Act Network, p.1-2.
[346] Response(s) to our February 2025 consultation: Ending Violence Against Women (EVAW), p.7. CHAYN, p.2, made a similar argument.

**Chapters 3-5**. For example, we have renamed **Action 7** 'Supporting women and girls,' to 'Providing support'.

# Case studies

## What we proposed

5.15 At consultation, we used case studies to provide more detail about the practical application of good practice of examples or how to achieve a specific action. Some case studies focused on particular service types or specific harm areas. The structure of the case studies varied depending on the scenario and good practice.

## Summary of stakeholder responses

5.16 Some stakeholders were supportive of case studies, saying they provided useful information on good practice in specific contexts.[347] One academic noted "the guidance is well supported by real-world case studies demonstrating the achievability of the proposed measures."[348] Some stakeholders said the case study evidence was qualitative and anecdotal.[349]

5.17 Industry stakeholders emphasised the importance of addressing how case studies will or will not be appropriate and whether they are applicable for all services, for example due to size and functionalities.[350] Others raised concerns about the applicability of the Guidance for smaller services or different service types,[351] for example, the need to evaluate to see if they can be adapted for smaller or resource-limited services and different service types.[352]

5.18 We also received feedback that case studies, or the Guidance more generally, needed to focus more on different user needs and circumstances such as children,[353] men and boys,[354] and those with intersectional identities (including race, gender identity and sexuality).[355] This is further detailed from paragraph 3.37 in this statement.

5.19 Further, as noted at in **Section 3** in this statement, many stakeholders called for more information about how to apply good practice to a service and what proportionate implementation looks like, particularly with regard to privacy and freedom of expression. We also received feedback to include more evidence on unintended risks or negative consequences in case studies, as well as examples of poor practice.[356] Some stakeholders also called on Ofcom to simplify the Guidance and terminology and ensure it is easy to read and use.[357]

---

[347] Response(s) to February 2025 consultation: Popa-Wyatt, M., p.2; LinkedIn, p.3.
[348] Response(s) to February 2025 consultation: Barker, K., p.10.
[349] Response(s) to February 2025 consultation: [✂]; Parity, p.8; Evans, M.I., 4; [✂]; Moxon, S.P., p.3.
[350] Response(s) to February 2025 consultation: Bumble, p.7; ACT The App Association, p.3.
[351] Response(s) to February 2025 consultation: [✂]; Parity, p.9, Evans, M.I., p.4; [✂].
[352] Response(s) to February 2025 consultation: Popa-Wyatt, M., p.2.
[353] Response(s) to February 2025 consultation: NSPCC, p.1; Office for the Commissioner for Children in Northern Ireland (NICCY), p.4.
[354] Response(s) to February 2025 consultation: [✂]; Parity, p.8, Evans, M.I., p.4; [✂]; Moxon, S.P., p.5.
[355] Response(s) to February 2025 consultation: The Minderoo Centre for Technology and Democracy at the University of Cambridge, p.2; Galop, p.4-5; Commissioner for Children and Young People (NICCY), p.11.
[356] Response(s) to February 2025 consultation: Belfast Area Domestic & Sexual Violence and Abuse Partnership, p.2; Flux Digital Policy, p.3; British and Irish Law, Education, and Technology Association (BILETA), p.20-21.
[357] Response(s) to February 2025 consultation: Kira, B. Asser, Z. Ruiz, J, p.6-7; Scottish Government, p.1.

### Our final decision

5.20 **We have adjusted our approach to case studies to improve readability and impact.** To do this, we have organised each case study under three sub-headings: Scenario, Steps to take and Considerations.

a) **Scenario:** this sub-section sets out details of the kind of service, harm area and user group the case study focuses on. In light of stakeholder feedback on the need to consider these dynamics more fully, we have taken care across the case studies to cover a wider range of service types and user groups. We now include case studies on new service types (messaging, image sharing, video sharing and discussion forums), in addition to the service types in the draft case studies on social media, pornography, gaming, dating, and search services. We have also incorporated the experience of survivors, as well as children, including boys into the case studies**.**

b) **Steps to take**: this sub-section clarifies or adds further details on what the foundational step or good practice step would look like for a particular service and what outcomes it would seek to achieve. We have framed the case studies from the perspective of services rather than users to ensure the Guidance is more applicable to decision makers at services.

c) **Considerations:** this sub-section provides information for all case studies to further contextualise what good implementation looks like. This includes unintended consequences to avoid, impacts on rights such as privacy and freedom of expression to consider, limitations of good practice to be aware of, and points around relevance or efficacy for different types and sizes of providers.

5.21 These changes improve readability and accessibility more generally (see also further adaptations for accessibility in **Annex A1** of this statement). The specific changes we have made are discussed in detail for each action in the following subsections.

5.22 We have also replaced a number of foundational case studies in the draft guidance with case studies on good practice. We now explain these changes under each action in this statement. Broadly, this is to incorporate and focus on feedback from stakeholders on ways to expand or strengthen our proposals on good practice. This includes replacing case studies on grooming default settings and hash matching for CSAM, as well as on comment controls and governance processes, as these are covered by other parts of Online Safety regulation. We continue to prioritise our efforts to tackle CSEA. As noted in **Section 4,** we have opened enforcement programmes on hash matching for CSAM and are consulting on additional measures to protect children from abuse and exploitation.

# Action 1: Ensure governance and accountability processes address online gender-based harms

## Overall approach and foundational steps

### What we proposed

5.23 At consultation, we proposed that effective governance and accountability processes provide the foundation for service providers to identify, manage and review risks of gender-based harm. We included foundational steps on:

a) Board review
b) Accountable individual

c) Writing statements of responsibilities
d) Internal monitoring and assurance function
e) Monitoring trends
f) Codes of conduct
g) Terms of service and publicly available statement
h) Compliance training

## Summary of stakeholder feedback

5.24 We received general feedback in support of the objective of improving governance and accountability to support women and girls' safety online.[358] Some stakeholders noted that existing governance systems fail to adequately address gender-based harms, or that more robust regulation is needed to improve accountability.[359]

5.25 Two stakeholders emphasised that platform governance needs to go beyond trust and safety functions and be embedded across the organisation,[360] while others noted the importance of proactive governance.[361] Many stakeholders suggested clarity, emphasis or good practice for providers on fostering a diverse culture and workforce, particularly diverse and responsible leadership[362] or further explored accountability processes.[363]

5.26 Some stakeholders noted that governance processes must balance safety with robust protections on freedom of expression and privacy.[364] The ICO suggested that where relevant under **Action 1**, "the final guidance reminds services that, where processing of personal information is taking place, they must comply with data protection law requirements, particularly the data minimisation principle".[365]

5.27 We received limited feedback on the foundational steps, however we address feedback on terms of service at 5.40 in this statement.

## Our final decision

5.28 **We are confirming our position at consultation to include Action 1.** We have emphasised the importance of diverse workforces and fostering a culture of inclusion and accountability in the introduction to **Action 1**, to reflect their impact as examples of inclusivity.

5.29 **We are confirming our position to include the foundational steps set out in paragraph 5.23 in this statement.** We discuss changes to terms of service in paragraph 5.40 in this statement and otherwise have retained the draft foundational steps with minor changes to improve clarity or readability.

5.30 We have also added a foundational step relating to providers' duties concerning freedom of expression and privacy under sections 22 and 33 of the Act (see Legal Annex, Annex A2,

[358] Response(s) to our February 2025 consultation: British and Irish Law, Education and Technology Association (BILETA), p.3; Suzy Lamplugh Trust, p.2; The Cyber Helpline, p.3; South West Grid for Learning (SWGfL), p.6.
[359] Response(s) to our February 2025 consultation: The Cyber Helpline, p.3; University of York, p.4.
[360] Response(s) to our February 2025 consultation: Integrity Institute, Council on Technology & Social Cohesion, University of Southern California, Marshall School Neely Center, p.3; White Ribbon UK, p.2.
[361] Response(s) to our February 2025 consultation: Image Angel, p.11; White Ribbon UK, p.2.
[362] Response(s) to February 2025 consultation: White Ribbon UK, p.2; Refuge, p.10; [✂]; Scottish Government, p.3; Women's Aid Federation of England, p.14; Gender + Tech Research Lab Department of Computer Science, p. 8; The four Welsh Office of Police and Crime Commissioners, p.4; Barker, K., p.7.
[363] Response(s) to our February 2025 consultation: Kira, B. Asser, Z. and Ruiz, J., p. 4; Refuge Annex, p.5
[364] Response(s) to our February 2025 consultation: Free Speech Union, p.6; British and Irish Law, Education, and Technology Association (BILETA), p.3; Do-Ngoc, T. and Carmel, E., p.7.
[365] Response(s) to our February 2025 consultation: Information Commissioner's Office (ICO), p.4.

paragraphs A2.29-A2.32). This is to emphasise the responsibility on providers as set out in the Act. We agree with stakeholders that it is core to good governance that providers effectively consider these rights.

5.31 We have not included a specific reference to the ICO guidelines in **Action 1** as the steps covered do not involve specific recommendations requiring processing the processing of personal data. However, we have added a sentence explaining providers' data protection obligations in **Chapter 1** of the Guidance. We consider the privacy rights of users in **Action 1** to be appropriately addressed by the additional signposting to data protection laws and the ICO's Guidance in **Chapter 1**.

## Terms of service and setting policies

5.32 This section summarises our proposals, stakeholder feedback and our final decision for both the foundational step on terms of service and publicly available statements and our good practice step on setting policies, given the thematic overlap between the two.

### What we proposed

5.33 As noted in paragraph 5.23 in this statement, at consultation, we included a foundational step on providers having clear and accessible provisions on how users are protected from illegal content (including illegal harms that disproportionately affect women and girls, such as stalking, harassment and intimate image abuse) as well as content harmful to children. Draft case study 1 provided a high-level view of how foundational steps set out under **Action 1**, including terms of service, can address online gender-based harm.

5.34 We also included a good practice step on setting policies that define and/or prohibit forms of online gender-based harms. We suggested different topics this could cover including illegal harms such as stalking, abuse affecting specific groups such as misogynoir (hate directed at Black women and girls), deliberate misgendering and the promotion of offsite abuse. We also included a case study (draft case study 2) which looked at good practice for setting policies.

### Summary of stakeholder feedback

5.35 Several stakeholders raised concerns that setting policies on illegal harms such as stalking, harassment and intimate image abuse was good practice rather than foundational.[366]

5.36 We also received suggestions for ways to strengthen the good practice steps on setting policies. Some stakeholders called on the Guidance to prevent rollback in policies, and for Ofcom to call out rollbacks.[367] Two stakeholders urged us to emphasise the need for providers to act on new risks.[368]

[366] Response(s) to February 2025 consultation: The Minderoo Centre for Technology and Democracy at the University of Cambridge, p.3; Suzy Lamplugh Trust, p.6; Johnstone, E., p.4; Refuge, p.1; End Violence Against Women Coalition (EVAW), p.9.
[367] Response(s) to February 2025 consultation: End Violence Against Women Coalition (EVAW), p.9; Glitch, p.5; Suzy Lamplugh Trust, p.2.
[368] Response(s) to our February 2025 consultation: Refuge Annex, p.11; Plan International UK, p.11.

5.37 Several respondents welcomed references to forms of abuse affecting specific groups (misogynoir[369] and misgendering[370]), and some called on us to emphasise these issues further.[371] However two other stakeholders queried whether reference to policies on 'deliberate misgendering' could lead to suppression of gender-critical beliefs, noting they are protected speech.[372] As noted in **Section 3** and the rights assessment (**Annex A3**), in this statement, others raised general concerns that the Guidance infringed on freedom of expression as it could lead to platforms banning or removing legal content. For example, BILETA argued policies need clear definitions to avoid chilling legitimate expression.[373]

5.38 5Rights Foundation emphasised the importance of providers clearly explaining their policies to users, including children.[374] One stakeholder suggested that providers' policies should also explain the practical actions they take against breaches of their terms of service.[375] Another stakeholder suggested that service providers need to make their guidelines public, and should be the same internally and externally.[376]

5.39 Several stakeholders called for the good practice step on setting policies to cover additional kinds of content. For example, stakeholders suggested that service providers use the British Board of Film Classification (BBFC) standards as a guideline and/or prohibit content that is 'unclassifiable' by the BBFC. [377] Collective Shout suggested that community standards should prohibit all sexualised, predatory and grooming-style comments.[378]

## Our final decision

5.40 We have removed the reference to setting policies on stalking, harassment and intimate image abuse as this is addressed within the foundational step on terms of service. To illustrate this, we have updated **Case study 1** to focus on a social media provider capturing stalking within its terms of service. In response to feedback to consider the needs of children, we have highlighted that the provider should ensure its terms of service are clear and accessible, including for the youngest users. We also explore how internal teams can work together to design a proportionate and clear policy, and how this links to other foundational steps such as monitoring trends and staff training. While we have not included a specific good practice step on preventing rollbacks on policies, we have added a consideration in **Case study 1** to remind providers that before making a significant change to their service, they will need to carry out a risk assessment in relation to the impacts of that change.

---

[369] Response(s) to our February 2025 consultation: Glitch, p.2; End Violence Against Women Coalition (EVAW), p.2-3.
[370] Response(s) to our February 2025 consultation: NSPCC, p.6. Other stakeholders also argued the importance of considering abuse directed at LGBTQ+ people online, including: The Minderoo Centre for Technology and Democracy at the University of Cambridge, p.2; Institute for Strategic Dialogue (ISD), p.14.
[371] Response(s) to our February 2025 consultation: Galop, p.2; Glitch, p.1-2: End Violence Against Women Coalition (EVAW), p.9.
[372] Response(s) to our February 2025 consultation: Free Speech Union, p.4; LGB Alliance, p.2.
[373] Response to February 2025 consultation: British and Irish Law, Education, and Technology Association (BILETA), p.3.
[374] Response(s) to our February 2025 consultation: 5Rights Foundation, p.8.
[375] Response(s) to February 2025 consultation: Heriot-Watt University - University of Edinburgh, p.12.
[376] Response(s) to February 2025 consultation: Are, C., p.3.
[377] Response(s) to February 2025 consultation: Baroness Bertin, p.2; British Board of Film Classification (BBFC), p.1-2; Centre to End All Sexual Exploitation (CEASE), p.6; CARE (Christian Action Research and Education), p.4-6.
[378] Response(s) to February 2025 consultation: Collective Shout, p.19.

5.41 **We have also amended the foundational step on terms of service and publicly available statements** to note that provisions should be easily accessible to users, including being easy to find, clearly formatted, written to a comprehensible reading age for the youngest user permitted to use the service without parental consent and designed to be compatible with assistive technologies like screen readers. This reflects the recommendations in our Illegal Content and Protection of Children Codes of Practice on how to make terms of service and publicly available statements clear and accessible.

5.42 **We have retained the good practice step on setting policies, including references to abuse affecting specific groups** (misogynoir and deliberate misgendering). We have added a footnote to explain that some gender critical beliefs are protected under the Equality Act 2010. We have not expanded the examples to include any additional areas as the list is not meant to be exhaustive. However, we have incorporated the feedback on the BBFC Guidelines within the good practice step on subject matter expertise (see paragraph 3.17 in the Guidance). We have decided not to add a good practice recommending banning specific types of legal pornographic content in a provider's term of service (e.g. based on BBFC standards). Recommending this would capture content outside of the scope of this Guidance and, therefore, it would not be proportionate.

5.43 **We have also updated Case study 2 which illustrates good practice in setting policies.** In line with the changes we have made to case studies set out in paragraphs 5.20-5.22 in this statement, the amended case study looks at how a discussion forum can update its policies to capture an emerging form of misogynistic abuse not obviously prohibited in its existing policies. We explain that legal and trust and safety teams work together to ensure the policy is precisely defined to avoid overreach. We also added considerations to the case study. First, we remind providers that ultimately, it is their choice where they choose to set their policies so long as they comply with their duties. Second, we emphasise that good policies only lead to safer outcomes if they are enforced.

5.44 Providers must remove illegal content on their services when they are aware of it, protect children from content harmful to them and must ensure their terms of service secure this outcome. However, we recognise that setting policies on other types of content that does not meet the threshold of illegality, and which extends to adults, has the potential to interfere with users' freedom of expression. We have carefully considered this good practice step in line with feedback set out above, as well as more general feedback on freedom of expression set out in the rights assessment (**Annex A3**). We remain of the view that if providers set policies that are precise and clearly explained, it will support our aim to protect the rights of women and girls, as well as other groups targeted by online gender-based harms. We have outlined the scope of the harm areas focused on in the Guidance in **Section 4** of this statement. Aside from illegal content and content where providers have duties under the Act in relation to content harmful to children, it is a matter for providers as to whether they choose to allow particular categories of content on their services.

## Other good practice steps in Action 1

### What we proposed

5.45 At consultation, we proposed additional good practice steps on:

a) Consulting with subject matter experts when designing policies.
b) Considering intersectionality in governance and decision-making processes
c) Training staff

d) Creating a media literacy-by-design policy
e) Establishing an oversight mechanism (draft case Study 3)

## Subject matter experts

### Summary of stakeholder feedback

5.46 Many stakeholders supported our recommendations to consult subject matter experts to improve their governance and accountability.[379] Industry stakeholders gave examples of how they engage with subject matter experts or emphasised the value of engagement.[380]

5.47 Some stakeholders called for more detail on how subject matter experts would be compensated.[381] One stakeholder said that "Ofcom must take steps to ensure those providing advice to service providers are being accurate in their representation of the law".[382] Another stakeholder requested clarity on what expertise would be expected, such as on freedom of expression.[383] Some noted the importance of consulting with trauma-informed experts and including victim-survivors, including within the external oversight arrangements.[384] However, one stakeholder flagged challenges with directly engaging with survivors and victims.[385] Two stakeholders recommended a joint advisory board for multiple services.[386] The Cyber Helpline also suggested Ofcom keep a database of vetted experts.[387]

### Our final decision

5.48 We are confirming the inclusion of a good practice step on subject matter experts but have made minor changes.

5.49 We have added what appropriate subject matter expertise could look like and how it can vary. To illustrate this, we use the example of services that allow pornographic content consulting classification bodies who have expertise in classifying pornography, such as the BBFC. This means we are suggesting that providers could seek advice on how and why to moderate, or otherwise address, certain types of content.[388]

5.50 We have also added a new case study (**Case study 3**) on a messaging provider working with subject matter experts to prevent and respond to coercive control. We explore identifying informed specialist groups and engaging with them as active participants, including through

---

[379] Response(s) to February 2025 consultation: Match Group, p.1; TikTok, p.2; Women's Aid Federation Northern Ireland, p.1; Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.2; British and Irish Law, Education, and Technology Association (BILETA), p. 3; Children's Commissioner for England's Office, p.4; Ending Violence Against Women Coalition (EVAW), p.9; Welsh Government, p.2-7.
[380] Response(s) to our February 2025 consultation: Match Group, p.2-3; TikTok, p.5-6; Meta Platforms Inc, p.1; [✂].
[381] Response(s) to our February 2025 consultation: Refuge, p.6; End Violence Against Women Coalition (EVAW), p.9; White Ribbon UK, p.5.
[382] Response(s) to our February 2025 consultation: LGB Alliance, p.3.
[383] Response(s) to February 2025 consultation: Free Speech Union, p.4.
[384] Response(s) to February 2025 consultation: [✂]; The Cyber Helpline, p.8; The four Welsh Office of Police and Crime Commissioners, p.4.
[385] Response(s) to our February 2025 consultation: Meta Platforms Inc, p.10.
[386] Response(s) to February 2025 consultation: The Cyber Helpline, p.3; British and Irish Law, Education, and Technology Association (BILETA), p.3.
[387] Response(s) to February 2025 consultation: The Cyber Helpline, p.8.
[388] Some providers may choose to ban this content, or they could apply other protections such as content warnings or reducing prominence. In any case, when services allow this content, children should be prevented from accessing it by means of highly effective age assurance.

co-design workshops and an advisory board. Under considerations, we flag issues around appropriate compensation for subject matter experts and how small or medium sized providers could engage with subject matter experts proportionately – we suggest that small and medium services may wish to use existing resources and research published by organisations with expertise in online gender-based harms.

5.51 As noted above, we stress the importance of identifying appropriate and informed organisations in both the good practice step and **Case study 3**. We have decided not to specify a list of organisations providers could partner with. As the online safety regulator, it is not for Ofcom to determine the organisations who can act as expert advisors for different harms areas, instead this is a matter for service providers and organisations who have this expertise to decide between themselves. There is a risk that if we were to publish a list of 'approved partners', we could undermine competition and innovation in the provision of advice and expertise of this kind, which would be inconsistent with our general duties to further the interests of consumers in relevant markets, including by promoting competition where appropriate.

## Other good practice steps and additional feedback

### Summary of stakeholder feedback

5.52 **Intersectionality:** One stakeholder welcomed the inclusion of this good practice step,[389] and another recommended that we include a dedicated case study.[390] However, Meta Platforms Inc. noted that services may "lack the nuanced and detailed context necessary to know about the potential intersecting parts of a user's experience". They suggested alternatives such as providing tools to help users control experiences, taking action against individual acts that violate their policies and signpost to external resources.[391] More generally, we received support from stakeholders on considering intersectionality across the Guidance (see paragraphs 3.37 in this statement and the equality impact assessment (**Annex A3**) for more detailed feedback).

5.53 **Media literacy by design:** Several stakeholders supported the recommendation to develop media literacy-by-design policy.[392] Stakeholders called for this to be more explicitly informed by gender-based harms,[393] or prioritise media literacy interventions that target children.[394]

5.54 **Staff training:** One stakeholder recommended that training and oversight should emphasise consistent, proportionate enforcement and protect women from abuse while not unduly censoring debate.[395] Several other stakeholders argued that moderators should be required to undergo training on bias, emerging risks, Ofcom's Guidance and cultural contexts of abuse, with input from subject matter experts and lived experience participants.[396] One

[389] Response(s) to our February 2025 consultation: Antisemitism Policy Trust, p.1.
[390] Response(s) to our February 2025 consultation: Refuge Annex, p.3.
[391] Response(s) to our February 2025 consultation: Meta Platforms Inc, p.9-10.
[392] Response(s) to February 2025 consultation: Internet Matters, p.11; Welsh Government, p.3; Girlguiding, p.8.
[393] Response(s) to February 2025 consultation: Refuge Annex, p.4.
[394] Response(s) to February 2025 consultation: Internet Matters, p.11-12.
[395] Response(s) to February 2025 consultation: British and Irish Law, Education, and Technology Association (BILETA), p.3.
[396] Response(s) to February 2025 consultation: Heriot-Watt University - University of Edinburgh, p.12; Suzy Lamplugh Trust, p.6; The Cyber Helpline, p.12; Johnstone, E., p. 7; End Violence Against Women Coalition

stakeholder suggested quality assurance in the design and delivery of training.[397] Another suggested training on LGBT+, disability and global majority perspectives.[398] Others suggested extending training to non-permanent staff such as contractors and emphasised the importance of effective standards for training[399] or mandating training for senior managers and board members.[400]

5.55 **External oversight:** Stakeholders welcomed this good practice step.[401] One stakeholder said the oversight mechanism, "can enhance accountability and provide due process for users, ensuring that mistaken removals or biases can be corrected".[402] One stakeholders suggested oversight should extend to broader operations of the service.[403] This stakeholder cautioned that the step could be a burden to trust and safety teams if not extended to wider operations involved in trust and safety decisions.[404]

5.56 **Additional feedback:** We also received feedback from stakeholders on the importance of sufficient resource to address harms.[405] For example, one stakeholder argued that "ensuring that tech companies provide adequate resource to address harms faced by women and girls is central to delivering safer experiences for women and girls."[406] The Institute for Strategic Dialogue (ISD) provided evidence that "election periods and crisis events must be addressed as high-risk contexts" as these events "are flashpoints for coordinated abuse, disinformation, and VAWG against women in public life" and provided recommendations for platforms, including "developing event-specific crisis protocols".[407]

### Our final decision

5.57 We are confirming our position at consultation to include good practice steps on intersectionality, media literacy by design and staff training. We have made some minor changes to respond to stakeholder feedback.

a) **Intersectionality:** We have not added a case study on intersectionality in **Chapter 3**, as we refer to this in **Case study 14** on automated detection of misogynoir.
b) **Media literacy:** We have noted the positive benefits for children and young adults.
c) **Training employees:** We have added that this good practice step should focus on proportionate enforcement and note that contractors should also receive adequate training.

---

(EVAW), p.9; South West Grid for Leaning (SWGfL), p.7; Refuge, p.9; Gender + Tech Research Lab Department of Computer Science, p.6

[397] Response(s) to our February 2025 consultation: Heriot-Watt University - University of Edinburgh, p.9,12.

[398] Response to February 2025 consultation: Galop, p.1-2.

[399] Response to February 2025 consultation: Gender + Tech Research Lab Department of Computer Science, p.6.

[400] Response(s) to our February 2025 consultation: Refuge Annex, p.4.

[401] Response(s) to our February 2025 consultation: Commissioner Designate for Victims of Crime Northern Ireland, p.4-5; End Violence Against Women Coalition (EVAW), p.8-9; The Cyber Helpline, p.3; Refuge Annex, p.5.

[402] Response(s) to our February 2025 consultation: British and Irish Law, Education, and Technology Association (BILETA), p.3.

[403] Response(s) to our February 2025 consultation: Integrity Institute; Council on Technology & Social Cohesion; University of Southern California, Marshall School Neely Center, p.3.

[404] Response(s) to our February 2025 consultation: Integrity Institute; Council on Technology & Social Cohesion; University of Southern California, Marshall School Neely Center, p.3.

[405] Response(s) to our February 2025 consultation: British and Irish Law, Education, and Technology Association (BILETA), p.18; End Violence Against Women Coalition (EVAW) Annex 1, p.6.

[406] Response(s) to our February 2025 consultation: 5Rights Foundation, p.7.

[407] Response(s) to our February 2025 consultation: Institute for Strategic Dialogue (ISD), p.9.

d) **External oversight:** Drawing on stakeholder feedback, we have expanded the purview of the oversight mechanism beyond trust and safety to include other systems and processes. In line with the general changes we have made to case studies, set out in paragraphs 5.20-5.22 in this statement, the amended **Case study 4** now focuses on a social media provider setting up an external arbitration process involving external subject matter experts. We note the cost of this could be prohibitive for smaller services and suggest other approaches.

5.58 We have also added a new good practice step in response to feedback and to align with our wider online safety work:

a) Ensuring adequate resourcing to develop ongoing policy and risk expertise to deliver trust and safety objectives. We note this could include adequate resource and expertise to respond to moments of increased risks of online gender-based harms, such as during periods of key civic moments (for example, elections).[408]

# Action 2: Conduct risk assessments that focus on harms to women and girls

## Overall approach and foundational steps

### What we proposed

5.59 At consultation, we proposed that service providers need to build an understanding of factors that enable and promote online gender-based harms in their online safety risk assessments to design safer systems and processes. We explain it is up to providers to decide which good practice steps are most appropriate for their service. We included foundational steps on:

a) Risk assessment (draft case study 4)
b) Internal content and search moderation policies

### Summary of stakeholder feedback

5.60 We received general feedback in support of our proposed **Action 2** from a range of stakeholders, including civil society, subject matter experts (specifically on violence against women and girls), academia, public sector organisations and individuals.[409]

5.61 We received stakeholder feedback requesting clarification on conducting gender-sensitive risk assessments, specifically how it links with services' duties to complete risk assessments for Illegal Harms and Protection of Children. Some stakeholders argued that an additional gender-sensitive risk assessment is onerous for service providers, considering the other mandatory risks assessments that service providers need to conduct to comply with the Illegal Content and Protection of Children Code measures.[410]

[408] In making this recommendation, we have also considered research on the experiences of online hate and abuse among women in politics. See: Ofcom, 2025, Experiences of online hate and abuse among women in politics.
[409] Response(s) to February 2025 consultation: British and Irish Law, Education and Technology Association (BILETA), p.4; Welsh Government, p.4; 5Rights Foundation, p.6-7; End Violence Against Women Coalition (EVAW), p.9; Children's Commissioner for England's Office, p.5; Johnstone, E., p.3.
[410] Response(s) to February 2025 consultation: Meta Platforms Inc, p.5-6; [✂].

5.62 The Women in Tech Policy Network indicated that "there should be a clear code of practice that are integral to guidance to facilitate enforcement." They additionally stated that Ofcom should be able to link guidance to the risk assessments that regulated services have to do under their safety duties.[411]

5.63 We also received stakeholder feedback that service providers should take into consideration additional data for their risk assessments:

a) User demographics,[412] such as how the age of online users intersects with their gender;[413]
b) Trigger words or phrases, hashtags, visual tags, user profile and bio contents, and how these indicators relate to potential harm with periodic comparisons.[414]

5.64 It was also suggested that service providers consider the unique experiences of marginalised communities and young people online.[415] Clean Up the Internet suggested effective harms prevention requires an understanding of how perpetrators interact on service providers' platforms.[416] Other stakeholders noted that service providers may lack information to know about the potential intersecting parts of a users' experience, but they can provide tools to give uses better control over their experiences or take action in response to individual acts that violate their terms of service.[417]

5.65 Regarding the collection and use of data, Do-Ngoc, T. and Carmel, E. indicated that the "guidance should explicitly state that data collection and monitoring practices must uphold privacy rights and be subjected to rigorous human rights impact assessments".[418] The ICO indicated that "demographic data collection for advertising or user experience improvement is frequently facilitated through storage of and access to information on users' devices, including via the use of cookies and similar technologies which are subject to the Privacy and Electronic Communications Regulations (PECR)". They further suggested that our guidance reference ICO resources on the use of storage and access technologies, including broader guidance on PECR and UK GDPR.[419]

5.66 Lastly, we received support for the case study on gender sensitive risk assessments and emphasised the importance of accounting for risks of harms to different individuals.[420]

## Our final decision

5.67 We are confirming our position at consultation to include **Action 2** on conducting risk assessment that focus on harms to women and girls. We acknowledge that risk assessment

---

[411] Response(s) to February 2025 consultation: Women in Tech Policy Network, p.2.
[412] Response(s) to February 2025 consultation: Antisemitism Policy Trust, p.3; Equality Now, p.1; End Violence Against Women Coalition (EVAW), p.10; Internet Matters, p.12; Moxon, S.P., p.4; Refuge, p.10-11; Heriot-Watt University – University of Edinburgh, p.7; [✂]; [✂]; [✂]; Age Check Certification Scheme, p.2; Girlguiding, p.6; White Ribbon UK, p.2; Parity, p.6; Evans, M.I., p.2; [✂].
[413] Response(s) to February 2025 consultation: Age Check Certification Scheme, p.2; Girlguiding, p.6.
[414] Response(s) to February 2025 consultation: University of Southampton; Lancaster University; University of Liverpool; Queen Mary University of London, p.3.
[415] Response(s) to February 2025 consultation: Internet Matters, p.12; Girlguiding, p.6; Antisemitism Policy Trust, p.3.
[416] Response(s) to February 2025 consultation: Clean Up the Internet, p.2.
[417] Response(s) to February 2025 consultation: Meta Platforms Inc., p.10; [✂].
[418] Response(s) to February 2025 consultation: Do-Ngoc, T. and Carmel, E., p.7.
[419] Response(s) to our February 2025 Consultation: Information Commissioners Office (ICO), p.12.
[420] Response(s) to February 2025 consultation: End Violence Against Women Coalition (EVAW), p.9; Young Women's Movement, p.7.

processes may include the collection, processing and storing of personal data, including in some cases special category data. As set out in further detail in the following sections, we have included additional references to ICO guidance and resources, where relevant, in both the foundational and good practice steps in **Action 2**. We consider this addresses concerns relating to privacy and data protection laws.

5.68 **We are confirming our position at consultation on the inclusion of the foundational steps set out at consultation.** We have made minor changes to clarify the duty to conduct a suitable and sufficient illegal content risk assessment. We have also made changes to the foundational step on internal content policies to include that providers must have processes in place for updating these policies in response to evidence of new and increasing illegal harm or harm to children on the service.

5.69 We have also retained the foundational steps case study on gender-sensitive risk assessment **(**draft case study 4, now **Case study 5**) set out in the consultation. However, after careful consideration of the stakeholder feedback, we have made some amendments to the case study:

a) In line with the general changes we have made to case studies, set out in paragraphs 5.20-5.22 in this statement, the amended case study looks at how a gaming service provider can identify the different types of risks girls and boys face on its service.
b) We have added language to encourage service providers to map how users with multiple protected characteristics experience unique and compounding risks by incorporating the framework of intersectionality into risk assessments.
c) We added a reference to additional ICO resources to support service providers in appropriately complying with Privacy and Electronic Communication Regulations and UK GDPR duties. We also signpost to the Age Appropriate Design Code.

5.70 We recognise that some stakeholders expressed concerns about the burden on service providers in conducting a specific risk assessment for women and girls. However, our position remains that gender-sensitive risk assessments provide valuable and necessary insights to effectively protect women and girls online. As such, we consider it proportionate to recommend this action given the benefits to protecting women and girls. The Guidance aims to set out how service providers can consider gender sensitive issues while fulfilling their duties to conduct risk assessments under the Illegal Content and Protection of Children Codes.

5.71 We consider that service providers can choose how best to conduct a gender-sensitive risk assessment. They could either:

a) integrate considerations of the gender-specific risks, and their impact, into an existing risk assessment (i.e., Illegal Harms and Protection of Children risk assessments); or
b) conduct an independent risk assessment tailored to women and girls.

## Good practice steps in Action 2

### What we proposed

5.72 At consultation, we proposed the following good practice steps as further mitigations:

a) Using external assessors for monitoring the threat landscape
b) Engaging with survivors and victims

c) Conducting user research (draft case study 5)
d) Conducting a rights impact assessment

## External assessors for monitoring the threat landscape

5.73 At consultation, we proposed that service providers use external assessors for monitoring the threat landscape, including local partners with regional and cultural knowledge and international partners with expertise in highly contextual risk areas such as cyberstalking and controlling or coercive behaviour.

### Summary of stakeholder feedback

5.74 We received feedback that supported this proposed good practice step[421] and one stakeholder recommended that service providers undergo regular, independent and external safety audits "to ensure truthful reporting and accountability" as self-assessments often downplay systematic risks tied to commercial interests.[422] Another stakeholder recommended that external assessors endorse the risk assessments conducted by service providers.[423]

5.75 End Violence Against Women Coalition (EVAW) requested clarity in the Guidance on the selection of appropriate external assessors,[424] and similarly another stakeholder suggested Ofcom provide a list of appropriate external assessors for service providers.[425] We also received feedback suggesting that Ofcom conduct quality assurance on external assessors for service providers.[426] One stakeholder suggested the Guidance identify law enforcement as an appropriate external assessor for service providers.[427]

5.76 Lastly, we received feedback from two stakeholders that highlighted third-party organisations are often under-resourced and, as a result, may face challenges in their capacity to engage in the risk assessment processes.[428] There was a recommendation that Ofcom encourage service providers to adequately fund external assessors for any engagement or support on the risk assessment process.[429]

### Our final decision

5.77 **We are confirming the inclusion of our proposed good practice on using external assessors.**[430] We acknowledge the stakeholder feedback requesting additional clarity on the selection of appropriate external assessors, including Ofcom's role in providing assurance on their quality. However, we do not consider it appropriate to recommend specific external assessors, including providing quality assurance. As the online safety regulator, it is

[421] Response(s) to February 2025 consultation: Scottish Government, p.4.
[422] Response(s) to February 2025 consultation: Harrison, J, p.3.
[423] Response(s) to February 2025 consultation: Scottish Government, p.3.
[424] Response(s) to February 2025 consultation: End Violence Against Women Coalition (EVAW), p.11.
[425] Response(s) to February 2025 consultation: Bolt Burden Kemp LLP, p.3.
[426] Response(s) to February 2025 consultation: Heriot-Watt University - University of Edinburgh, p.12.
[427] Response(s) to February 2025 consultation: Association of Police and Crime Commissioners, p.2.
[428] Response(s) to February 2025 consultation: Refuge, p.7; Gender + Tech Research Lab Department of Computer Science, p.3.
[429] Response(s) to February 2025 consultation: Refuge, p.7; Gender + Tech Research Lab Department of Computer Science, p.3.
[430] This is an example of an 'enhanced input' under the risk assessment process laid out in the Illegal Content Risk Assessment Guidance and Children's Risk Assessment Guidance (namely seeking the views of independent experts). We expect enhanced inputs for some kinds of service providers to ensure their illegal content and children's risk assessments are suitable and sufficient, but this is optional (and therefore good practice) for other providers.

not for Ofcom to determine the organisations who can act as expert advisors in different harms areas, instead this is a matter for service providers and organisations who have this expertise to decide between themselves. There is a risk that if we were to publish a list of 'approved partners', we could undermine competition and innovation in the provision of advice and expertise of this kind, which would be inconsistent with our general duties to further the interests of consumers in relevant markets, including by promoting competition where appropriate. Rather, we set out relevant types of subject matter experts that may be beneficial in an external assessor, such as law enforcement or civil society organisations, which may help service providers with the selection process.

5.78 We also recognise the capacity concerns raised about third-party organisations. However, we do not consider it appropriate to directly call on service providers to provide financial compensation to organisations, as this type of recommendation extends beyond Ofcom's remit. Rather, we have revised **Case study 3** on engaging with subject matter experts to explicitly note that as third-party organisations are often under-resourced, it is good practice for a service provider to provide appropriate compensation for any work dedicated to improving the service provider's policies or practices (this includes external assessors for risk assessments).We additionally mention the importance of fair treatment of partners in **Case study 21**, which incorporates the good practice step on trusted flagger programmes.

## Engaging with subject-matter experts and vulnerable groups

### Summary of stakeholder feedback

5.79 Many stakeholders emphasised the importance of involving women with lived experiences of online harm in the risk assessment process, such as through co-design labs, user surveys and focus groups.[431] It was also suggested this engagement should be trauma-informed and conducted in a sensitive manner, and participating individuals should receive compensation.[432] Additional feedback included:

a) Meta Platforms Inc indicated that "Ofcom should enable services to tailor their existing risk assessments to their unique operational contexts and leverage the expertise of internal and external stakeholders, including subject matter experts on various harm areas. By doing so, services can develop more effective and targeted risk assessments that address the distinct needs of their users and types of platforms".[433] They also highlighted the challenges of engaging directly with survivors and victims and suggested engaging with third-party organisations that work with victims and survivors instead.[434]

b) Gender + Tech Research Lab Department of Computer Science indicated that "guidance must also be provided setting out how they [service providers] can do so sensitively and in a way which will not trigger or cause any further harm to the individuals involved. Feedback from victims-survivors must also be representative,

[431] Response(s) to February 2025 consultation: End Violence Against Women Coalition (EVAW), p.11; Suzy Lamplugh Trust, p.3; Welsh Government, p.3; Children's Commissioner for England's Office, p.5; Refuge Annex, p.9; University of York, p.4; Welsh Women's Aid, p.4; Girlguiding, p.11; White Ribbon UK, p.6.
[432] Response(s) to February 2025 consultation: Refuge Annex, p.8; Gender + Tech Research Lab Department of Computer Science, p.3; The Minderoo Centre for Technology and Democracy at the University of Cambridge, p.2.
[433] Response(s) to February 2025 consultation: Meta Platforms Inc, p.6.
[434] Response(s) to February 2025 consultation: Meta Platforms Inc, p.10.

methodologically sound, and address the risk of piecemeal improvements which mask broader harms".[435]

c) End Violence Against Women Coalition (EVAW) expressed support for the inclusion of "survivors' voices and needs"[436] in the risk assessment process. However, they indicated that it is important that "this work is not tokenistic or extractive and leads to meaningful change to platform design… Likewise, as this guidance is also for combatting harm against girls, young people's voices should also be included in the design process to ensure their needs are met".[437]

d) Do-Ngoc, T. and Carmel, E. suggested making lived experiences, including those specifically of children, central to the design, implementation and ongoing evaluation of safety measures. They recommended that "Ofcom should therefore support the creation of standing participation panels, including survivor panels, youth advisory boards, and expert working groups".[438]

5.80 The ICO noted that personal information recorded through engagement with victims and survivors and users with protected characteristics may constitute special category data, under Article 9 of the UK GDPR. The ICO referenced guidance on special category data and criminal offence data, and suggested providers consult these documents to ensure compliance with data protection law.[439]

5.81 We also received a significant amount of feedback that suggested service providers engage with external organisations, such as civil society and law enforcement, to inform their risk assessments.[440]

### Our final decision

5.82 We are confirming the inclusion of our proposed good practice on engaging with subject matter experts. We did not make any changes to this good practice.

5.83 We recognise the importance of meaningful and respectful engagement with subject matter experts, including survivors and victims of gender-based violence. We carefully considered the stakeholder feedback and decided the Guidance needed to better illustrate how service providers can appropriately engage with subject matter experts and victims and survivors. As such, we have added a good practice case study on engagement with subject matter experts, including survivors and victims of gender-based violence under **Action 1** (**Case study 3**). As noted in paragraphs 5.20-5.22 in this statement, this case study illustrates how service providers are expected to engage with subject matter experts, including survivors and victims, to address gender-based violence. This includes acknowledging the need to minimise the risk of re-traumatisation. We have referred to the

[435] Response(s) to February 2025 consultation: Gender + Tech Research Lab Department of Computer Science, p.3.
[436] Response(s) to February 2025 consultation: End Violence Against Women Coalition (EVAW), p.11.
[437] Response(s) to February 2025 consultation: End Violence Against Women Coalition (EVAW), p.11.
[438] Response(s) to February 2025 consultation: Do-Ngoc, T. and Carmel, E., p.6.
[439] Response(s) to February 2025 consultation: Information Commissioners Office (ICO), p.5.
[440] Response(s) to February 2025 consultation: Women's Aid Federation of England, p.8; Refuge Annex, p.8; Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.2; Centre for Protecting Women Online, p.16; The Cyber Helpline, p.3, [✂]; End Violence Against Women Coalition (EVAW), p.10-11; Bolt Burden Kemp LLP, p.3; Association of Police and Crime Commissioners, p.2; Heriot-Watt University – University of Edinburgh, p.9; Equality Now, p.1; NSPCC, p.15; Plan International UK, p.11. Ofcom / Young People's Action Group roundtable, 7 July 2025.

ICO's guidance to ensure that providers are aware of the impacts on the data protection rights and their obligations when taking this step and other related good practice.

## Conducting user research

### Summary of Stakeholder Feedback

5.84 We received stakeholder feedback on both the good practice for conducting user research and the associated case study (draft case study 5, now **Case study 6**) on trauma-informed user surveys.

5.85 Suzy Lamplugh Trust indicated that "dating platforms are often the initial meeting site but perpetrators might start stalking their victims across various other platforms after this. This should be reflected in the case study to prompt platforms to think about how they could safeguard victims when the majority of behaviours are being experienced on other sites".[441]

5.86 We also received feedback from White Ribbon UK that indicated "Ofcom should encourage similar surveys targeted at men and boys to better understand their online experience".[442] They further recommended adding an additional good practice step for service providers to conduct research into, and risk assessments on, what men and boys are viewing online and its impact and another encouraging providers to facilitate regular attitude surveys with users to detect harmful trends early and develop proactive interventions.[443]

5.87 Gender + Tech Research Lab Department of Computer Science indicated that service providers need to engage carefully with victims and survivors with regards to conducting trauma-informed user surveys. They noted that "victim-survivors often do not recognise what they are experiencing as abuse, due to both the normalisation of digital surveillance and control, and a lack of awareness around emerging forms of harm".[444] They further indicated that user surveys that do not account these dynamics risk producing misleading results and may be used to safety-wash company behaviour.[445]

### Our final decision

5.88 We are confirming the inclusion of our proposed good practice on conducting user research. We did not make any changes to this good practice.

5.89 We updated **Case study 6** on conducting trauma-informed research and user surveys. In line with the changes we have made to case studies set out in paragraphs 5.20-5.22 in this statement, the amended case study looks at an online dating service provider with users experiencing stalking and coercive control. The revised case study provides greater clarity on the expected actions of a service provider when addressing stalking and coercive control. We also signpost to relevant ICO guidance.

5.90 We recognise the importance of ensuring survivors and victims are not re-traumatised by participating in this type of engagement. We therefore recommend that service providers collect data in a sensitive manner, including in a way which is compatible with data protection law, and recommend that providers ensure users receive appropriate support by

[441] Response(s) to February 2025 consultation: Suzy Lamplugh Trust, p.7-8.
[442] Response(s) to February 2025 consultation: White Ribbon UK, p.5.
[443] Response(s) to February 2025 consultation: White Ribbon UK, p.2.
[444] Response(s) to February 2025 consultation: Gender + Tech Research Lab Department of Computer Science, p.3.
[445] Response(s) to February 2025 consultation: Gender + Tech Research Lab Department of Computer Science, p.3.

signposting in the survey results to organisations that offer supportive information, additional personalised support on sexual trauma and access to a trauma-informed therapist, depending on the users' specific results.

5.91 We also recognise the importance of service providers taking a holistic approach to protecting all its users from harmful content or activity online, including men and boys. For information on our approach, refer to **Section 3** in this statement.

## Conducting additional assessments

### Summary of stakeholder feedback

5.92 We received stakeholder feedback recommending that the risk assessments include information on how algorithms, virality, and content moderation systems or processes contribute to online gender-based harms.[446] For example, the Institute for Strategic Dialogue (ISD) that service providers "assess how their recommender systems contribute to VAWG, including gendered exposure to hate, harassment, and radicalising ideologies, and in this include an intersectional lens to consider the profiling and disproportionate impact on specific groups based on race, gender identity, disability and or religion."[447] Welsh Women's Aid recommended that service providers publish and conduct annual independent audits of their safety processes and systems for women, including checks of how algorithms treat gendered content and the accuracy of moderation decisions.[448]

5.93 The ICO suggested that the Guidance provide clarification that additional assessments, such as impact assessments on privacy, are separate from existing obligations for Data Protection Impact Assessment (DPIA) under data protection law.[449]

### Our final decision

5.94 We are confirming the inclusion of our proposed good practice on conducting additional assessments on users' self-expression, freedom from discrimination and privacy.

5.95 We acknowledge the feedback requesting that risk assessments include information on algorithms, virality and content moderation systems or processes. We have indicated that service providers can evaluate algorithmic systems such as content moderation and recommender systems for a variety of risks in relation to bias and discrimination.

5.96 Further, under this good practice we note that user-to-user services should also ensure that children's recommender feeds exclude or limit the prominence of content harmful to children, which may also involve undertaking algorithmic assessments. See **Action 6** and **Case study 10** in the Guidance for more information.

5.97 We have also clarified in the Guidance that impacts on users' privacy will often be considered under a data protection impact assessment (DPIA) and that a DPIA is a separate legal requirement under data protection law where services undertake processing of personal data that is likely to result in a high risk to the rights and freedoms of individuals. This includes certain specified types of processing, and the ICO has developed screening

---

[446] Response(s) to February 2025 consultation: Institute for Strategic Dialogue (ISD), p.7-8; End Violence Against Women Coalition (EVAW), p.9; Popa-Wyatt, M., p.1; British and Irish Law, Education, and Technology Association (BILETA), p.4; Collective Shout, p.19; Welsh Women's Aid, p.7.
[447] Response(s) to February 2025 consultation: Institute for Strategic Dialogue (ISD), p.7.
[448] Response(s) to February 2025 consultation: Welsh Women's Aid, p.7.
[449] Response(s) to February 2025 consultation: Information Commissioner's Office (ICO), p.5.

checklists to help determine when a DPIA is necessary. We provide links to the ICO's guidance on DPIAs and screening checklist.

## Additional feedback on Action 2

### Summary of stakeholder feedback

5.98 We received stakeholder feedback recommending that service providers consider the risks associated to supply chain requirements, including risks from outsourcing online safety actions and business relationships.[450] This included:

a) The Institute for Strategic Dialogue (ISD) indicated the importance of addressing supply chain harms, including apps and tools that facilitate gender-based violence but are not controlled or operated by the specific service provider.[451]
b) The End Violence Against Women and Girls Coalition (EVAW) indicated that service providers outsource their business functions, including contracting out their safety measures, which has an impact on the quality of moderation (i.e., moderators with poor working conditions). They also noted that contractors will not be required to adhere to the Guidance. They recommended that risk assessments consider impacts arising from business relationships. ISD also recommended service providers that outsource any part of their business (i.e., moderation of content, applications, GIFs, images, or any other content or tools) need to ensure the contractor adheres to the providers terms of service and outsourced user safety tools must also be fully compliant with the platforms' duties through the Codes as well as the recommendations made in this Guidance.[452]
c) The 5Rights Foundation suggested that service providers understand the risks posed to women and girls from their supply chains and communicate them in their risk assessments. They also indicated that understanding the impact of supply chains helps service providers evaluate risks of emerging technologies, in particular artificial intelligence as its built using datasets or models from third-parties.[453]

### Our final decision

5.99 **We have included a new good practice step proposing that service providers consider the risks associated with their supply chain that may impact the quality of actions taken to address gender-based violence on their service.**

5.100 We carefully considered the evidence submitted during the consultation that highlighted the importance of service providers understanding and accounting for any supply chain risks. We consider the evidence demonstrates a likely risk to a service providers' effectiveness in protecting women and girls online. Although this could be an issue that forms part of the provider's risk assessment (for example, when considering how their existing systems and processes impact the risk of harm), we recognise that the Risk Assessment Guidance, including the Children's Risk Assessment Guidance, does not expressly cover supply chain risks and we therefore decided to include this as a good practice step.

---

[450] Response(s) to February 2025 consultation: 5Rights Foundation, p.2; NSPCC, p.12; End Violence Against Women Coalition (EVAW), p.10; End Violence Against Women Coalition (EVAW) Annex 1, p.5; End Violence Against Women Coalition (EVAW) Annex 2, p.6, Institute for Strategic Dialogue (ISD), p.8,10.
[451] Response(s) to February 2025 consultation: Institute for Strategic Dialogue (ISD), p.8,10.
[452] Response(s) to February 2025 consultation: End Violence Against Women Coalition (EVAW), p.10.
[453] Response(s) to February 2025 consultation: 5Rights Foundation, p.6.

# Action 3: Be transparent about women and girls' online safety

## Overall approach

### What we proposed

5.101 At consultation, we proposed that transparency reporting is an important source of online safety information for users, which will shine a light on service providers' safety performance and empower users to make informed choices about the services they use. This could be particularly relevant for women and girls who face disproportionate risk online and therefore have to curate their experiences to keep themselves safe online. We explain it is up to providers to decide which good practice steps are most appropriate for their service. We proposed that in-scope services (which we call "categorised services") will be required to comply with additional duties focused on transparency.

### Summary of stakeholder feedback

5.102 We received general support for our proposed action from a range of stakeholders, including civil society, subject matter experts (specifically on violence against women and girls), academia, public sector organisations, and individuals.[454]

5.103 We received feedback from several stakeholders that requested additional clarity on the expectations for transparency reporting.[455] One stakeholder indicated that the Guidance does not provide an adequate discussion of how the specific transparency recommendations relate to violence against women and girls. For instance, they indicated that it is unclear whether information on gender-based harms are core or thematic information requirements, and whether the effectiveness of automated detection will be separately assessed for different harms.[456]

5.104 We also received feedback from two stakeholders suggesting that the foundational steps for transparency should apply to all platforms.[457] Whereas, another stakeholder suggested extending the scope of service providers to non-categorised services undermines the Online Safety Act.[458]

5.105 Stakeholders also raised concerns related to data protection and privacy, which we summarise and address under the relevant steps from 5.110 in this statement.

### Our final decision

5.106 **We are confirming our position at consultation on the inclusion of the foundational steps set out at consultation.** We did not make any changes to the foundational steps, including that the transparency duties only apply to providers of categorised services. However, the

[454] Response(s) to February 2025 consultation: Are, C., p.4; Plan International UK, p.12; Baroness Morgan of Cotes, p.1; Welsh Government, p.4; Belfast Area Domestic & Sexual Violence and Abuse Partnership, p.2.
[455] Responses to February 2025 consultation: Women's Aid Federation of England, p.15; The Cyber Helpline, p.4; Kira, B. Asser, Z. and Ruiz, J., p.11; Welsh Women's Aid, p.5; Popa-Wyatt, M., p.2; End Violence Against Women Coalition (EVAW), p.11; Scottish Government, p.4.
[456] Response(s) to February 2025 consultation: Kira, B. Asser, Z. and Ruiz, J., p.11.
[457] Response(s) to February 2025 consultation: Suzy Lamplugh Trust, p.8; Johnstone, E., p.7.
[458] Response(s) to February 2025 consultation: Meta Platform Inc., p.7.

Guidance is voluntary and, therefore, any service can implement the suggested actions to protect users from gender-based violence online.

5.107 We are confirming our position at consultation to not include a case study for the foundational steps. We currently do not have sufficient evidence to provide an illustrative example of how a service provider may implement the suggested foundational steps. We will consider updating the Guidance to include a practical example once Ofcom's transparency reporting regime is further developed and we have a better understanding of industry practice in this area.

5.108 We acknowledge the feedback that the draft guidance did not clearly communicate the transparency actions for service providers. For this reason, we decided to expand our explanation of the duties related to transparency reporting, including how it can protect women and girls from harmful activity online. To note, we do not specify the type of information that service providers need to include in their transparency notices because Ofcom is required to apply various principles and consider several factors in determining what we ask a service provider to publish.

5.109 We have also carefully reviewed feedback from stakeholders related to data protection and privacy, in particular regarding good practice steps. We have added signposting to the ICO's resources and guidance, as well as the data sharing code of practice, which we consider to appropriately address any concerns related to data protection and privacy impacts of this action. This is detailed in the following sections.

## Good practice steps in Action 3

### What we proposed

5.110 At consultation, we proposed three good practice steps:

a) Sharing information about the prevalence of different forms of online gender-based harms and the effectiveness of measures in place to address them
b) Providing more detail about which posts are flagged
c) Exercise caution in sharing information

### Sharing information about the prevalence of different forms of online gender-based harms

#### Summary of stakeholder feedback

5.111 We received support for the recommendation to include data on the prevalence of harm in transparency reporting.[459] Specifically, several stakeholders supported our recommendation for service providers to publish disaggregated data,[460] noting the benefits of age-,[461] race-,[462] gender-disaggregated data[463] as well as data on Scottish users.[464] For

[459] Response(s) to February 2025 consultation: University of York, p.5; [✂].
[460] Response(s) to February 2025 consultation: Evans, M.I., p.8; Institute for Strategic Dialogue (ISD), p.4; Southwest Grid for Learning (SWGfL), p.7; Parity, p.13; Popa-Wyatt, M., p.3; [✂]; [✂]; Equality Now, p.4.
[461] Response(s) to February 2025 consultation: Plan International UK, p.11; Internet Matters, p.12; Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.8.
[462] Response(s) to February 2025 consultation: Ending Violence Against Women Coalition (EVAW), p.11; Institute for Strategic Dialogue (ISD), p.3.
[463] Response(s) to February 2025 consultation: Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.8; [✂]; Institute for Strategic Dialogue (ISD), p.3.
[464] Response(s) to February 2025 consultation: Ofcom Advisory Committee for Scotland, p.3.

example, Equality Now indicated that anonymised demographic data disaggregated by gender, race, age and other relevant characteristic can help illustrate the effectiveness of safety tools in equitably protecting users.[465]

5.112 Conversely, industry stakeholders emphasised the difficulty of collecting and publishing demographic data disaggregated by these characteristics, particularly due to data privacy and data minimisation principles.[466] Meta Platforms Inc indicated that service providers "may not be able to provide specific data about women and girls and more broadly the gender of users in relation to violations of policies. Reviewers typically only see the content of the post that may violate the policy, and as part of the review process they may not know or label the gender of the parties involved in the violation including the poster or the recipient/reporter".[467] Similarly, Pinterest indicated that they do not collect some types of the suggested disaggregated data, such as data on users' race.[468]

5.113 In line with these concerns, some stakeholders recommended that effective transparency requires appropriate balancing and recognition of data protection.[469] The ICO recommended that the Guidance link to their data sharing code of practice, which includes case studies on secure data sharing and outlines the necessary steps that service providers will need to take to effectively demonstrate transparency and accountability. This includes adopting best practices such as establishing a data sharing agreement where necessary.[470]

**Our final decision**

5.114 We are confirming the inclusion of a good practice step on sharing information, for service providers not already in scope of the transparency reporting duties. We have clarified that providers should aim to publish information on online gender-based harms, and we specify the value of data-disaggregation. We have not set out specific metrics or definitions for data-disaggregation because of the range, availability and proportionality of data that service providers can publish. We ultimately expect increased transparency to improve the safety of different users' groups at risk of harm online, including men and boys.

5.115 We recognise the concerns raised regarding the limitations for providers to collect and report on some types of disaggregated data. However, we consider the action is appropriate and proportionate because these types of data, if available, can significantly help provider's understanding and prevention of gender-based violence on their service. However, we recommend service providers exercise caution in sharing information that perpetrators could exploit to circumvent safety measures, as well as details of specific incidents that could identify an individual or group, including location, sexual orientation, religion or other sensitive information that could put them at risk.

5.116 To support providers to ensure they comply with data protection law and in recognition of the data privacy risks related to the good practice steps in this action, we included a reference to ICO's guidance and resources on data protection law. We also provided a link to the ICO's code of practice on data sharing.

---

[465] Response(s) to February 2025 consultation: Equality Now, p.4.

[466] Response(s) to February 2025 consultation: Flux Digital Policy, p.3; Meta, p.6-7; Pinterest, p.6.

[467] Response(s) to February 2025 consultation: Meta Platforms Inc., p.7.

[468] Response(s) to February 2025 consultation: Pinterest, p.6.

[469] Response(s) to February 2025 consultation: Kira, B. Asser, Z. and Ruiz, J., p.12; British and Irish Law, Education, and Technology Association (BILETA), p.7; Information Commissioner's Office (ICO), p.6.

[470] Response(s) to February 2025 consultation: Information Commissioners Office (ICO), p.6.

## Providing more detail about which posts are flagged

### Summary of stakeholder feedback

5.117 We received a significant amount of stakeholder feedback regarding the recommendation for service providers to share more detail about posts detected by automated content moderation systems and processes, including:

a) Information on the context in which content moderation decisions were made by service providers, including on non-automated content moderation actions.[471]
b) Greater transparency in content moderation decision-making is required, including providing detailed outcomes of content moderation decisions by reporting mechanisms and sharing data on automated tool error rates.[472]
c) Role of recommender systems in content dissemination,[473] including shadow-banning of users.[474]
d) Information about flagged content and how that may impact content circulation, including shadow banning.[475]
e) Information on actions taken on content,[476] including on take-down[477] and outcomes of reports.[478] There was a request to report on this information with regards to pornography specifically. [479]

### Our final decision

5.118 **We are confirming the inclusion of a good practice step on sharing information.** We recognise that stakeholders recommended several types of additional information that service providers could report on as part of their transparency reporting obligations. We consider these recommended data types will be captured by this good practice and, therefore, we have not made any additional changes.

## Exercise caution in sharing information

### Summary of stakeholder feedback

5.119 We received feedback from the British and Irish Law, Education and Technology Association (BILETA) that cautioned against "transparency that might expose personal data or enable abuse… For instance, if a company publishes case studies of abusive incidents, they must anonymize identities so as not to retraumatize victims or inadvertently "name and shame" individuals without due process".[480] They also further indicated a risk of "overly detailed disclosure of automated moderation rules could allow malicious actors to game the system".[481] They ultimately recommended that service providers share "enough

[471] Response(s) to February 2025 consultation: Are, C., p.3.
[472] Response(s) to February 2025 consultation: Kira, B. Asser, Z. and Ruiz, J., p.13.
[473] Response(s) to February 2025 consultation: Kira, B. Asser, Z. and Ruiz, J., p.11; Institute for Strategic Dialogue (ISD), p.12-13; Equality Now, p.2; Collective Shout, p.19.
[474] Response(s) to February 2025 consultation: Essity, p.3.
[475] Response(s) to February 2025 consultation: Essity, p.3.
[476] Response(s) to February 2025 consultation: Welsh Women's Aid, p.5; British and Irish Law, Education and Technology Association (BILETA), p.5.
[477] Response(s) to February 2025 consultation: Chayn, p.7.
[478] Response(s) to February 2025 consultation: South West Grid for Learning (SWGfL), p.18.
[479] Response(s) to February 2025 consultation: Centre to End All Sexual Exploitation (CEASE), p.6.
[480] Response(s) to February 2025 consultation: British and Irish Law and Education and Technology Association (BILETA), p.5.
[481] Response(s) to February 2025 consultation: British and Irish Law and Education and Technology Association (BILETA), p.5.

information to illuminate the effectiveness and fairness of safety measures (e.g. percentages of content removed, median response times to abuse reports, existence of appeals), but not so much as to undermine those measures".[482]

#### Our final decision

5.120 **We are confirming the inclusion of a good practice step on exercising caution.** As explained above, we have signposted to the ICO resources and guidance, and data sharing code of practice. This will support service providers to appropriately consider and protect users' data protection rights and privacy. We also note that **Case study 6** on 'trauma-informed research and user surveys' illustrates how a service provider should engage with survivors and victims, in an attempt to minimise the risk of re-traumatisation.

## Additional feedback on Action 3

### Sharing evidence on emerging trends and risks

#### Summary of stakeholder feedback

5.121 We received feedback from stakeholders that highlighted the importance of information sharing, with regards to risks to users, and recommended service providers share information with specific actors or organisations. Several stakeholders recommended that service providers share information pertaining to risks to users including:

a) image sharing and how this impacts risks to users;[483]
b) recommender algorithms;[484]
c) exploitation of service providers' tools and functionalities;[485]
d) safety incidents;[486] and
e) summaries of risk assessments.[487]

5.122 We also received input from stakeholders regarding the sharing of these types of information with relevant actors. One stakeholder highlighted the importance of publishing reports requested by Ofcom, citing specifically "law enforcement could benefit from an understanding of these reports, where they may focus on certain issues, measures or successes that service providers are seeing, to support potential targeting of resources and focus".[488] Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales indicated that the Guidance should encourage service providers to engage with national and local strategic need assessment processes, and wider information sharing processes to inform prevalence data, cost analysis and service design.[489]

---

[482] Response(s) to February 2025 consultation: British and Irish Law and Education and Technology Association (BILETA), p.5.
[483] Response(s) to February 2025 consultation: Moonshot, p.5.
[484] Response(s) to February 2025 consultation: Kira, B., Asser, Z. and Ruiz, J., p.11; Institute for Strategic Dialogue (ISD), p.12-13; Equality Now, p.2; Collective Shout, p.19.
[485] Response(s) to February 2025 consultation: Centre for Protecting Women Online, p.14.
[486] Response(s) to February 2025 consultation: Women's Aid Federation of England, p.6.
[487] Response(s) to February 2025 consultation: The Cyber Helpline, p.3; End Violence Against Women Coalition (EVAW), p,10.
[488] Response(s) to February 2025 consultation: Association of Police and Crime Commissioners, p.2.
[489] Response(s) to February 2025 consultation: Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.8.

5.123 Several stakeholders indicated that information pertaining to transparency should be shared with support services or organisations.[490] In addition, several stakeholders also noted that service providers should share information with other service providers. For example, stakeholders suggested this could enable cross-platform coordination, evidence collection and improve understandings of the patterns of harm, in particular for offences like stalking.[491]

#### Our final decision

5.124 We have added a good practice step proposing that:

a) Service providers share information, to the extent relevant and at an appropriate level of detail, on the emerging risks to users with key actors involved in prevention, such as civil society, law enforcement, and researchers.

5.125 This good practice step directly responds to stakeholder feedback, including the need to share information between relevant actors on emerging risks to users.

5.126 However, we have decided not to recommend service providers share information with other providers due to the likely operational risks and challenges related to platform or account level data-sharing (e.g. lack of infrastructure, privacy). However, if service providers choose to share information, we recommend safeguards (in the 'Exercise caution' good practice step) to facilitate the sharing of information in a responsible manner. We have also included signposting to relevant resources published by the ICO on data sharing.[492]

### Sharing information about additional assessments (See Action 2) and the effectiveness of measures

#### Summary of stakeholder feedback

5.127 We received feedback noting that there is a gap in the transparency reporting requirements with regards to how algorithmic tools and recommender systems contribute to violence against women and girls online.[493] This stakeholder further expressed a view that transparency measures should focus not only on the use of technologies to moderate content but also how those tools facilitate a culture of violence against women and girls online.[494]

#### Our final decision

5.128 We have included a new good practice step proposing that:

a) Service providers share information regarding additional assessments undertaken (see **Action 2**) and the effectiveness of measures in place to address online gender-based harms. For example, sharing the outcomes of algorithmic evaluations to allow researchers and civil society to better understand how these systems work and the risks of bias and discrimination.

---

[490] Response(s) to February 2025 consultation: NSPCC, p.18; Institute for Strategic Dialogue (ISD) p.10; The Cyber Helpline p.3.

[491] Response(s) to February 2025 consultation: Institute for Strategic Dialogue (ISD), p.10; Suzy Lamplugh Trust, p.4; End Violence Against Women Coalition (EVAW), p.3; Johnstone, E., p.7.

[492] We added the following footnote to this step in the Guidance: "More information on data privacy risks and complying with the requirements of data protection law can be found here. See also the ICO's Data sharing: a code of practice".

[493] Response(s) to February 2025 consultation: Kira, B. Asser, Z. and Ruiz, J., p.12.

[494] Response(s) to February 2025 consultation: Kira, B. Asser, Z. and Ruiz, J., p.12.

5.129 This decision aims to align with, and complement, the good practice step under **Action 2** that recommends service providers conduct additional assessments. This means that service providers would need to share information regarding any additional assessments on users' self-expression, freedom from discrimination and privacy, including on their algorithmic processes and systems.

## Ensuring that published information and findings are clear and accessible

### Summary of stakeholder feedback

5.130 We received stakeholder responses on the accessibility of information published by service providers. One stakeholder indicated that transparency should extend to explaining user options, including that women and girls should be able to easily find information on how to adjust settings or get help if abused.[495] Similarly, Bolt Burden Kemp LLP indicated that transparency data needs to be "digestible" for "users, parents, carers, local authorities and schools".[496] The Welsh Government also expressed concern that transparency reporting should be accessible to users, including being easily found, read and understood, particularly for youth.[497] Another stakeholder indicated that users require access to "clear information about how their data is used in safety interventions and retain control over their personal information. This needs to be understandable to young people independently, and to adults responsible for caring for children".[498]

5.131 Two stakeholders suggested this information is published on an online dashboard to maximise accessibility.[499] For example, the Institute for Strategic Dialogue indicated that the regular updates on transparency metrics should be communicated via a dashboard.[500] Similarly, Equality Now indicated that "Ofcom should also require platforms to adopt real-time transparency mechanisms, such as live dashboards or regularly update public metrics, particularly for high-risk content categories like image-based abuse and harassment".[501]

5.132 We also received feedback from two stakeholders that called for more regular publication of information.[502] One stakeholder suggested that "it would be helpful if the guidance set out how often companies will be expected to publish" the transparency data.[503] They suggested that service providers "proactively publish their data at regular intervals rather than await a request from Ofcom".[504] Similarly, the Institute for Strategic Dialogue (ISD) indicated that service providers should "publish regular updates on metrics such as time to removal, prevalence of abuse against public figures, and algorithmic exposure to misogynistic content — disaggregated by gender where possible".[505]

---

[495] Response(s) to February 2025 consultation: British and Irish Law, Education and Technology Association (BILETA), p.5.
[496] Response(s) to February 2025 consultation: Bolt Burden Kemp LLP, p.3.
[497] Response(s) to February 2025 consultation: Welsh Government, p.4.
[498] Response(s) to February 2025 consultation: Do-Ngoc, T. and Carmel, E., p.7.
[499] Response(s) to February 2025 consultation: Equality Now, p.4; Institute for Strategic Dialogue (ISD), p.12.
[500] Response(s) to February 2025 consultation: Institute for Strategic Dialogue (ISD), p.12.
[501] Response(s) to February 2025 consultation: Equality Now, p.4
[502] Response(s) to February 2025 consultation: Bolt Burden and Kemp LLP, p.3; Institute for Strategic Dialogue (ISD), p.12.
[503] Response(s) to February 2025 consultation: Bolt Burden and Kemp LLP, p.3.
[504] Response(s) to February 2025 consultation: Bolt Burden and Kemp LLP, p.3
[505] Response(s) to February 2025 consultation: Institute for Strategic Dialogue (ISD), p.12.

#### Our final decision

5.133 We have added a new good practice step proposing that:

a) Service providers ensure transparency reports are accessible to a range of audiences. For example, service providers may consider publishing different versions of the transparency reports that are tailored to specific audiences including children and young people. This should also include making sure information is well contextualised and explained so people are able to accurately interpret the findings.

5.134 We have added this good practice in response to stakeholder feedback that suggested accessible information being available to a range of actors, including having sufficient context to accurately interpret the data, is important for transparency reporting.

5.135 We also note the issues stakeholders raised on working with service providers and organisations to disseminate transparency information. This new good practice will encourage greater public access to information about service providers, which will improve organisations' (including those identified by stakeholders, such as safeguarding organisations, users and law enforcement) access to this information.

# Action 4: Conduct abusability evaluations and product testing

## Overall approach and foundational steps

### What we proposed

5.136 At consultation, we proposed that providers use product testing methods called abusability evaluations or 'red teaming' to anticipate and prevent abuse of users. We included foundational steps on:

a) Product testing (draft case study 6)
b) Significant change risk assessment
c) Recommender system testing

### Summary of stakeholder feedback

5.137 We received general feedback in support of this **Action 4**.[506]

5.138 However, some stakeholders called for more standardised or quality assured models for product testing evaluations,[507] such as cybersecurity 'maturity models'.

5.139 Other stakeholders wanted us to include more types of testing including "A/B testing" to understand how changes in design can increase risk[508] and product testing of age verification and age restricted features.[509] In contrast, a stakeholder noted that "both

[506] Response(s) to our February 2025 consultation: British and Irish Law, Education, and Technology Association (BILETA), p.5; Commissioner Designate for Victims of Crime for Northern Ireland, p.4; Gender + Tech Research Lab Department of Computer Science, p.3; Heriot-Watt University - University of Edinburgh, p.3; Internet Matters, p.13; Johnstone, E, p.2; Lucy Faithful Foundation, p.3; Match Group, p.3; The Cyber Helpline, p.4; Welsh Government, p.3; Ofcom Stakeholder Roundtable, Belfast, 8 May 2025.
[507] Response(s) to our February 2025 consultation: Centre for Protecting Women Online; Women's Aid Federation of England, p.8; The Cyber Helpline, p.4
[508] Response(s) to our February 2025 consultation: 5Rights Foundation, p.7.
[509] Response(s) to our February 2025 consultation: Children First, p.5; Yoti, p.1.

evaluations and product testing could vary by service, product, feature etc. Being overly prescriptive may hinder innovation and stifle security and progress".[510]

5.140 We also received feedback suggesting abusability testing should include metaverse, AR/ VR and smart home technologies, and specific functions such as autoplay, search and GenAI.[511]

5.141 More specifically, one stakeholder asked that we expand the scope of the foundational step on recommender system testing and recommend providers evaluate whether their algorithmic systems are likely to increase "exposure to 'harmful,' 'borderline,' or 'violative' content, not just illegal content".[512]

5.142 Another stakeholder called for us to discuss further how product design can deter abuse in the case study on abusability testing,[513] for example recommender connection lists can be used by stalkers to identify victims across different sites.[514]

### Our final decision

5.143 We are confirming our position at consultation to include **Action 4** on abusability and product testing.

5.144 **We are also confirming the inclusion of the foundational steps set out in paragraph 5.136 in this statement.** We have clarified that the foundational step on recommender system testing is for user-to-user services.

5.145 We have not recommended testing age verification as it is outside the core focus of our Guidance, however we have previously set out our expectations for highly effective age assurance for Part 3 services.

5.146 We acknowledge that abusability testing could be applied to other services and technologies. For example, where GenAI services which fall under the definition of user-to-user services and search services in the Act are in scope of this Guidance. However, we have not incorporated smart home technologies where such technology is beyond the scope of the Act. This is line with our position in paragraph 3.29 in this statement setting out which services are in scope of this Guidance.

5.147 **We updated Case study 7 on abusability testing**. In line with the general changes we have made to case studies set out in paragraphs 5.20-5.22 in this statement, the amended case study looks at a social media provider tackling pile-ons and coordinated harassment. We also moved the case study to sit with the good practice steps.

## Good practice steps in Action 4

5.148 At consultation we proposed six good practice steps in **Action 4**. This included:

a) Using red teaming (draft case study 7)
b) Working with experts
c) Using personas

---

[510] Response(s) to our February 2025 consultation: Meta Platforms Inc, p.7,
[511] Response(s) to our February 2025 consultation: Gender + Tech Research Lab Department of Computer Science, p.4; The Cyber Helpline, p.4.
[512] Response(s) to February 2025 consultation: Integrity Institute, Council on Technology & Social Cohesion, University of Southern California, Marshall School Neely Center, p.3.
[513] Response(s) to February 2025 consultation: End Violence Against Women Coalition (EVAW), p.12.
[514] Response(s) to February 2025 consultation: Suzy Lamplugh Trust, p.7.

d) Media literacy

## Using red teaming and working with experts

### Summary of stakeholder feedback

5.149 **Red teaming:** Several stakeholders noted that conducting red teaming exercises successfully, service providers need to stay up to date with research on perpetrator behaviour.[515] One stakeholder suggested that civil society and researchers should have greater access to raw data on red teaming to assess the process.[516] Another stakeholder argued red teaming should be used to test how features may chill lawful speech.[517]

5.150 We also received feedback on the case study (draft case study 7) on red teaming for deepfake intimate image abuse. Stakeholders welcomed the recommendation that AI models need safeguards against intimate image abuse.[518] One stakeholder suggested references to deepfakes should highlight AI-generated child abuse images and AI-generated images for sextortion.[519] Another stakeholder questioned whether it would be possible to ban large language model (LLM) developers from using images not verified as consensual to train LLMs.[520] We also received feedback that suggested we adopt an "medium or creation agnostic" approach to the generation of intimate image abuse, as AI may be surpassed by other technologies in the future.[521]

5.151 **Working with experts:** Many stakeholders were supportive of the proposed good practice step on working with experts[522] although there were calls to strengthen the language,[523] and ensure experts are fairly compensated for their work.[524] Many stakeholders recommended including victim survivors and diverse users in abusability testing.[525]

### Our final decision

5.152 We are confirming the inclusion of the two good practice steps. However, we have made minor amendments.

5.153 **Red teaming**: We have not recommended encouraging greater access to raw data in red teaming as detailed information can be misused. However, we propose that providers share evidence on emerging trends and risks in **Action 3**. We also have not recommended red teaming to test how features may chill lawful speech as we consider the good practice step on conducting additional assessments (see **Action 2**) is more appropriate for this purpose.

---

[515] Response(s) to February 2025 consultation: [✂]; Heriot-Watt University - University of Edinburgh, p.9.
[516] Response(s) to February 2025 consultation: Integrity Institute, Council on Technology & Social Cohesion, University of Southern California, Marshall School Neely Center, p.4.
[517] Response(s) to February 2025 consultation: Free Speech Union, p.7.
[518] Response(s) to February 2025 consultation: [✂]; Women in Tech Policy Network, p.20
[519] Response(s) to February 2025 consultation: Association of Police and Crime Commissioners, p.2.
[520] Ofcom / Baroness Owen of Alderley Edge Meeting, 3 July 2025.
[521] Response(s) to February 2025 consultation: Classification Office, p.2.
[522] Response(s) to February 2025 consultation: End Violence Against Women Coalition (EVAW), p.12; Johnstone, E. p.2; Integrity Institute, Council on Technology & Social Cohesion, University of Southern California, Marshall School Neely Center, p.4; Mayor of London, p.9; University of Southampton, Lancaster University, University of Liverpool, Queen Mary University of London, p.3; White Ribbon UK, p.3; Women's Aid Federation of England, p.8.
[523] Response(s) to February 2025 consultation: Johnstone, E, p.2; Refuge Annex, p.13; Suzy Lamplugh Trust, p.4.
[524] Response(s) to February 2025 consultation: White Ribbon UK, p.3.
[525] Response(s) to February 2025 consultation: British and Irish Law, Education, and Technology Association (BILETA), p.6; End Violence Against Women Coalition (EVAW), p.12; Galop, p.2.

We have also added a new good practice step on quality assurance for product testing to emphasise the importance of standardised, robust procedures.

5.154 **We have updated Case Study 8 on red teaming**. In line with the general changes we have made to case studies set out in paragraphs 5.20-5.22 in this statement, the amended case study explores how a large general search provider can conduct a red teaming exercise to help identify vulnerabilities in its GenAI summary feature. We also note that the Government has announced upcoming legislation that will allow designated bodies to scrutinise AI models to check they cannot be exploited to generate CSAM, extreme pornography and non-consensual intimate images.[526] To ensure we do not cut across this live legislative work, the case study now focuses on red teaming for harmful user queries.

5.155 **Working with experts:** We have emphasised that engaging with experts can enable providers to stay up to date with perpetrator tactics which evolve quickly. We have also linked this good practice step with **Case study 3** on engaging with subject-matter experts (see paragraphs in 5.50 in this statement).

## Using personas and media literacy

### Summary of stakeholder feedback

5.156 **Using personas:** The use of personas was supported by some stakeholders as a way to introduce intersectionality,[527] but another stakeholder argued personas bring biases and simplify a complex group to an average user. They suggested we refer to the user experience term 'user journeys' instead.[528]

5.157 **Media literacy:** One stakeholder was supportive of the reference to the Best Practice Design Principles for Media Literacy, with some noting media literacy needs to be delivered alongside comprehensive education programmes.[529] Another stakeholder supported the use of media literacy as part of a prevention and education strategy .[530] We also received feedback that suggested Ofcom's Best Practice Design Principles for Media Literacy lack ambition, detail and clarity, and that better media literacy is needed for all users, not just children.[531]

### Our final decision

5.158 We are confirming our position at consultation to include good practice steps on using personas and media literacy. We have made some minor changes to respond to stakeholder feedback:

a) **Using personas:** We have highlighted that personas can map user journeys.
b) **Media literacy:** As noted in **Action 1** (paragraph 5.57 in this statement), we have emphasised that media literacy interventions can be particularly important and valuable for children and young adults. We are retaining our position that it is helpful and

[526] See Department for Science, Innovation and Technology, Liz Kendall MP, and Jess Phillips, MP, 2025. New law to tackle AI child abuse images at source as reports more than double. [accessed 12 November 2025]
[527] Response(s) to February 2025 consultation: Gender + Tech Research Lab Department of Computer Science, p.4.
[528] Response(s) to February 2025 consultation: Integrity Institute; Council on Technology & Social Cohesion; University of Southern California, Marshall School Neely Center, p.5.
[529] Response(s) to our February 2025 consultation: Girlguiding, p.8-9.
[530] Response(s) to our February 2025 consultation: Mayor of London, p.10-11.
[531] Response(s) to February 2025 consultation: End Violence Against Women Coalition (EVAW), p.8.

relevant to signpost providers to the Best Practice Principles for Media Literacy Design as it can promote critical and informed use of a service.

# Action 5: Set safer defaults

## Overall approach

### What we proposed

5.159 At consultation, we proposed that providers embed safer defaults in their service design to encourage safer behaviour by making their services less susceptible to abuse. We included foundational steps on:

a) Safe settings (Case study 8)
b) Group chats
c) Supportive information
d) Safe search

### Summary of stakeholder feedback

5.160 The majority of stakeholders, including civil society, front-line specialists, academia, public sector organisations, and individuals expressed support for our proposals on safer default settings.[532] However, other stakeholders cautioned that relying on settings places the onus on women and girls to protect themselves from harm depending on which settings they have on. Some stakeholders argued there should be a greater focus on frictions for those perpetrating harm.[533]

5.161 A small number of stakeholders suggested the foundational steps on default settings apply to all users.[534] We address this feedback in paragraph 3.45 in this statement.

5.162 Some stakeholders noted that defaults settings must balance safety with robust protections on freedom of expression and privacy, including where default settings are not clearly explained to users.[535] For example, Parity said that they support safer defaults where they do not compromise user autonomy and are gender-neutral, however "there should be caution regarding measures that require additional personal data to access accounts, as these could disproportionately infringe on privacy rights."[536] Several stakeholders noted strong default settings can prevent users from benefitting from online services and may reduce the visibility of women in public life and user engagement.[537] Another stakeholder

[532] Response(s) to our February 2025 Consultation: British and Irish Law, Education and Technology Association (BILETA), p.6; End Violence Against Women Coalition (EVAW), p.12; Institute for Strategic Dialogue (ISD), p.7; Lucy Faithfull Foundation, p.3; Refuge, p.12; Suzy Lamplugh Trust, p.4, 7; Welsh Government, p.4; The Cyber Helpline, p.4; Women's Aid Federation Northern Ireland, p.4; Gender + Tech Research Lab Department of Computer Science, p.4; Heriot-Watt University – University of Edinburgh, p.3; Integrity Institute, Council on Technology & Social Cohesion, University of Southern California, Marshall School Neely Center, p.5; Age Check Certification Scheme, p.1; Girlguiding, p. 9; Internet Matters, p.13.
[533] Response(s) to our February 2025 Consultation: South West Grid for Learning (SWGfL), p.8; End Violence Against Women Coalition (EVAW), p.12.; Refuge Annex, p.14; White Ribbon UK, p.3; Lucy Faithfull Foundation, p.3; Ofcom Stakeholder Roundtable, Belfast, 8 May 2025.
[534] Response(s) to our February 2025 Consultation: Suzy Lamplugh Trust, p.7; [✂].
[535] Response(s) to our February 2025 Consultation: Free Speech Union, p.9-10.; [✂]; Evans, M.I., p.3.
[536] Response(s) to our February 2025 Consultation: Parity, p.6;
[537] Response(s) to our February 2025 Consultation: Institute for Strategic Dialogue (ISD), p.7; British and Irish Law, Education and Technology Association (BILETA), p.7; Meta Platforms Inc, p.8.

indicated that Ofcom should "coordinate with the ICO as needed, to ensure consistency between safety by design and privacy by design principles."[538] The ICO considered that strong default settings enhance the protection of users' personal information in addition to contributing to their online safety.[539]

### Our final decision

5.163 **We are confirming our position at consultation to include Action 5 on safer defaults.** We have amended the introduction to the action to highlight that safer defaults can be a powerful tool when complemented with the harm prevention methods set out in **Action 6**. This is in line with our safety-by-design approach, which encourages services to draw from good practice steps across the nine actions. We have also highlighted that safer defaults can reduce the 'safety work' experienced by survivors and victims in the action introduction.

5.164 We are confirming our position at consultation on the inclusion of the foundational steps set out in 5.159 in this statement.

5.165 In line with the general changes we have made to case studies, including replacing foundational case studies on CSEA explained in paragraph 5.22 in this statement, we have replaced draft case study 8 on preventing grooming through safer defaults with case studies on good practice. We have also incorporated guidance and feedback from the ICO across the good practice steps as explained below.

## Good practice steps in Action 5

### What we proposed

5.166 At consultation we proposed six good practice steps in **Action 5**. This included:

a) Interaction defaults
b) Privacy defaults (draft case study 9)
c) Bundles
d) Strengthening account security
e) Account access
f) Reminders

### Interaction defaults, privacy defaults and bundles

#### Stakeholder feedback

5.167 We received minimal feedback on the interaction defaults good practice step. More generally, several stakeholders noted that default settings should be set to the highest bar of protection with options to lower them,[540] particularly for children as they're less likely to change the default setting,[541] with some suggesting age tiering apply to different groups.[542]

[538] Response(s) to our February 2025 consultation: British and Irish Law, Education and Technology Association (BILETA), p.7
[539] Response(s) to our February 2025 consultation: Information Commissioner's Office (ICO), p.7.
[540] Response(s) to our February 2025 consultation: Suzy Lamplugh Trust, p.7; End Violence Against Women Coalition (EVAW), p.12; Ofcom Stakeholder Roundtable, Cardiff, 1 May 2025.
[541] Response(s) to our February 2025 consultation: NSPCC, 14; Ofcom Stakeholder Roundtable, Belfast, 8 May 2025.
[542] Ofcom Stakeholder Roundtable, Belfast, 8 May 2025.

5.168 Several stakeholders expressed support for **Case study 9** on removing geolocation information by default),[543] and suggested that providers introduce regular reminders to users when they are sharing their location**.** [544]

5.169 The ICO said that Ofcom's good practice steps aligned with their guidance on Article 25 of the UK GDPR,[545] which requires systems, services, and practices to prioritise the safeguarding of personal information by creating a 'privacy by design and default' approach. They noted the reference to their Children's Code and to advocating for limiting location-sharing opportunities, disabling geolocation by default, and providing clear warnings when location tracking is active. They said that these measures contribute to the online safety of women and girls and enhance the protection of their personal information.

5.170 Many respondents were supportive of bundles,[546] but some raised concerns that bundles may limit user agency, including children, to customise settings.[547] The ICO also noted that bundles should be clearly explained to users, including information about data processing.[548]

5.171 A small number of stakeholders raised concerns that bundles could impact freedom of expression. For example, the British and Irish Technology, Law, and Education Association (BILETA) recommended defaults should "not silence users' outgoing expression" and should focus on intrusions like unwanted messages, tracking and tagging.[549] The Free Speech Union raised concerns that, given the evidence cited in this action included content defaults, expanding bundles to content controls could lead to suppression of "lawful speech, particularly where that speech forms part of ongoing social or political debate."[550]

5.172 The ICO raised concerns about the step concerning bundled privacy settings, noting that while bundling privacy settings may seem time-efficient, it is important to recognise that this approach could increase the risks of users not being fully informed about how their personal information is processed or the significance of the choices they make regarding their data.[551] They said that if providers are considering implementing bundled privacy settings, they should adhere to the transparency principle outlined in Article 5(1)(a) of the UK GDPR, as well as the requirement to provide individuals with specific privacy information set out in Articles 13 and 14. They suggested signposting to a number of ICO

---

[543] Response(s) to our February 2025 consultation: Children First, p. 6; Bolt Burden Kemp LLP, p. 2.
[544] Response(s) to our February 2025 consultation: Integrity Institute, Council on Technology & Social Cohesion, University of Southern California, Marshall School Neely Center, p. 5.
[545] Data protection by design and default | ICO
[546] Responses to our February 2025 Consultation: Office of the Derbyshire Police and Crime Commissioner, p.2. University of York, p. 6; Welsh Women's Aid, p.5; Women's Aid Federation of England, p.8-9; Refuge Annex, p.15.
[547] Response(s) to our February 2025 consultation: Cybersafe Scotland, p.2; Bolt Burden Kemp LLP, p. 3.
[548] Response(s) to our February 2025 consultation: Information Commissioner's Office (ICO), p. 8.
[549] Response(s) to our February 2025 consultation: British and Irish Law, Education, and Technology Association (BILETA), p.7.
[550] Response(s) to our February 2025 consultation: Free Speech Union, p.9.
[551] They said that if transparency information is vague or non-specific, users may struggle to grasp how their data is used, shared, or processed. They noted that Article 12 of the UK GDPR requires controllers to provide information about data processing in a concise, transparent, intelligible, and easily accessible format, using clear and plain language. See response(s) to our February 2025 consultation: The Information Commissioner's Office (ICO), p.8.

guidance documents to assist providers to comply with their data protection and privacy obligations concerning bundling and consent.[552]

### Our final decision

5.173 We are confirming the inclusion of the good practice steps set out in paragraph 5.166 in this statement, but have made minor changes.

5.174 In the good practice introduction, we have highlighted the impact safety defaults settings can have when the highest option is pre-selected. Under both good practice steps on interaction and privacy defaults, we have noted that adults should have the ability to change their settings. We consider these additions strike the right balance that safer defaults can be a powerful safety measure while providing adult users with flexibility to change these settings and control how they participate online.

5.175 **Interaction defaults:** In regard to the good practice step on interaction defaults, we have maintained our position set out at consultation and explicitly acknowledge that adults should have the ability to change their settings.

5.176 **Privacy defaults:** We have added location settings as an example under the good practice step on privacy defaults to draw out the link between this good practice and **Case study 9.** We have updated **Case study 9** in line with changes set out in in paragraphs 5.20-5.22 in this statement. The amended case study looks at how a social media service provider can reduce the risk of stalking through location data by switching off geolocation options by default. We have also signposted to the ICO Age Appropriate Design Code.

5.177 **Bundles:** We have clarified that poorly designed bundles may undermine user agency or increase the risk of poor data processing. With this change, we have emphasised the need for clear explanation and data protection compliance to address the privacy and data protection concerns raised by stakeholders. We have maintained our position that providers should offer customisation to allow users to make more granular choices outside of the bundles. We have also highlighted that adults should be able to change their interaction settings and privacy defaults. We consider our approach to sufficiently balance the benefits of bundles and the importance of user agency. We have also signposted to the ICO guidance on right to be informed, transparency, default settings, valid consent under UK GDPR and the ICO and CMA joint paper on harmful design.

5.178 While we acknowledge concerns about impacts on the right to freedom of expression from bundles that may supress particular types of content, we do not recommend bundling for any kinds of content controls. We have clarified that bundles apply to interaction and privacy defaults. Further, as noted in **Section 4** of this document, we have clarified the scope of online gender-based harms. We therefore do not consider that this good practice step risks infringing upon the right to freedom of expression by restricting upon lawful speech, particularly where that speech forms part of ongoing social or political debate.

[552] These were: ICO's guidance on the right to be informed (to help service providers understand the necessary measures to ensure users are clear on how their data is used); The ICO and CMA's joint paper on harmful design (which warns that bundled consent is more likely to be invalid than granular consent options, as it often lacks specificity and fails to ensure users are fully informed— potentially violating the "lawfulness" requirement under Article 5(1)(a)); The ICO's consent guidance (which emphasises the importance of offering granular consent options for different processing purposes, unless doing so would be unduly disruptive or confusing.)

## Account security and account access

### Summary of stakeholder feedback

5.179 On strengthening account security, the ICO noted that services must ensure that data processing is adequate, relevant, and limited to what is necessary, in compliance with data protection law. The ICO signposted to their guidance on data minimisation as a resource for services to consider when implementing this good practice step and they said the step aligned closely with their guidance on data security. [553] A small number of stakeholders welcomed the inclusion of the good practice step on two- or multi-factor authentication feature,[554] but highlighted how it can be bypassed by motivated perpetrators.[555]

5.180 On account access, Refuge suggest that providers should provide account access information to survivors and to relevant law enforcement agencies about the use of technology which is causing harms; and that reminders should include easy-to-understand language with options for translation.[556]

### Our final decision

5.181 We have retained the good practice step on strengthening account security. We have incorporated stakeholder feedback by adding reference in the good practice step to ICO guidance that emphasises the importance of strong authentication when personal data is involved. We have also highlighted the need to provide advice to users about protecting their data and for providers to understand how authentication can be bypassed by determined perpetrators.

5.182 We have added in detail to the good practice step on account access that information about access can support survivors and victims in putting together a case if nonconsensual monitoring occurs. We have also signposted to the ICO guidance on data minimisation.

5.183 As explained above in the feedback on our overall approach – we have included a good practice step on clear communication to address stakeholder feedback about easy-to-understand language.

## Reminders and additional feedback

### Summary of stakeholder feedback

5.184 Refuge noted the importance of providing information in a variety of formats, using simple language and easily accessible translate options.[557]

5.185 The Cyber Helpline suggested that providers consult with subject-matter experts when designing default settings.[558] Many stakeholders said that default settings should be

[553] Response(s) to our February 2025 consultation: Information Commissioner's Office (ICO), p.9.
[554] Response(s) to our February 2025 consultation: British and Irish Law, Education and Technology Association (BILETA), p. 17-18; Refuge Annex, p. 14.
[555] Response(s) to our February 2025 consultation: Refuge Annex, p.14.
[556] Response(s) to our February 2025 consultation: Refuge Annex, p.17.
[557] Response(s) to our February 2025 consultation: Refuge Annex, p.17.
[558] Response(s) to our February 2025 consultation: The Cyber Helpline, p. 4.

accessible and easy to use, including for vulnerable users.[559] A few stakeholders noted that users should be informed when settings change.[560]

5.186 We also received a range of suggestions for additional settings, including disabling, restricting or discouraging functionalities or features like disappearing photos, video calling, or highly gendered avatars. Other suggestions included hiding user bios (which we consider falls under privacy default) and notifying users when they are tagged in content or if their content is screenshotted. [561]

### Our final decision

5.187 **We are confirming the inclusion of a good practice step on reminders, but have made minor changes.** We have added that the reminders should be in easy-to-understand language and that providers should have regard to the needs of their UK user base in considering what languages are needed or available to ensure the reminders are accessible.

5.188 We considered stakeholder suggestions on expanding the good practice steps and suggestions to add new steps. **We have added three new good practice steps in line with stakeholder feedback:**

a) Engaging with subject matter experts particularly those with experience supporting survivors and victims, when designing privacy and security settings. We have signposted to **Case study 3** which set outs considerations for service providers when engaging with expert organisations. We further explain our rationale for engaging with subject matter experts in paragraph 5.48 in this statement. We have also noted that providers should consult ICO resources to support organisations to consider data privacy and security.
b) Clear communication because we recognise that default settings and bundles should be clearly explained to all users, including when these settings change.
c) Notification settings, such as notification when a user is tagged in another user's content, and location sharing. We recognise that people experiencing gender-based harms, in particular stalking and coercive control, need to be informed when other users' activity has an impact on their online presence, for example when they are tagged in another user's content. We also acknowledge that users should control how they participate online.

5.189 We are not proposing that providers disable specific functionalities, such as disappearing photos, video calling, or highly gendered-avatars, as this is out of scope of **Action 5** which focuses on privacy and safety settings. We encourage providers to conduct abusability evaluations to determine how a feature can enable online gender-based harms and introduce safer settings to mitigate these risks.

---

[559] Response(s) to our February 2025 consultation: Refuge, p. 12; British and Irish Law, Education and Technology Association (BILETA), p.7; Are, C, p. 3; Gender + Tech Research Lab Department of Computer Science, p. 4; Heriot Watt University – University of Edinburgh, p. 10; Ofcom Stakeholder Roundtable, Cardiff, 1 May 2025

[560] Response(s) to our February 2025 consultation: The Cyber Helpline, p. 4; Suzy Lamplugh Trust, p.4; Ofcom Stakeholder Roundtable, Cardiff, 1 May 2025.

[561] Response(s) to our February 2025 consultation: CyberSafe Scotland, p.3; Yoti, p.1; Girlguiding, p.7, 10; Harrison, J, p.3; Pinterest, p.3; [✂]; Internet Matters, p. 13, Children First, p.6; NSPCC, p.19-22.

# Action 6: Reduce the circulation of content depicting, promoting or encouraging online gender-based harms

## Overall approach

### What we proposed

5.190 At consultation, we proposed that providers could reduce the spread of online gender-based harms, which can reduce the burden on those reporting content and limit impact of second-hand exposure from such content.

5.191 We also included a range of good practice which include automated detection. We organised these under three main methods: persuasion (supportive or deterrence messaging), removal (preventing uploads or taking down content), or reduction (limiting circulation or reducing visibility). We explained that providers should choose which methods are most appropriate given the type of service and content being addressed.

### Summary of stakeholder feedback

5.192 Many stakeholders were supportive of this action.[562] Several stakeholders called for the action to be strengthened,[563] for example by applying measures on content harmful to children to adults as well.[564] Other stakeholders asked us to address the root causes of misogyny or develop a more comprehensive prevention and education strategy on issues such as bystanders, challenging harmful narratives, healthy relationships and consent, and digital safety.[565] The Cyber Helpline emphasised need for safeguards to avoid driving online gender-based harms "more underground to platforms that create a stronger echo-chamber and more extremist communities."[566]

5.193 Some stakeholders argued that 'prevention' is an inaccurate description for the action as they consider prevention only occurs before content upload.[567]

5.194 Meta Platforms Inc urged Ofcom to adopt a "flexible approach when guiding services to reduce potentially disagreeable content and acknowledge the unique challenges and opportunities presented by different services and technologies." They said that users have the right to engage in discourse on potentially controversial topics as long as they do not violate platform policies.[568] BILETA said that "Action 6 is sufficient in outline and

[562] Response(s) to our February 2025 Consultation: Engendering Change, p.1; Refuge Annex, p.17; The Cyber Helpline, p.4; the four Welsh Office of Police and Crime Commissioners, p.4.
[563] Response(s) to our February 2025 Consultation: Clean Up the Internet, p.2; End Violence Against Women Coalition (EVAW), p.4; Heriot-Watt University - University of Edinburgh, p.10.; Kira, B. Asser, Z. Ruiz, J., p.6; Plan International UK, p.12; South West Grid for Learning (SWGfL), p.8
[564] Response(s) to our February 2025 Consultation: End Violence Against Women Coalition (EVAW), p.13; Plan International UK, p.12.
[565] Response(s) to our February 2025 Consultation: Association of Police and Crime Commissioners, p.2; Heriot-Watt University – University of Edinburgh, p.6; Mayor of London, p.2.; Plan International UK, p.14; Belfast Area Domestic & Sexual Violence and Abuse Partnership, p.1; End Violence Against Women Coalition (EVAW), p.7; Refuge, p.4; [✂]; Ofcom Stakeholder Roundtable, Edinburgh, 22 April 2025; Ofcom Stakeholder Roundtable, Cardiff, 1 May 2025.
[566] Response(s) to our February 2025 consultation: The Cyber Helpline, p.5.
[567] Response(s) to our February 2025 Consultation: End Violence Against Women Coalition (EVAW), p.7; End Violence Against Women Coalition (EVAW) Annex 1, p.9. Ofcom Stakeholder Roundtable, Edinburgh, 22 April 2025.
[568] Response(s) to our February 2025 consultation: Meta Platforms Inc, p.8.

technologically feasible, but its implementation must tread carefully on free expression" and "it should focus on genuinely abusive or contextually harmful spread (such as dog-piled harassment or non-consensual images) and be transparent and adjustable."[569] TikTok emphasised the importance of giving users the opportunity to share freely, however they noted that "free expression is not an absolute right – it is always considered in proportion to its potential harm and does not extend to having your content recommended in the For You feed."[570]

5.195 Other stakeholders said that **Action 6** steps raised freedom of expression concerns, including in relation to online gender-based harms being too broadly or vaguely defined (see **Section 4**).[571] Stakeholders also commented on freedom of expression concerns, in particular in relation to removal and reduction. These are summarised under the relevant sections below.

## Our final decision

5.196 **We are confirming our position at consultation to include Action 6.** We have shortened the introduction to focus on setting out our objectives and providers' duties. We have clarified that, in line with our position in **Section 3** in this statement, providers can choose to allow legal but harmful content for adults such as violent content in their terms of service.

5.197 We agree that designing effective content moderation processes for gender-based harms requires collaborative action, including parents, carers, and educators. Beyond the Guidance, we engage with different groups, including through our media literacy work.[572]

5.198 We have also made changes to our overall approach to good practice under **Action 6** in response to feedback freedom of expression. We have specified which harms (as clarified and defined in **Section 4**) apply to which of the three good practice methods we focus on to ensure proportionate approach:

a) **Persuasion:** These steps can be taken to address all four harm areas. This is because persuasion does not block users from posting or encountering content. Instead, these methods aim to encourage people to reflect on their actions. Ultimately, people can override persuasive methods, and therefore we consider it proportionate to apply to online gender-based harms in the round.
b) **Removal:** These steps only apply to illegal content and activity (stalking and coercive control and image-based sexual abuse). We note that providers may use removal techniques on content which violates terms of service.[573]
c) **Reduction:** These steps can be taken to address all four harm areas where content and activity is not clearly illegal.[574] This is because, as with persuasion, these techniques do not block or remove content. Instead, they aim to reduce exposure to online gender-

[569] Response(s) to our February 2025 consultation: British and Irish Law, Education and Technology Association (BILETA), p.8.
[570] Response(s) to our February 2025 consultation: TikTok, p.2
[571] Response(s) to our February 2025 consultation: Free Speech Union, p.3; [✂]; Evans, M.I., p.3, p.5; Parity, p.6, p.9; [✂]; [✂]; LGB Alliance, p. 3-4.
[572] For more information on our Media Literacy work, see Ofcom's three-year media literacy strategy, published in April 2024.
[573] We did not specify what service providers' terms of service should regulate, but rather review how they can enforce the policies they set out in their terms of service (see Setting Policies under Action 1).
[574] As noted in the Legal Annex (**Annex A2**), all known illegal content must be swiftly removed.

based harms, especially those not seeking out such content. However, we recognise the risks where reduction is blunt, inconsistent or not clearly explained to users, and we have amended relevant good practice steps (and added additional steps) to address these risks.

5.199 This action sets out good practice steps that can enable providers to address the circulation of illegal content, content harmful to children, and content which violates their terms of service. As we note in the Guidance, it is up to providers to decide which steps are most appropriate for the type of content they are targeting, including in line with their safety duties (see Legal Annex (**Annex A2**)) and duties concerning freedom of expression (see paragraph 5.30 in this statement). We believe providers should be clear and transparent with people about the content they may be exposed to (see **Action 1** and **Action 3**).

## Foundational steps in Action 6

### What we proposed

5.200 At consultation, we included foundational steps on:

a) Automated content moderation, including hash matching for CSAM (draft case study 10)
b) Recommender systems (draft case study 11)
c) Search moderation (draft case study 12)
d) CSAM warnings for search
e) Highly effective age assurance
f) Signposting children to support

### Summary of stakeholder feedback

5.201 Most of the relevant feedback for foundational steps and draft case studies 10-12 focused on recommender systems (including draft case study 11). Many stakeholders emphasised or provided evidence about the importance of addressing misogynistic content amplified by recommender algorithms, including the link with business models.[575] One stakeholder cautioned against overfocusing on 'misogynistic influencers' as other forms of misogynistic content circulate on children's feeds.[576]

5.202 Several stakeholders called for this case study to go further, for example by preventing rather than reducing such content in children's feeds.[577] The Information Commissioner's Office suggested signposting to their guidance on AI and Fairness in relation to the case study on recommender systems.[578]

5.203 As explained under **Action 2**, we also received feedback requesting that risk assessments include information on algorithms.

[575] Response(s) to our February 2025 consultation: Women's Aid Federation of England, p.14; Classification Office, p.4; Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales , p.9; The Minderoo Centre for Technology and Democracy at the University of Cambridge, p.4.
[576] Response(s) to our February 2025 consultation: Cybersafe Scotland, p.4
[577] Response(s) to our February 2025 consultation: Women's Aid Federation of England, p.9; Cybersafe Scotland, p.5
[578] Response(s) to our February 2025 consultation: The Information Commissioner's Office (ICO), p.12-13.

### Our final decision

5.204 **We are confirming our position at consultation on the inclusion of the foundational steps set out in 5.200 in this statement.** We have reordered the foundational steps to group together similar measures and have split content moderation and hash matching for CSAM into separate steps.

5.205 In line with our approach to case studies in paragraphs 5.20-5.22 in this statement, we have made the following changes:

a) Removed draft case study 10 on hash matching for CSAM. We have separately set out our expectations for how providers should use hash matching for CSAM in our Illegal Content Codes of Practice and continue to prioritise this via enforcement.[579]
b) Amende draft case study 11 (renumbered to **Case study 10**) to focus on how a video sharing service provider can evaluate and retrain its recommender systems to reduce the promotion of misogynistic abuse and sexual violence to children.[580] We have added information including on the ICO's AI and Fairness guidance, the role of media literacy, and record keeping in line with stakeholder feedback. We have not expanded this case study to include content beyond that set out under the Act as harmful to children in line with our Codes. We have also not referenced business models in this case study as this is addressed under risk assessments (**Action 2**).
c) Moved draft case study 12 under good practice (renumbered to **Case study 13**, see paragraph 5.250 in this statement)

## Automated detection

### What we proposed

5.206 At consultation, we noted that many foundational and good practice steps to reduce the circulation of content specified will rely on automated detection techniques to scan, identify, and filter content depicting online gender-based harms. We included **Case study 15** on automated detection of misogynoir. Drawing on our broader work on proactive technology,[581] we set out it is important that automated detection is:

a) Accurate, effective, contextually nuanced and minimises bias
b) Continually evaluated and improved to reduce risks of both over- and under-detecting
c) Effective for different kinds of formats

[579] In March 2025, we launched an enforcement programme to assess the measures being taken by providers of file-sharing and file-storage services that present risks of harm to UK users from image-based CSAM. The enforcement programme remains open as of November 2025, and we will continue our work in this area as part of tackling the dissemination of CSAM.
[580] User-to-user services should ensure that children's recommender feeds exclude or limit the prominence of content harmful to children, which may also involve undertaking algorithmic assessments.
[581] We have set out a principles-based approach when recommending proactive technology to detect or support the detection of target illegal content and/or content harmful to children in the Additional Safety Measures consultation. In having regard to accuracy, effectiveness and lack of bias, we have developed proactive technology criteria that we propose should be met when providers are sourcing, developing, and/or assessing existing proactive technology. These criteria are designed to ensure that proactive technology is sufficiently accurate, effective and free from bias while giving providers the flexibility to assess and, if appropriate, deploy the right proactive technology for their service. For more information, see para 9.9 – 9.16 in our consultation on Additional Safety Measures.

## Summary of stakeholder feedback

5.207 Several stakeholders supported the use of automated detection but called for it to be strengthened. One stakeholders calling for automated blocking of content such as sharing of porn sites, adult chatbots, and nudification sites in spaces that can be accessed by children. [582] Others highlighted the importance of improving automated detection such as efficacy for different formats such as livestreaming, non-text content like emojis, and GenAI content,[583] ensuring capture of coded, implicit or changing language,[584] as well as repetition and patterns, as content in isolation may not seem harmful.[585] A stakeholder suggested that content moderation capacities should be adapted for the Welsh language.[586] Further, stakeholders called for changes in algorithmic design (for example, moving away from engagement-based algorithms), the inclusion of algorithmic audits or testing (see in paragraph 5.92 in statement), or using bots to detect and mitigate harms.[587]

5.208 TikTok emphasised that "while automation plays a key role, we recognise the critical value of human review."[588] Others noted the importance of hybrid automated and human content moderation, with some calling for it to be recognised as good practice.[589] One stakeholder said that there should be a framework mandating systemic testing, justification and continuous evaluation of automated detection approaches.[590]

5.209 Several stakeholders raised freedom of expression concerns related to automated detection. BILETA recommended further guidance on how moderation practices and "free speech considerations" should interact with automated content moderation systems, given the potential for bias in these systems to either fail to detect harmful content targeting women and girls or unfairly censor their speech.[591] The Free Speech Union said, "while automation may be effective for removing clearly illegal content, it also brings the danger of blunt enforcement, especially where the definition of harm is vague, subjective or culturally contingent."[592] For example, as noted at in paragraph 4.66 in this statement, some stakeholders raised concerns about over-moderation of people sharing information about women's health or testimonies of sexual violence.

---

[582] Response(s) to our February 2025 consultation: Internet Matters, p.14.
[583] Response(s) to our February 2025 consultation: NSPCC, p.21; Refuge Annex, p.23; Ofcom / Young People's Action Group Roundtable, 7 July 2025.
[584] Response(s) to our February 2025 consultation: Do-Ngoc, T., Carmel, E., p.3; The Minderoo Centre for Technology and Democracy at the University of Cambridge, p.1; Children First, p.7; University of Southampton; Lancaster University; University of Liverpool; Queen Mary University of London, p.8; Refuge Annex, p. 23; University of Portsmouth, p. 3-4.
[585] Response(s) to our February 2025 consultation: Johnstone, E., p. 6-7; Suzy Lamplugh Trust, p.4.
[586] Response(s) to our February 2025 consultation: [✂]; Harrison, J., 16.
[587] Response(s) to our February 2025 consultation: Integrity Institute; Council on Technology & Social Cohesion; University of Southern California, Marshall School Neely Center, p.7; Centre to End All Sexual Exploitation (CEASE), p. 6; Welsh Government, p.1; Heriot-Watt University - University of Edinburgh, p.1.
[588] Response(s) to our February 2025 consultation: TikTok, p.4
[589] Response(s) to our February 2025 consultation: Pinterest, p.3; Refuge, p.5; Do-Ngoc, T., Carmel, E., p.4; University of Southampton; Lancaster University; University of Liverpool; Queen Mary University of London, p.8-9.
[590] Response(s) to our February 2025 consultation: Centre for Protecting Women Online, p.20.
[591] Response(s) to our February 2025 consultation: British and Irish Law, Education, and Technology Association (BILETA), p.22.
[592] Response(s) to our February 2025 consultation: Free Speech Union, p.11.

5.210 A stakeholder flagged other risks from automated detection and AI driven safety tools, including burden of implementation for smaller providers, false positives, limitations in identifying nuanced content, over-reliance on automation, and bias.[593]

5.211 Others noted data privacy concerns. One stakeholder said that "while automated monitoring tools may help flag harmful content, their deployment should always be accompanied by transparency, accountability, and strict data minimisation practices" and noted that such techniques must not enable the surveillance of users, especially marginalised groups.[594] The ICO noted the need to comply with data protection law when using content moderation technologies and processes and asked us to signpost its guidance on this matter.[595]

5.212 Several stakeholders welcomed draft case study 15 (now **Case study 14**), with some calling for more specific or practical recommendations, and further consideration of the impact on Black women when the engage in counter speech.[596]

## Our final decision

5.213 We have strengthened and clarified our proposals on good practice for automated detection.[597] Changes include:

a) Emphasising the role of evaluation for verifying and assessing the efficacy of an automated detection, including accounting for nuance and cultural context. We have not added a good practice step on algorithmic audits here as this is covered in **Action 2**.
b) Adding details on training algorithms, including new evidence on large language models.
c) Clarifying that efficacy of detection for different formats includes livestreaming.
d) Adding information on safeguards for freedom of expression, including routes to contest wrongly moderated content and the role of human moderation. We recognise the risks of over- and under- moderation from ineffective automated detection, and we consider this addition to support a proportionate use of these technologies.

5.214 Further, as set out in **Section 4**, we have also clarified the scope of harms we cover across the Guidance to ensure a proportionate approach to online gender-based harms, without hindering the ability of users to share legitimate criticisms or engage in debate.

---

[593] Response(s) to our February 2025 consultation: British and Irish Law, Education, and Technology Association (BILETA), p.16, p.22; [✂].
[594] Response(s) to our February 2025 consultation: Dgo-Ngoc, T., Carmel, E., p.6-7.
[595] In particular, they said this will help providers to determine whether they are making solely automated decisions within their content moderation systems and whether these decisions are likely to have legal or similarly significant effects on users. They pointed out that if such conditions apply, the additional provisions of Article 22 of the UK GDPR will govern the data processing. Response(s) to our February 2025 consultation: The Information Commissioner's Office (ICO), p.10.
[596] Response(s) to our February 2025 consultation: Victims Commissioner and Domestic Abuse Commissioner, p. 4; End Violence Against Women Coalition (EVAW) Annex 1, p.12; Glitch, p.4; British and Irish Law, Education and Technology Association (BILETA), p.6.
[597] At the time of publication, Ofcom's consultation on Additional Safety Measures has closed, and we are carefully considering responses. It includes proposed Codes measures on assessing the role that automated tools can play in detecting a wider range of content, including child abuse material, fraudulent content and content promoting suicide and self-harm, and implementing new technology where it is available and effective. As the proposals are currently at draft stage, we have included this as part of the good practice steps for now. We will reflect the outcomes of this consultation in future updates to this Guidance. Consultation: Online Safety - Additional Safety Measures - Ofcom.

5.215 We have also updated draft case study 15 (now **Case study 14**) on automated detection of misogynoir, in line with our position in paragraphs 5.20-5.22 in this statement. The case study now focuses on practical ways a social media provider can improve its detection of misogynoir, accounting for nuance and context. We also highlight issues raised by stakeholders under considerations, including preventing over-moderation (e.g. survivors speaking about their experiences), efficacy for different languages (which can cover the Welsh language), and data protection laws.

5.216 We acknowledge the data protection and privacy concerns raised and consider that the additional signposting and guidance for service providers on data protection and privacy will ensure that any risk of interference with users' right to privacy will be appropriately mitigated and will ensure that providers are aware of cross cutting issues concerning data privacy.

5.217 We also acknowledge that automated detection can have significant freedom of expression implications, including from false positives where that results in content which does not violate providers' terms of service being removed or otherwise reduced in terms of visibility, as we have explained in detail in our Additional Safety Measures consultation.[598] However, we consider that given the volume of gender-based harms online, automated detection remains an important technique to address content and activity disproportionately affecting women and girls. We consider that our good practice for this area, which is voluntary and not required for compliance with the safety duties, provided it is deployed with appropriate safeguards as noted in our Guidance, can provide important protections for the safety of women and girls, and others affected by these harms. As to any comments which also apply to measures we have recommended in our Additional Safety Measures consultation, we will consider these in preparing our statement and making any changes to our Codes and may revisit our Guidance in light of what we decide if appropriate.

## Good practice steps in Action 6: Persuasion

### What we proposed

5.218 At consultation, we said that methods using persuasion can be more respectful of users' autonomy and help educate users, however they are less likely to be effective where perpetrators are highly motivated. We proposed the following good practice steps:

a) Nudges (draft case study 13)
b) Allowing users to verify their identity (included within draft case study 14 that looks at a range of persuasion and removal methods)

### Summary of stakeholder feedback

5.219 **Nudges:** Many stakeholders were supportive of this step and/or the associated case study.[599] Match Group explained how they use nudges to deter harmful behaviour on their

[598] Please see Chapters 8 and 9 (on Proactive Technology) of our Additional Safety Measures Consultation - Consultation Additional Safety Measures

[599] Response(s) to our February 2025 Consultation: Integrity Institute, Council on Technology & Social Cohesion, University of Southern California, Marshall School Nelly Center, p.8; Lucy Faithfull Foundation, p.4; Mayor of London, p.10; [✂]; British and Irish Law, Education and Technology Association (BILETA), p.8; Internet Matters, p.18. Ofcom / Men and Boys Roundtable, 29 May 2025.

apps, noting that Tinder users served a nudge changed their behaviour 17% of the time.[600] Pinterest noted they serve and signpost to supportive resources when users are searching for potentially harmful content.[601] However, some stakeholders expressed doubts about the effectiveness of nudges in certain contexts.[602] One stakeholder raised concerns that nudging, particularly if detected through automated detection, could "overreact to perfectly legal criticism of ideas" and deter people from expressing themselves.[603]

5.220 Others suggested a range of ways frictions can be strengthened to deter or support users such as A/B testing to optimise nudges for diverse user experiences, [604] using warnings, reminders or other pop-ups (such as educational pop-ups) when people use harmful words,[605] search for or view harmful content,[606] or engage in risky behaviours including unintentional sharing of personal information, [607] and educating users about respectful behaviour.[608] One stakeholder suggested frictions within account creation to prevent perpetrators from immediately creating new accounts. [609]

5.221 **Identity verification**: Some stakeholders called for this step to be strengthened,[610] for example through linking it with age verification,[611] removing options for anonymous accounts,[612] or linking to interaction controls.[613] Two stakeholders provided evidence that girls often call for stronger identity verification.[614] Others argued that, if ineffective, this

[600] Response(s) to our February 2025 consultation: Match Group, p.4: "*For example, our 'Are You Sure?' feature encourages a change in behaviour, aiming to prevent harm from occurring in the first place. These prompts were sent 250,000,000 times on Tinder in H1 2024. Users who received a prompt changed their behaviour 17% of the time.*"
[601] Response(s) to our February 2025 consultation: Pinterest, p. 4.
[602] Response(s) to our February 2025 consultation: Refuge Annex, p.18; Ofcom / Men and Boys Roundtable, 29 May 2025.
[603] Response(s) to our February 2025 consultation: LGB Alliance, p.3-4.
[604] Response(s) to our February 2025 consultation: Integrity Institute; Council on Technology & Social Cohesion; University of Southern California, Marshall School Neely Centre, p.8.
[605] Responses to our February 2025 Consultation: British and Irish Law, Education, and Technology Association (BILETA), p17; [✂].
[606] For example, the Lucy Faithfull Foundation suggested that once material is removed using hash-matching, instead of an Error 404 message, serve a warning to the user who tried to access the hashed image. See response to our February 2025 Consultation: Lucy Faithfull Foundation, p.4; End Violence Against Women and Girls Coalition (EVAW) suggested warnings for CSAM should be expanded to all searches for illegal content. See response to our February 2025 Consultation: End Violence Against Women and Girls Coalition (EVAW), p.13; During the Ofcom / Men and Boys Roundtable, 29 May 2025, stakeholders suggested serving users information explaining financial structures connected to influencers.
[607] For example, Young People's Action Group (YPAG) roundtable participants suggested warnings to prevent 'self-doxing' (posting of personal information) or prevent users consuming a lot of a particular type of content. NSPCC, p.20, suggested a similar use of warnings for children. Ofcom / Young People's Action Group Roundtable, 7 July 2025.
[608] Response(s) to our February 2025 Consultation: Image Angel, p.5.
[609] Response(s) to our February 2025 Consultation: Clean Up the Internet, p.2.
[610] Responses to our February 2025 Consultation: Yoti, p.1; Plan International, p.13; Welsh Government, p.4; Ofcom Stakeholder Roundtable, Belfast, 8 May 2025.
[611] Response(s) to our February 2025 Consultation: Welsh Government, p.4.
[612] Response(s) to our February 2025 Consultation: Engendering Change, p.2.
[613] Ofcom Stakeholder Roundtable, Belfast, 8 May 2025.
[614] Response(s) to our February 2025 consultation: Plan International UK, p.13; Girlguiding, p.7.

step could offer a false sense of security while putting users at risk.[615] The importance of explaining the purpose of identity verification to users was also noted.[616]

5.222 Further, several stakeholders noted privacy and data protection implications of this step, including the importance of anonymity, privacy for survivors and marginalised groups.[617] The ICO highlighted that identity verification may present significant privacy concerns, particularly for survivors and victims. They suggested that the good practice step and associated case study should direct service providers to the ICO's guide to UK GDPR to ensure their approach to implementing user verification is necessary, proportionate, and compliant with data protection law, and that particular consideration should be given to any processing of special category data like biometric face scans to uniquely identify a person. They also said that services should consider the data protection implications of restricting anonymity for users, including identifying and mitigating risks of harm or other detriment to users.[618] The ICO said it was concerned that services may misinterpret the suggestions in the case study focused on identity verification as a best practice for verification, potentially leading to excessive data collection for identity or consent verification purposes. [619] They suggested including links to relevant ICO guidance within the case study.

## Our final decision

5.223 We are confirming our proposals to include the two good practice steps in paragraph 5.218 in this statement. However, we have made some changes to our proposals.

5.224 **Nudges:** We have renamed the good practice step 'introducing deliberate frictions' to capture a wider range of techniques that providers can use. We have also added details on how frictions can be used by search services or providers offering search functionalities, including where search services integrate a large language model to generate text-based summaries of search results. Further, we have amended draft case study 13 (renumbered to **Case study 11**) to focus on a dating app deterring harmful behaviour and added considerations including how to ensure prompts are effective, and how they interact with education and media literacy initiatives.

5.225 As noted in paragraph 5.198 in this statement, we specify that these steps can be applied to all four harm areas. We acknowledge the concern from the LGB Alliance that frictions could interfere with expression of legal speech. We have addressed concerns about automated detection in paragraph 5.213 in this statement and have clarified that this good practice step and case study targets misogynistic abuse and sexual violence (see **Section 4**). While we recognise that frictions may not deter highly motivated perpetrators, and we acknowledge this in the Guidance, we consider that frictions serve a helpful purpose by asking people to reflect without blocking someone from participating online, which has

[615] Response(s) to our February 2025 consultation: Ofcom Stakeholder Roundtable, Edinburgh, 22 April 2025.
[616] Ofcom / Men and Boys Roundtable, 29 May 2025.
[617] Responses to our February 2025 Consultation: End Violence Against Women Coalition (EVAW), p.13; Refuge Annex, p.19; Women's Aid Federation of England, p.10; Chayn, p.3-4.
[618] Response(s) to our February 2025 consultation: The Information Commissioner's Office (ICO), p.14.
[619] They said that service providers to consider a range of options for their service before determining whether the proposed approaches set out in the case study are the appropriate and proportionate means of implementing the good practice step in the context of their specific service. This would help them to demonstrate that their personal information processing is necessary and proportionate.

been shown to prevent harm in some circumstances. We therefore consider that frictions are a proportionate step for us to highlight to protect people from violence and abuse.

5.226 **Allowing users to verify their identity.** We recognise the trade-offs with this good practice step, such as data protection considerations and the risks to survivors of stalking or coercive control who may wish to remain anonymous for their safety and have noted the complexity of this evidence base. However, we consider that giving users the option to verify their identity can be useful in certain situations, and therefore are retaining the step, but have made several changes. We explain the complexity of the evidence base, and that we will be considering details of identity verification in a future consultation.[620] To address the ICO's comments, we have added information about compliance with data protection and privacy rights and linked to guidance from the ICO both in the good practice step, and in draft case study 14 (renumbered to **Case study 12**).

5.227 We also have carefully considered the privacy concerns raised by stakeholders from identity verification processes. We consider that the additional signposting to ICO guidance will ensure that service providers are aware of cross cutting issues concerning data protection and privacy and that any risk of interference with users' right to privacy is appropriately mitigated.

## Good practice: steps in Action 6: Removal

### What we proposed

5.228 At consultation, we said that methods using removal refer to using technical tools to block uploads of harmful content, or to remove it after it has been uploaded. We acknowledged that removal can raise a variety of concerns related to a service provider's control over users' ability to express themselves freely. We proposed the following good practice steps:

a) Using hash matching to prevent known intimate image abuse content[621]
b) Requiring consent from those depicted in intimate content
c) Implementing prompt and output filters
d) Implementing time-out features

5.229 Draft case study 14 (now **Case study 12**) referenced hash matching and requiring consent as tools to prevent intimate image abuse (alongside identity verification).

### Summary of stakeholder feedback

5.230 As noted in paragraph 5.207 in this statement, we received feedback on removal techniques that rely on automated detection. Further, one stakeholder welcomed our position that providers may choose to remove violative content.[622] In addition, several industry respondents provided information about what content is prohibited in their policies, with some noting they remove violative content or operate a zero-tolerance policy for gender-based violence.[623]

---

[620] Phase 3 consultation: Duties on categorised services, incl. transparency, see Ofcom's approach to implementing the Online Safety Act

[621] Since the publication of the draft guidance, we have consulted on a measure on a draft Code of Practice covering the use of hash matching for intimate image abuse on user-to-user and search services. See Ofcom's Online Safety – Additional Safety Measures consultation for further information.

[622] Response(s) to our February 2025 consultation: University of Southampton; Lancaster University; University of Liverpool; Queen Mary University of London, p.4.

[623] Response(s) to our February 2025 consultation: TikTok, p.3; Pinterest, p.2; Bumble, p.10; Match Group, p.1.

5.231 The Free Speech Union said that "While the removal of clearly illegal content is a legitimate regulatory objective, we are concerned that the scope of this action – particularly as it relates to automated enforcement, undefined harms and expanding notions of "intimate image abuse" – risks entrenching a model of cultural censorship through technology."[624]

5.232 **Hash matching:** Many stakeholders welcomed recommendations related to hash-matching for intimate image abuse, with some calling for greater technological investment or research into efficacy.[625] Some stakeholders raised concerns about hash matching, for example limitations of tackling video content including deepfakes,[626]limited applicability for sex workers and others who wish to reuse their own content ,[627] ease of bypassing,[628] or noted that hash matching for NCII may not be an appropriate solution for all types of services, the technology is still in development and can have high rate of false positives.[629] One stakeholder also noted that the "same video across several platforms may be wrongly flagged and all videos will be deleted automatically."[630] More generally, stakeholders emphasised pairing or expanding hash matching with other approaches.[631]

5.233 **Requiring consent:** Several stakeholders[632] supported this step, with one saying it "can play a critical role in proactively preventing the circulation of non-consensual content, particularly on platforms hosting user-generated explicit material."[633] A stakeholder asked for clarity on the process of consent verification, including in relation to specific technologies like facial recognition.[634] As noted in paragraph 5.222 in this statement, the ICO raised the importance of compliance with data protection laws to verify consent, noting that Case study 14 could "potentially [lead] to excessive data collection for identity or consent verification purposes" particularly when considering how the technologies used to verify consent or identity incorporate the necessary safeguards.[635]

5.234 A number of stakeholders expressed support for prompt and output filters, or other removal and deterrence methods for tackling deepfake intimate image abuse.[636] One

[624] Response(s) to our February 2025 consultation: Free Speech Union, p.10.
[625] Response(s) to our February 2025 consultation: [✂]; Free Speech Union, p.10; End Violence Against Women Coalition (EVAW), p.18; TikTok, p.7; Kira, B. Asser, Z. Ruiz, J, p.13; The Cyber Helpline, p.4; Women's Aid Federation Northern Ireland, p.10; Refuge Annex, p.20; [✂].
[626] Response(s) to our February 2025 consultation: Do-Ngoc,T., Carmel,E., p.2.
[627] Response(s) to our February 2025 consultation: Image Angel, p.3.
[628] Response(s) to our February 2025 consultation: University of York, p.7-8; Do-Ngoc,T., Carmel,E., p.2; Image Angel, p.3; [✂].
[629] Response(s) to our February 2025 consultation: Mid-Size Platform Group, p.4; Bumble, p.8; Hammy Media Ltd/xHamster, p.3.
[630] Response(s) to our February 2025 consultation: Hammy Media Ltd/xHamster, p.3.
[631] Response(s) to our February 2025 consultation: University of York, p.7-8; Do-Ngoc,T., Carmel,E.,p.2; Image Angel, p.3; [✂]; Welsh Women's Aid, p.5
[632] Response(s) to our February 2025 consultation: Verifymy, p.2. Bolt Burden and Kemp LLP, p.4; [✂].
[633] Response(s) to our February 2025 consultation: Verifymy, p.2.
[634] Response(s) to our February 2025 consultation: [✂]; The Information Commissioner's Office (ICO), p.14.
[635] Response(s) to our February 2025 consultation: The Information Commissioner's Office (ICO), p.14.
[636] Response(s) to our February 2025 consultation: Refuge Annex, p.21; The four Welsh Office of Police and Crime Commissioners, p.4; [✂]; End Violence Against Women Coalition, p.4; Women's Aid Federation of England, p.13; Centre to End All Sexual Exploitation (CEASE), p.3.

stakeholder called for removal of nudity content from training datasets.[637] Others supported time-outs or temporary freezes for frequently reported or new users.[638]

## Our final decision

5.235 **We are confirming our proposals to include the four good practice steps.** As noted in paragraph 5.198 in this statement, we have narrowed the application of removal techniques to illegal content; this helps to address concerns about the impact of these techniques on freedom of expression. We note that providers may remove content violating their terms of service.

5.236 **Hash matching:** In June 2025 we published a consultation that included a proposal to add hash matching for intimate image abuse to our illegal harms Codes. We acknowledge the feedback on hash matching for intimate image abuse and will take into account this and other feedback before finalising our proposed codes measure. We have retained this as good practice step but may update this Guidance once we have taken the final decision on the inclusion of hash matching for intimate image abuse in our Codes.

5.237 **Requiring consent and draft case study 14:** In line with changes to case studies set out in paragraphs 5.20-5.22 in this statement and feedback from stakeholders, we have made several changes to draft case study 14 (renumbered **Case study 12**). The case study focuses on a pornography service provider taking a range of persuasion and removal steps to mitigate the risk of intimate image abuse including consent verification, deliberate frictions (in this case, deterrence messages) and hash matching for intimate image abuse through initiatives such as StopNCII.org to identify and block the upload of known intimate image abuse content. We layer multiple techniques together to respond to feedback on the importance of multiple mitigations. We do not specify specific techniques for consent verification, as providers can chose the most appropriate method in line with data protection laws. To emphasise this, we have also added a consideration within the case study with links to ICO guidance and data protection considerations noted by the ICO relevant to identity and consent verification. We have also added a consideration on applying good practice to different business models in the pornography industry.

5.238 We also recognise that removal methods in particular impact upon the right to freedom of expression. However, we consider our good practices under this step (including where steps rely on of automated detection, see paragraph 5.213 in this statement) to be an important tool to tackle harms against women and girls. We have limited the scope of our recommendations around removal to illegal gender-based harms such as intimate image abuse (see **Section 4**). As expressly noted in the Guidance, the right to freedom of expression is not absolute. Illegal content such as intimate image abuse impacts on other people's rights.

5.239 We also acknowledge the feedback about the potential privacy impacts related to the use of consent and identity verification. We consider that these techniques can support the reduction of intimate image abuse in some cases but highlight that such techniques (if they are implemented) must be implemented in line with data protection law. We consider the additional signposting to the ICO resources and guidance will ensure that providers are

[637] Response(s) to our February 2025 consultation: Women's Aid Federation of England, p.13.
[638] Response(s) to our February 2025 consultation: British and Irish Law, Education and Technology Association (BILETA), p.16-17; White Ribbon UK, p.3; Refuge Annex, p.20.

aware of cross cutting data privacy issues arising from this good practice and that any risk of interference with users' right to privacy will be appropriately mitigated.

## Good practice steps in Action 6: Reduction

### What we proposed

5.240 At consultation, we said that methods using reduction refers to limiting the circulation and visibility of content rather than removing it entirely. We noted it is increasingly commonplace among services that use content recommender algorithms, as well as search services which mediate the search results but cannot remove content from those sites. We proposed the following good practice steps:

a) Deprioritising harmful content in recommender algorithms
b) De-monetising content that is harmful but not clearly illegal
c) Removing links to dedicated sites hosting or generating non-consensual intimate images (draft case study 14)
d) Scanning for and delisting duplicates of known intimate image abuse content (draft case study 14)
e) Blurring nudity and harmful content

### Summary of stakeholder feedback

5.241 **Recommender algorithms, removing links, demonetisation:** Many stakeholders emphasised or provided evidence how online gender-based harms are amplified by recommender algorithms including to those not seeking out the content, with many noting the link between algorithms, engagement and business models.[639] For example, Welsh Women's Aid argued "while this content reaches women, this algorithm also floods men's feeds, fuelling misogynistic culture further."[640] In contrast, one stakeholder said that recommender systems are themselves not inherently harmful and can lead to reduced costs/ increased quality and greater efficiency, with "minimal antitrust issues when users can easily switch to another platform." However, they said they supported the ambition to protect vulnerable people from harm by preventing the recommendation and repetition of harmful content.[641]

5.242 Several stakeholders suggested ways to improve safety of content recommender algorithms. TikTok said that "content that does not meet our standards will be ineligible for the FYF [For You Feed]."[642] Some stakeholders recommended that user feeds (ads and user generated content) should be designed so that pornography does not appear automatically.[643] End Violence Against Women Coalition (EVAW) supported deprioritising

[639] Response(s) to our February 2025 consultation: Women's Aid Federation of England, p.13; Classification Office, p.3-4; Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.9; The Minderoo Centre for Technology and Democracy at the University of Cambridge, p.4; Centre to End All Sexual Exploitation (CEASE), p.3; End Violence Against Women and Girls Coalition (EVAW), p.4; Clean Up the Internet, p.2; Integrity Institute, Council on Technology & Social Cohesion, University of Southern California, Marshall School Neely Center, p.7. Ofcom / Men and Boys Roundtable, 29 May 2025. Ofcom Stakeholder Roundtable, Edinburgh, 22 April 2025.
[640] Response(s) to our February 2025 consultation: Welsh Women's Aid, p.2
[641] Response(s) to our February 2025 consultation: ACT the App Association, p.2
[642] Response(s) to our February 2025 consultation: TikTok, p.3.
[643] Response(s) to our February 2025 consultation: Mayor of London, p.24; Ofcom Advisory Committee for Scotland, p.3.

harmful content for all users in relation to harmful content unless they have actively searched for it.[644]

5.243 Designing algorithms that promote positive content or counternarratives was also suggested,[645] as well algorithms that "promote gender transformative content and diversity"[646] or amplify feminist content to dilute hateful narratives.[647]

5.244 Several stakeholders said that users should be made aware of any de-amplification or what triggers downranking to avoid perceptions of bias or censorship, including a suggestion that users have recourse if their content is actioned, in line with the EU's Digital Services Act.[648]

5.245 We received support for the demonetisation good practice step.[649] For example, one stakeholder said the "overall de-monetising approach, which is reinforced again in case study 13, is vital to combatting online gender-based harms and misogynistic content to ensure that users and platforms are not profiting from the abuse of women and girls."[650]

5.246 One stakeholder was concerned that some search engines rank search results relating to "deepfake pornography tools and sites" despite commitment to de-rank them.[651] Several stakeholders raised more general concerns about how links enable the circulation of online gender-based harms, in particular sites that allow for the creation and circulation of intimate image abuse.[652] Further, several stakeholders raised concerns about 'nudification' apps or links to sites dedicated to hosting intimate image abuse content, emphasising the need to reduce their promotion and availability.[653]

5.247 **Additional feedback:** Several stakeholders said blurring images is an effective method to prevent sharing or viewing explicit images, or more broadly welcomed the measure on blurring nudity.[654] Match Group noted the range of techniques they use to detect and take action against nudity, which is prohibited on their platform.[655]

5.248 Stakeholders gave feedback or provided evidence on introducing temporary limits on functionalities for new users or users who are frequently reported against, for example freezing posting rights or to reduce the circulation of online gender-based harms. [656] For example, the Integrity Institute provided evidence and examples of how a small but active number of users perpetuate misogyny online, suggesting that "To combat these bad actors,

---

[644] Response(s) to February 2025 consultation: End Violence Against Women Coalition (EVAW), p.13.
[645] Ofcom / Men and Boys Roundtable, 29 May 2025.
[646] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (EVAW), p.4
[647] Response(s) to our February 2025 consultation: British and Irish Law, Education, and Technology Association (BILETA), p.8.
[648] Response(s) to our February 2025 consultation: British and Irish Law, Education, and Technology Association (BILETA), p.8; The Cyber Helpline, p.8.
[649] Response(s) to our February 2025 consultation: Internet Matters, p.16; End Violence Against Women Coalition (EVAW), p.13-14; Refuge Annex p.22
[650] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (EVAW), p.13-14.
[651] Response to our February 2025 Consultation: Moonshot, p.6.
[652] Response(s) to our February 2025 consultation: Women's Aid Federation of England; Name Withheld 3, p.1;
[653] Response(s) to our February 2025 consultation: Internet Matters, p. 7-8; [✂]; End Violence Against Women Coalition (EVAW), p.4; Name Withheld 3, p.1; Internet Matters, p.8-9.
[654] Response(s) to our February 2025 consultation: Women's Aid Federation of England, p.10; Refuge Annex p.22; The Cyber Helpline, p. 9; [✂]; [✂].
[655] Response(s) to our February 2025 consultation: Match Group, p.2.
[656] Response(s) to our February 2025 consultation: Integrity Institute; Council on Technology & Social Cohesion; University of Southern California, Marshall School Neely Center, p. 7; British and Irish Law, Education, and Technology Association (BILETA), p.16-17; Welsh Government, p. 4.

Ofcom should include rate limits as a mitigation measure. "Rate limits, especially for new users, are a key tool to reduce the circulation of harmful content."[657]

## Our final decision

5.249 **We are confirming our position at consultation to include five good practice steps,** however in line with feedback from stakeholders we have made tweaks, for example to show how the steps can complement other actions. As noted in paragraph 5.198 in this statement, we recommend reduction can address content and activity that is not immediately able to be identified as illegal or violative,[658] and to reduce unmitigated or unwanted exposure to misogynistic abuse, sexual violence and pile-ons.

5.250 We have also added four new good practice steps under **Action 6**:

a) Designing recommender systems that promote content diversity and variety, to respond to feedback on amplifying a range of content and topics, including to prevent rabbit holes (i.e. funnelling users towards content of increasing thematic intensity).
b) Sharing information regarding what kinds of posts might trigger downranking, de-prioritisation, or exclusion. This is to incorporate feedback on transparency to mitigate perceptions of bias and censorship. We note in the Guidance, however, that this step should be carefully considered, as there may be instances where sharing this information could help malicious users bypass safety measures.
c) Reducing the prominence of misogynistic abuse and sexual violence in search results, for example by downranking such content or promoting content that is high-quality, yet relevant. In response to feedback on search services, we have also updated **Case study 13** to set out how a search service can take good practice steps (e.g. delisting and downranking) to reduce access to dedicated intimate image abuse sites.
d) Imposing rate limits (such as a limit of how many comments a user can make in a specific time period). This was recommended by stakeholders, and having considered the evidence and feedback provided, we agree it could help prevent pile-ons or other harms where perpetrators exploit features that allow continuous or high-volume activity.

5.251 We recognise the risks to freedom of expression where reduction methods are imprecise, inconsistent or not clearly explained to users. We have added good practice steps (and made amendments to steps proposed at consultation) to add safeguards:

a) The new good practice step on promotion of diverse content offers one way to reduce intensity of exposure to potentially harmful content, while still ensuring people can see different content (also noting user controls on what people see, which is discussed in **Action 7**).
b) Similarly, the new good practice step on sharing information regarding what kinds of posts might trigger downranking, de-prioritisation, or exclusion is to make sure people understand how their content may be actioned so users can make informed decisions, while also promoting consistency and accountability for services.
c) In line with position in **Section 4**, we have ensured a clearer definition of content and activity within scope of the Guidance. We cover reducing the amplification of

[657] Response(s) to our February 2025 consultation: Integrity Institute; Council on Technology & Social Cohesion; University of Southern California, Marshall School Neely Center, p. 7-9.
[658] Illegal content must be removed swiftly once a user-to-user provider is aware of it. Providers can choose what other content is prohibited for adults and how to action it.

misogynistic abuse and sexual violence in recommender systems and search results. We do not capture legitimate criticisms or debate within this scope.

5.252 While we acknowledge this can impact on other users' rights to freedom of expression if service providers choose to adopt this practice, we remain of the view that it is helpful to highlight these techniques as good practice to protect women and girls from the harms outlined (as well as other groups affected by gender-based harms) .

# Action 7: Give users better control over their experiences

## Overall approach and foundational steps

### What we proposed

5.253 At consultation, we proposed in this action that providers should consider that 'safety' may look different to those at risk of online gender-based harms and how safety needs can change over time. We included foundational steps on:

a) Blocking and muting
b) Disabling comments draft case study 15
c) Negative feedback
d) Group chats
e) Supportive information (draft case study 16)
f) Support materials

### Summary of stakeholder feedback

5.254 Many stakeholders supported the aims of **Action 7,** with some voicing experiences of frustrating design and use of user settings.[659] BILETA said "enhancing user control is generally positive for rights. It *advances privacy* (users decide who can interact with them and who sees their content) and *advances freedom of expression* in a nuanced way: it allows women to continue expressing themselves online while minimizing the exposure to hostile audiences."[660]

5.255 We also received specific feedback supporting the foundational steps on 'supportive information'[661] and 'enabling children to give negative feedback on content from a recommender system', [662] as well as the action's focus on user-centric design.[663]

5.256 Some stakeholders highlighted that platforms should prioritise accessibility and create easier user journeys for setting or changing user settings. [664] We also received feedback on

[659] Response(s) to our February 2025 consultation: University of York, p.7; Plan International UK, p.14; Refuge Annex, p.24; Welsh Government, p.4; Barker, K., p.8; Marie Collins Foundation, p.4.
[660] Response(s) to our February 2025 consultation: British and Irish Law, Education and Technology Association (BILETA), p.10.
[661]Response(s) to our February 2025 consultation: Girlguiding, p.9; Johnstone, E, p.7; Marie Collins Foundation, p.4; [✂]; Plan International UK, p.14; [✂]; Welsh Government, p.5.
[662] Response(s) to our February 2025 consultation: Girlguiding, p.7.
[663] Response(s) to our February 2025 consultation: British and Irish Law, Education, and Technology Association (BILETA), p.9.
[664] Response(s) to our February 2025 consultation: Children First, p.7; Plan International UK, p.14; Refuge Annex, p.24; Welsh Government, p.4; British and Irish Law, Education, and Technology Association (BILETA), p.9;

explaining more clearly that users should not face an undue burden for their own safety and making clear user settings were part of a wider picture of platform action.[665] Similar feedback was received on our **Action 5** on setting safer defaults (see paragraph 5.160 in this statement)

5.257 We also received feedback from several stakeholder asking us to include good or bad practices by specific services.[666]

5.258 One group of academic stakeholders queried the conclusion drawn in draft case study 16 on supportive information from the cited sources on signposting. They questioned if the claim that encountering supportive material was useful for all users, not just for those who had reported harmful content, was fully supported by the evidence cited.[667] One stakeholder also raised that the case study did not offer enough information on how civil society organisations inform supportive material.[668]

## Our final decision

5.259 **We are confirming our position at consultation to include Action 7 on giving users better control over their experiences. We are also confirming our position at consultation on the inclusion of the foundational steps set out in paragraph 5.253 in this statement. We have made minor changes to provide clarity.** To reflect stakeholder feedback on frustrating design and ease of use, including the importance of accessibility, we have added an additional footnote in the introduction to **Action 7** reminding providers of their obligations under other relevant legislation such as the EA 2010, as well as industry standards and good practice to ensure their services meet the access needs of disabled users. We have reworded our good practice step on supportive information to specify that this information should include explanatory resources on the most suitable user or privacy options for their needs, in line with the foundational steps on supportive information and support materials for this action which require this for children under our Protection of Children Codes. To address stakeholder concern about the burden on users, we have set out more clearly in the **Chapter 5** introduction that user controls are part of a wider picture of service action, and providers should not place an undue burden on users for their own safety. We have also added wording to **Case study 15** on blocking and muting to note clearly under considerations for providers that user controls form part of a wider picture of service action, and we also noted Ofcom's upcoming consultation on user empowerment duties.

5.260 We have not included examples of good or bad practices from specific services as suggested by stakeholders. We received related feedback on other parts of the Guidance and have explained our approach to case studies.

5.261 In line with our position set out in paragraphs 5.20-5.22 in this statement, we have replaced the foundational case study on supportive information which was in the draft guidance to focus on good practice case studies. We have retained the foundational step on supportive information and added clarification to the further good practice step on supportive

---

[665] Response(s) to our February 2025 consultation: [✂]; Suzy Lamplugh Trust, p.5; British and Irish Law, Education, and Technology Association (BILETA), p.9; Ofcom Stakeholder Roundtable, Edinburgh, 22 April 2025.

[666] Response(s) to our February 2025 consultation: NSPCC, p.17,18; The Cyber Helpline, p.9.

[667] Response(s) to our February 2025 consultation: University of Southampton, Lancaster University, University of Liverpool, Queen Mary University of London, p.9.

[668] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (EVAW), p.14.

information in this action to clarify our recommendation of signposting users to support when they provide negative feedback on content they have encountered to address stakeholder feedback on this issue. To ensure the harm area of misogynistic abuse and sexual violence is adequately considered within the case studies in **Chapter 5**, we have made changes to draft case study 18 (now **Case study 16**) on content filtering to be centred on this harm. We have also added references to Ofcom Behavioural Insights research on content filtering to strengthen the evidence supporting this suggestion.

## Good practice steps in Action 7

### What we proposed

5.262 At consultation, we proposed good practice steps on:

a) Visibility settings for content
b) Blocking and muting multiple accounts simultaneously (draft case study 17)
c) Filtering users who have not provided identity verification
d) User controls for content recommendations
e) User preferences and feedback on content (draft case study 18)
f) Supportive information on specific gender-based harms

### Summary of stakeholder feedback

5.263 We received several suggestions on our good practice steps on filtering users who have not completed identity verification and on supportive information, and both our foundational and good practice steps on blocking and muting. These suggestions included: that user verification status should be more visible,[669] consideration of the risk of user verification for victims of domestic violence who may need to use pseudonyms to protect their anonymity[670] and that platforms should support prepopulated block lists of known misogynistic content creators.[671]

5.264 One stakeholder suggested we could make draft case study 17 on mass-blocking more specific to pile-ons, and suggested centring on a woman in gaming.[672]

### Our final decision

5.265 **We are confirming our position at consultation to include the good practice steps set out in paragraph 5.265.** However, in line with feedback from stakeholders we have made tweaks to improve clarity. In response to stakeholder feedback on user verification, please see paragraph 5.221 under **Action 6** in this statement for further discussion of feedback on this topic.

5.266 In line with the changes, we have made to case studies set out in paragraphs 5.20-5.22 in this statement, we have combined draft case studies 15 and 17 (now **Case study 15**) due to their similar focus on user tools available for muting, blocking and disabling comments. We have focused this case study on women in public life facing pile-ons on a social media service.

---

[669] Response(s) to our February 2025 consultation: Clean Up the Internet, p.3.
[670] Response(s) to our February 2025 consultation: Women's Aid Federation of England, p.9.
[671] Response(s) to our February 2025 consultation: University of Southampton, Lancaster University, University of Liverpool, Queen Mary University of London, p.4.
[672] Response(s) to our February 2025 consultation: Flux Digital Policy, p.4.

5.267 We have not included the suggestion of prepopulated block lists, due to considerations of the practicality of this suggestion, particularly where it might involve service providers having to make a judgement of who would meet the criteria to be added to a pre-populated blocklist. We consider that our good practice steps on user control and blocking and muting already cover users' ability to exclude content or specific users.

## Additional feedback in Action 7

### Summary of stakeholder feedback

5.268 We received several additional suggestions for good practice in **Chapter 5**, including rate-limiting to prevent perpetrators repeatedly posting in a pile-on[673] and including the suggestion of "offering users functionality to see what the other user(s) see when they block or mute prior to making the decision".[674] One other stakeholder suggested similar functionality on previewing visibility settings.[675]

### Our final decision

5.269 We have included the suggestion on rate-limiting in **Action 6** and in **Case study 15** on customisable blocking and muting options. We have not included additional recommendations where there was a lack of existing evidence on their impact on improving user safety, such as previewing new user settings.

# Action 8: Enable users who experience online gender-based harms to make reports

## Overall approach and foundational steps

### What we proposed

5.270 At consultation, we proposed under **Action 8** that providers can encourage and enable users to make reports by designing reporting systems which are accessible, transparent, easy-to-use, and account for the specific dynamics of online gender-based harms. We included foundational steps on:

a) Complaints processes (draft case study 19)
b) Complaints systems (draft case study 20)
c) Complaints communications
d) Predictive search

### Summary of stakeholder feedback

5.271 We received a significant amount of stakeholder feedback on reporting, from across civil society, front-line specialists, academia, public sector organisations, law enforcement and individuals. Much of this feedback expressed frustration in existing reporting systems and shared first-hand experience of users having little confidence in providers' reporting

[673] Response(s) to our February 2025 consultation: Integrity Institute, Council on Technology & Social Cohesion, University of Southern California, Marshall School Neely Center, p.8.
[674] Response(s) to our February 2025 consultation: Refuge Annex, p.24.
[675] Response(s) to our February 2025 consultation: NSPCC, p.22.

systems and responses to reports (covered in **Action 9**). Many stakeholders expressed support for this action,[676] and our calls for embedding trauma-informed design.[677]

5.272 Several respondents called for us to address and clarify our expectations related to reporting categories across foundational and good practice steps. Stakeholders highlighted that reporting categories can be restrictive[678] and providers should have additional reporting categories for specific gender-based harms, including domestic abuse or stalking,[679] and allow people to "specify multiple grounds of discrimination".[680]

5.273 Stakeholders noted that perpetrators can maliciously use reporting systems to target women and girls by mass false reporting of accounts or posts.[681] For example, BILETA also noted that effective reporting mechanisms "could further freedom of expression for victims" and that processes must be designed to avoid bias or abuse.

5.274 Some stakeholders queried the use of the term 'gender-based' throughout this action, arguing it is ambiguous and could lead to over-censorship if users misinterpret what constitutes a gender-based harm online and therefore over-report content. We address the how we have defined 'online gender-based harm' in Section 4 in this statement.[682]

5.275 The ICO encouraged further consideration of how providers incorporate their UK GDPR obligations in reporting systems. They highlighted that where a user engages with a service provider as part of this process, there may be a possibility that they could exercise their data protection rights under UK GDPR at the same time. They gave the example of where a "user may complain about certain content on the platform and request its removal. This may qualify as a valid 'right to erasure' request under UK GDPR".[683] Another stakeholder noted that platforms should handle sensitive information (such as when sharing information on why content is abusive, which could reveal personal context) securely and "only use it for the purpose of addressing the report". They suggested offering the option to report anonymously.[684]

## Our final decision

5.276 We are confirming our position at consultation to include **Action 8** on reporting. We are confirming our position at consultation on the inclusion of the foundational steps set out in paragraph 5.273 in this statement. We have made minor changes.

---

[676] Response(s) to our February 2025 consultation: Welsh Government, p.5; Internet Matters, p.16, Girlguiding, p.7; Children's Commissioner for England's Office, p.5; Women's Aid Federation Northern Ireland, p.6; British and Irish Law, Education, and Technology Association (BILETA), p.10; Barker, K., p.8; Response(s) to our February 2025 consultation: The four Welsh Office of Police and Crime Commissioners, p.4.

[677] Response(s) to our February 2025 consultation: The Cyber Helpline, p.6; The four Welsh Office of Police and Crime Commissioners, p.4.

[678] Ofcom Stakeholder Roundtable, Cardiff, 1 May 2025

[679] Response(s) to our February 2025 consultation: Commissioner for Children and Young People (NICCY), p.12; Collective Shout, p.21; [✂]; Refuge Annex, p.29; End Violence Against Women Coalition (EVAW), p.14. Ofcom / Refuge's Survivor Panel, 10 June 2025.

[680] Response(s) to our February 2025 consultation: Antisemitism Policy Trust, p.4.

[681] Response(s) to our February 2025 consultation: British and Irish Law, Education, and Technology Association (BILETA), p.10; McLaughlan, M. Stevenson, S, p.4.

[682] Response(s) to our February 2025 consultation: [✂]; Evans, M.I., p.3; Parity, p.7; [✂].

[683] Response(s) to our February 2025 consultation: Information Commissioner's Office (ICO), p.10.

[684] Response(s) to our February 2025 consultation: British and Irish Law Education and Technology Association (BILETA), p.11.

5.277 We have clarified the introduction to the action to make it clear that having appropriate reporting categories and the ability for the user to add contextual information is crucial, and we specifically note the importance of this in the context of users reporting the harms of stalking and coercive control. We have also added an explicit reference to the relevance of context in the good practice step on incident reporting and in **Case study 23**, on coercive control training for moderation teams. Additionally, we emphasise the need to allow reporting of different types of media in **Case study 18** on reporting options and the need for dedicated reporting channels in good practice step. We have added new wording to the introduction to **Action 8** to suggest providers should consider the potential for malicious use of reporting systems to target women and girls when designing their reporting systems, and have included an additional evidence source on the prevalence of this harm.

5.278 To reflect the ICO and BILETA's suggestions, we have included an additional footnote in the action introduction to remind providers of their UK GDPR responsibilities and linked to the relevant ICO guidance on individual rights under the UK GDPR. We have also added further links to ICO guidance where relevant throughout **Action 8**. We consider that this addition will address the concerns related to privacy and data protection raised by stakeholders, and enable services to take the necessary steps to ensure compliance with data protection rights.

5.279 On points raised on anonymous reporting, we refer to the foundational step on complaints processes, which reference the Illegal Harms and Protection of Children Codes measures on allowing affected persons to make a relevant complaint (including a report) to a service (highlighted in **Case study 17**). All users, regardless of whether they are registered with a service, should be able to make various types of relevant complaints, including complaints about illegal content.

## Good practice steps in Action 8

5.280 At consultation, we proposed six good practice steps in **Action 8**. This included:

a) Report tracking (draft case study 21)
b) Incident reporting (draft case study 23)
c) Exit buttons:
d) Trusted flaggers (draft case study 22)
e) User feedback
f) Media literacy

### Report tracking and incident reporting

#### Summary of stakeholder feedback

5.281 We received feedback on our good practice steps on report tracking and incident reporting. Related to the wider feedback on **Action 8** noted above on reporting options, End Violence Against Women Coalition (EVAW) also suggested we further acknowledge victims being able to report multiple incidents at a time .[685]

5.282 We also received feedback on reporting incidents of offline abuse and the associated draft case study 21 (now **Case study 22**). The ICO raised that services will need to fully comply with their data protection obligations if they are taking the good practice step of incident reporting. The ICO said that we should ensure providers "take a data protection by design

[685] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (EVAW), p.14.

and default approach to the processing ensuring that necessary safeguards are integrated to protect the rights and freedoms of users" and recommended that the Guidance signpost to their guidance on criminal offence data. The ICO also queried use of the word 'investigate' in the off-service behaviour case study, with the concern it could incentivise service providers to carry out disproportionately intrusive checks.[686] The Scottish Government also asked us to clarify the possible data retention implications for the purposes of monitoring and reporting online and offline abuse.[687]

5.283 The ICO also provided comments that it is equally important for providers to recognise that all individuals involved in these reports—including survivors, reporters, and alleged perpetrators—retain their data protection rights. This includes access to their data, the ability to request corrections, and, in certain cases, the right to object or request erasure. They said that service providers must have robust processes in place to handle these requests fairly and efficiently and that fairness in data processing is essential, particularly if automated systems are used to analyse reports or determine enforcement actions. They said that any use of technology for this purpose must be transparent and free from bias and highlighted that their guidance on UK GDPR principles and automated decision-making and profiling can help services implement these measures responsibly.

5.284 Stakeholders supported our good practice step on tracking of reports[688] including the reporting dashboard in draft case study 21.[689]

### Our final decision

5.285 **We have retained the good practice steps on report tracking and incident reporting.** We have made changes to our good practice step on tracking reports and the case study on tracking and managing reports (**Case study 20**) on survivors and victims being able to share their report with third parties, including front line services and law enforcement. In line with the general changes we have made to case studies set out in paragraphs 5.20-5.22 in this statement, **Case study 20** now looks at a social media provider developing a report dashboard for its users. We have signposted to ICO guidance on subject access request and UK GDPR.

5.286 **We have also updated Case study 22 on off-service behaviour.** In line with the general changes we have made to case studies set out in paragraphs 5.20-5.22 in this statement, the amended case study looks at a livestreaming service provider addressing stalking. To address the concerns noted by the ICO, we have also made amendments to avoid the implication that service providers should investigate by way of disproportionately intrusive checks rather than simply to evaluate reports of off-service behaviour. To assist providers to comply with data protection obligations in connection with issues arising from this case study and associated good practice steps, we have added references to relevant ICO guidance. We consider that referencing ICO guidance will assist other stakeholders who queried the possible data retention consequences.

---

[686] Response(s) to our February 2025 consultation: Information Commissioner's Office (ICO), p.15.
[687] Response(s) to our February 2025 consultation: Scottish Government, p.4.
[688] Response(s) to our February 2025 consultation: Plan International UK, p.2; Ofcom Stakeholder Roundtable, Edinburgh, 22 April 2025; Ofcom Stakeholder Roundtable, Cardiff, 1 May 2025; Ofcom Stakeholder Roundtable, Belfast, 8 May 2025.
[689] Response(s) to our February 2025 consultation: The four Welsh Office of Police and Crime Commissioners, p.6. Integrity Institute, Council on Technology & Social Cohesion, University of South Carolina, Marshall School Neely Center, p.12.

## Other feedback on good practice

### Summary of stakeholder feedback

5.287 Several stakeholders voiced their support the inclusion of trusted flaggers as a good practice step.[690] Other stakeholders raised there can often be an imbalanced relationship between providers and frontline organisations.[691] One respondent queried whether trusted flagger relationships should be described as good practice, given trusted flagger relationships can put too much "onus on civil society to identify and report harm" rather than on service providers. They noted the reference to the VAWG Codes of Practice, which they contributed to, as evidence supporting this recommendation in the associated case study (draft case study 22).[692]

5.288 Several stakeholders commented on our good practice step on quick exit buttons, noting that users should be made aware of the limitations, particularly that all browsing history is not erased when an exit is made.[693]

### Our final decision

5.289 **We have retained our good practice steps set out in paragraph 5.283 in this statement**. We added an additional evidence source on the impact of trusted flagger programmes to reporting systems. We have added wording to the considerations in the case study on trusted flaggers (draft case study 22, now **Case study 21**) to underscore the need for clear criteria for what content trusted flagger organisations can report, and also added a consideration that trusted flaggers should be treated fairly and provided with necessary resource and support.

5.290 **We have retained our good practice step on quick exit buttons.** We have changed the reference cited on the impact of quick exit buttons to a more comprehensive source on the design choices and considerations that providers may wish to consider and made amendments to clarify that protecting the privacy of victims and survivors is the intention of this step.

## Feedback on law enforcement and evidence collection

### Summary of stakeholder feedback

5.291 Much of the additional feedback received on **Action 8** was on the relationship between providers' reporting systems and criminal reporting systems. Many stakeholders raised the issue of barriers they said that survivors and victims face when trying to collect evidence from platforms to share with third parties, such as frontline organisations or law enforcement.[694] Several stakeholders, including public bodies, civil society, and law enforcement, suggested that there should be links provided to law enforcement reporting

---

[690] Response(s) to our February 2025 consultation: Women's Aid Northern Ireland p.6, Chayn, p.4; Galop, p.2.
[691] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (EVAW), p.15; The Cyber Helpline, p.6; Refuge Annex, p.28; Office of the Derbyshire Police and Crime Commissioner, p.4; Women's Aid Federation of England, p.11; Ofcom Stakeholder Roundtable, Belfast, 8 May 2025; Ofcom / Young People's Action Group Roundtable, 7 July 2025.
[692] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (EVAW), p.15.
[693] Response(s) to our February 2025 consultation: The Cyber Helpline, p.5; Women's Aid Federation of England, p.11; Refuge Annex, p.27; Ofcom Stakeholder Roundtable, Cardiff, 1 May 2025.
[694] Response(s) to our February 2025 consultation: [✂]; The Cyber Helpline, p.7; Refuge Annex, p.56; End Violence Against Women Coalition (EVAW), p.3; Gender + Tech Research Lab Department of Computer Science, p.5; Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.7.

during reporting processes, or suggested an integration where reports could be forwarded to law enforcement systems.[695]

5.292 One stakeholder also raised the related need for more signposting to specialist support services during a reporting process.[696] Others provided different suggestions of what supportive information should be captured, including information on specific harms, that information should be UK specific, or localised for different regions of the UK,[697] links to further support from frontline organisations, and information on how to report a crime.[698]

### Our final decision

5.293 We have not included specific recommendations for services to automatically pass on reports to law enforcement, for example by including a forwarding mechanism in reporting systems. Integrating services' reporting processes with law enforcement could be technically challenging as law enforcement needs to keep the nature and capabilities of their reporting and wider technical systems private and secure. Such integration would also need to consider data protection laws and guidance from the ICO, particularly around sharing personal data with third parties. It would also mean that service providers would either have to assess which reports met a threshold for reporting to law enforcement, or pass on all reports made by users.

5.294 However, we recognise the evidence barriers that survivors and victims face with sharing information with law enforcement and frontline organisations, and acknowledge the range of stakeholders who raised this as an important issue for survivors of gender-based harms. We have added wording the good practice step on report tracking to highlight the need for users to share their reports more easily with frontline support organisations and law enforcement, if they wish to do so. In line with the general changes to case studies set out in paragraphs 5.20-5.22 in this statement, we have also updated **Case study 20** on tracking and managing reports, to highlight a scenario where victims and survivors are able to download and share reports with third parties. We have included a reference to the ICO's guidance in this case study, to make clear any sharing or downloading functionality must comply with existing data protection laws.

5.295 **We have further added a new good practice step on support during reporting**, where we suggest that providers signpost to supportive information during a report process where appropriate, including information about frontline support organisations and information on reporting a crime. We have added a footnote noting that providers should have regard to the needs of their UK user base in considering what languages are needed for supportive information shared with users.

---

[695] Response(s) to our February 2025 consultation: The Cyber Helpline, p.7; Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.7; [✂].

[696] Response(s) to our February 2025 consultation: The four Welsh Office of Police and Crime Commissioners, p.4

[697] Response(s) to our February 2025 consultation: Ofcom Advisory Committee for Scotland, p.5; Ofcom Stakeholder Roundtable, Cardiff, 1 May 2025.

[698] Response(s) to our February 2025 consultation: British and Irish Law, Education, and Technology Association (BILETA), p.10; Refuge Annex, p.26; Harrison, J., p.16; The four Welsh Office of Police and Crime Commissioners, p.4; Collective Shout, p.21; [✂].

## Additional feedback in Action 8

### Summary of stakeholder feedback

5.296 Stakeholders also raised additional points about the accessibility and design of reporting systems. For example, we received suggestions for improving the design of reporting systems through easy access to terms of service during reporting,[699] enabling voice note reports,[700] including a date range option to capture all communications from a particular account more easily,[701] better user feedback options during reporting.[702]

5.297 Some stakeholders raised the existing use of prompts or nudges to report,[703] the ability to speak to a human during a reporting process[704], or that we should recommend that a human moderator should always review reports,[705] and further considerations of children's experience with reporting tools.[706]

5.298 In relation to draft case study 19 on reporting as a non-user, Galop called for us to recognise that transgender people may face barriers to reporting if systems rely on pre-transition images .[707]

### Our final decision

5.299 In response to stakeholder feedback on accessibility and design and children's experience of reporting tools, we have added a new case study **(Case study 19)** which reflects several feedback points related to ease of use, clear communication and transparency during a reporting process. The case study centres a transparent user journey while reporting, including informing users on potential outcomes, as well as surfacing relevant policies and user feedback options to use in future design changes. We have also highlighted ICO guidance on UK GDPR and right to be informed.

5.300 In response to stakeholder suggestions on the use of nudges to report content, we have added an extra consideration to **Case study 11** on misogynistic abuse on a dating app, suggesting that a service provider could also consider introducing nudges or prompts on the opposite side of the user interaction, directing users towards reporting systems if abusive content is detected in a message they receive.

5.301 We have not included a good practice step that suggests providers must have human reviewers to interact with as part of a reporting process. We note that stakeholders referred to the need to speak to human moderators while reporting. To the extent that this suggests the need for a helpline or other live chat function, we have decided not to recommend this, as it is likely to involve significant costs and resourcing that would be prohibitive to smaller services. Other stakeholders referred to the need for involvement of human moderators more generally. We already acknowledge in our good practice step on moderator review in **Action 9** that gender-based harms are nuanced and highly contextual and so human moderators with specific training are likely to be highly effective in

---

[699] Ofcom Stakeholder Roundtable, Belfast, 8 May 2025.
[700] Ofcom / Refuge's Survivor Panel, 10 June 2025.
[701] Ofcom / Refuge's Survivor Panel, 10 June 2025.
[702] Ofcom Stakeholder Roundtable, Belfast, 8 May 2025; Ofcom Stakeholder Roundtable, Cardiff, 1 May 2025.
[703] Response(s) to our February 2025 consultation: Match Group, p.4; Women's Aid Federation of England, p.9, Ofcom / Young People's Action Group Roundtable, 7 July 2025.
[704] Response(s) to our February 2025 consultation: Galop, p.3; The Cyber Helpline p.5.
[705] Response(s) to our February 2025 consultation: Refuge Annex, p.30.
[706] Response(s) to our February 2025 consultation: CyberSafe Scotland, p.5; Children First, p.8; NSPCC, p.23.
[707] Response(s) to our February 2025 consultation: Galop, p.3.

addressing these. Certain types of reports (such as those with contextual information) may require human moderators, while automated moderation may be more effective in reviewing other complaints in a way that resolves them swiftly. Providers may consider various approaches to effectively manage reports based on their specific needs and circumstances, such as the size of their service. As we emphasise in our good practice steps on dedicated reporting channels and in our case studies on coercive control training (**Case study 23**) and external arbitration (**Case study 4**), providers should ensure both human and automated moderation systems account for the specifics of gender-based harms.

5.302 We have not included suggestions for additional reporting methods, such as voice note reporting, which lacked supporting evidence for improving the reporting process.

5.303 In line with the general changes we have made to case studies, set out in paragraphs 5.20-5.22 in this statement, the amended case study on affected persons (draft case study 19, now **Case study 17**) focuses on an adult content service provider enabling external reports of intimate image abuse. We have also made it clear that it is necessary for reporting systems to allow reporting on behalf of a victim and survivor to prevent re-traumatisation.

5.304 In response to Galop's feedback, we refer to the paragraph 5.282, where we note that the foundational step on reporting is that providers should allow affected persons to be able to report, regardless of whether they are an existing user and without having to register with the provider.

# Action 9: Respond appropriately when online gender-based harms occurs

## Overall approach and foundational steps

### What we proposed

5.305 At consultation, we proposed that providers can reduce the impact of online gender-based harms by taking appropriate action when it occurs on their service and that improving responses to user reports allows providers to better support women and girls who have experienced online gender-based harms. We included foundational steps on:

a) Taking action
b) Performance targets
c) Prioritisation
d) Moderation teams (draft case study 24)
e) Complaints
f) Appeals

### Summary of stakeholder feedback

5.306 Many stakeholders supported this action[708] and raised frustrations with providers not responding to reports, or response systems that did not appropriately handle the complexities of gender-based-harms.

5.307 Several stakeholders raised suggestions for the foundational step on moderator training, specifically what this training should include. Suggestions included: training on cultural

[708] Response(s) to our February 2025 consultation: The Cyber Helpline, p.9; Welsh Government, p.5; Barker, K., p.8; Refuge Annex p.30; Internet Matters, p.16.

sensitivity and LGBT+ harms,[709] nudification apps and incest pornography,[710] misogynistic attitudes and behaviours,[711] mental health training,[712] grooming and coercive and controlling behaviours.[713] Our roundtable with Young People's Action Group (YPAG) also suggested we should provide a glossary of key terms that teams could use to identify harmful content using coded language.[714]

5.308 Some stakeholders queried the use of the term 'gender-based' throughout this action, arguing it is ambiguous and could lead to over-censorship and impacts on the right to freedom of expression if users misinterpret what constitutes a gender-based harm online and therefore over-report content. We address the use of the term 'gender-based' in paragraph 4.12 in this statement.[715]

5.309 BILETA noted that freedom of expression rights are engaged when it comes to "punitive action" like content removal or account bans. The response also noted that appropriate action should always include an element of due process: "users who are penalized should be informed of what rule they violated and have an opportunity to appeal if they believe it, was a mistake."[716]

## Our final decision

5.310 **We are confirming our position at consultation to include Action 9** but have renamed this from 'Taking action when online gender-based harms occur' to 'Respond appropriately when online gender-based harms occur' to emphasise the importance of providers' responses to online gender-based harms being appropriate to the level of harm.

5.311 We are confirming our position at consultation on the inclusion of the foundational steps set out at 5.308. We have made minor changes.

5.312 We have not made changes to the foundational step on moderator training to reflect stakeholder feedback because this step reflects our existing measures from our Illegal Content and Protection of Children Codes. From paragraph 3.62, we address feedback that called for changes to our Codes measures.

5.313 Additionally, this Guidance is intended for different service types, and we expect that different service providers will have different needs for moderator training. Our view is it is not beneficial to be overly prescriptive in the Guidance on moderator training topics, especially with the risk that emerging harms might be overlooked. We suggest the best way for providers to stay up-to-date and include relevant topics on specific gender-based harms to be addressed is to work with specialist services and external experts to inform moderator training. We have included an example of working with organisations with frontline expertise in **Case study 23** on coercive control training for moderation teams (see **Case study 3** for further examples on engaging with external experts).

---

[709] Response(s) to our February 2025 consultation: NSPCC, p.24; Galop, p.4.
[710] Response(s) to our February 2025 consultation: Centre to End All Sexual Exploitation (CEASE), p.6.
[711] Response(s) to our February 2025 consultation: White Ribbon UK, p.1.
[712] Response(s) to our February 2025 consultation: British and Irish Law, Education, and Technology Association (BILETA), p.19.
[713] Response(s) to our February 2025 consultation: Engendering Change, p.2.
[714] Ofcom / Young People's Action Group Roundtable, 7 July 2025.
[715] Response(s) to our February 2025 consultation: [✂]; Evans, M.I., p.3; Parity, p.7; [✂].
[716] Response(s) to our February 2025 consultation: British and Irish Law, Education, and Technology Association (BILETA), p.12.

5.314 In response to feedback on freedom of expression considerations for enforcement action, we have amended the wording of our good practice step on enforcement action (alongside other changes noted in the following section) to include the recommendation that any action should be communicated clearly to the user facing the action. We have also clarified our wording in **Case study 24** on strike-based enforcement systems (draft case study 25) to state that the user is informed of the reason and consequences of a strike in the scenario detailed.

5.315 We consider that, in line with these changes and those detailed below, our final good practice steps for this action are appropriate and proportionate to protect women and girls from the harms outlined (as well as other groups affected by gender-based harms).

## Good practice steps in Action 9

5.316 At consultation, we proposed seven good practice steps in **Action 9**. This included:

a) Enforcement action (draft case study 25)
b) Upholding bans
c) Fact-checking and labelling
d) Watermarks and metadata
e) Moderator review
f) Hiding content
g) Dedicated reporting channels

### Enforcement action and user bans

#### Summary of stakeholder feedback

5.317 Several stakeholders commented on our good practice steps on enforcement action and user bans. Many raised concerns that perpetrators can bypass any enforcement action by making new and/or anonymous accounts.[717] Several mentioned recommending better detection methods for this (such as further identity verification, device fingerprinting, IP address tracking or account linking).[718]

5.318 Some stakeholders suggested we recommend specific actions, such as de-platforming, time-outs and user freezes depending on the volume of reports, and permanent bans.[719] Some stakeholders also asked for the Guidance to set thresholds for different types of enforcement action.[720] Several other responses mentioned the need to call out different treatment for repeat offenders,[721] such as those convicted of stalking.[722] BILETA noted that enforcement action should be consistent, while transversely some may exhibit overzealous enforcement with discriminatory impact.[723]

---

[717] Response(s) to our February 2025 consultation: University of York, p.8; University of Portsmouth, p.10; Refuge Annex, p.32; [✂]; British and Irish Law, Education, and Technology Association (BILETA), p.12.
[718] Response(s) to our February 2025 consultation: [✂]; End Violence Against Women Coalition (EVAW) Annex 1, p.14; Yoti, p.2; End Violence Against Women Coalition (EVAW) Annex 2, p.4; Refuge Annex, p.32.
[719] Response(s) to our February 2025 consultation: British and Irish Law, Education, and Technology Association (BILETA), p.16; Internet Matters, p.16; Welsh Women's Aid, p.5.
[720] Response(s) to our February 2025 consultation: White Ribbon UK, p.4.
[721] Response(s) to our February 2025 consultation: Plan International UK, p.14; Ofcom Stakeholder Roundtable, Belfast, 8 May 2025.
[722] Response(s) to our February 2025 consultation: Suzy Lamplugh Trust, p.5.
[723] Response(s) to our February 2025 consultation: British and Irish Law, Education, and Technology Association (BILETA), p.12.

5.319 Stakeholders suggested there should be greater information sharing and collaboration between services to prevent perpetrators moving between platforms.[724] Some additionally suggested that repeat offenders should be escalated to law enforcement.[725]

5.320 Stakeholders suggested that children who violate policies should be treated differently from adults, particularly those with neurodivergence.[726] Others suggested there should be different repercussions in cases where children may not have fully understood their actions, such as accidentally sharing illegal content.[727]

5.321 On draft case study 25, which focused on strike-based enforcement systems, one stakeholder supported strike-based enforcement but suggested it should consider perpetrators using multiple accounts.[728] The ICO welcomed inclusion of their content moderation guidance within the case study. They suggested we should include a reminder that their guidance applies to all forms of moderation, including removing content, restricting user access to specific features, reducing content visibility, or providing users with nudges and warnings.[729]

### Our final decision

5.322 We have combined the good practice steps on enforcement action and upholding bans into one good practice step – 'enforcement action'. This underscores that these steps are inter-dependent, and upholding bans or sanctions is crucial to effective enforcement action.

5.323 We have not made specific recommendations on the technical methods to identify users to uphold a ban. Common technical identifiers (such as IP addresses or device characteristics) may be shared by multiple users or changed frequently. Further, being prescriptive may inadvertently publicise information on identification methods that could be used by bad actors to circumvent a ban. Consistent enforcement for providers in this area is likely to include multiple different technologies or indicators in order to increase friction, so that perpetrators are unable or disincentivised to return.

5.324 We have not made specific suggestions of different enforcement action outcomes for different gender-based harms in this action. In **Chapter 3**, we discuss the need for policies which account for the specific dynamics of gender-based harms (see **Action 1**, and **Case study 1** on capturing stalking in terms of service). This should include, where appropriate and relevant to the offence, policies that detail a provider's stance on specific gender-based harms, and where relevant their policy on permitting known or suspected perpetrators on their service. As discussed above, if a provider's terms of service include upholding bans or sanctions on known or convicted perpetrators, it should uphold this policy consistently in its enforcement action. Such scenarios are addressed in **Chapter 5** in **Case study 22** on stalking and off-service behaviour policies, and **Case study 24** on strike-based enforcement methods on GenAI abuse from repeat perpetrators. To reflect this further, we have added the word 'consistent' to the good practice step to describe the action providers should take, to reflect the above and related stakeholder feedback on providers exhibiting inconsistency in how they enforce against users. Such scenarios are addressed in **Chapter 5** in **Case study 22** on

[724] Ofcom Stakeholder Roundtable, Belfast, 8 May 2025
[725] Response(s) to our February 2025 consultation: Engendering Change, p.2; Association of Police and Crime Commissioners, p.3; McLaughlan, M., Stevenson, S., p.4; [✂].
[726] Response(s) to our February 2025 consultation: NSPCC, 5; Internet Matters, p.16.
[727] Ofcom Stakeholder Roundtable, Cardiff, 1 May 2025
[728] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (EVAW), p.16.
[729] Response(s) to our February 2025 consultation: Information Commissioner's Office (ICO), p.11.

stalking and off-service behaviour policies, and **Case study 24** on strike-based enforcement methods on GenAI abuse from repeat perpetrators.

5.325 We recognise that enforcement action against children is a complex issue, which requires nuanced consideration that depends on the context and severity of the harm. We have included a reference to considering child users in the case study on strikes and repeat perpetrators (**Case study 24**), which states that providers may wish to consider if the user is an adult or child. We have also included an additional footnote with a reference to Ofcom's Additional Safety Measures consultation, which was published after the draft guidance. This consultation contains our proposals for additional Illegal Content and Protection of Children Codes measures on user bans and sanctions.

5.326 We have also added to the consideration in **Case study 24** to reflect the ICO's feedback, encouraging service providers to consult ICO guidance which applies to all forms of methods and content moderation.

## Other good practice steps and additional feedback

### Summary of stakeholder feedback

5.327 Stakeholders supported the good practice steps on fact-checking and labelling[730] and watermarks and metadata.[731] The Centre for Protecting Women Online provided additional evidence that while labels are a valuable tool in raising awareness of AI-generated content they need to be implemented with care to avoid mislabelled content.[732]

5.328 Pinterest raised concerns about our good practice step of dedicated reporting channels. They said that having different channels could lead to increased costs for platforms and create more complicated reporting processes for users.[733]

5.329 Several stakeholders noted that platforms need to be timelier with report handling,[734] and suggested that we set out how quickly a platform should respond to and action a report.[735]

5.330 We also received a suggestion for better transparency on enforcement action patterns so that bias in decisions can be challenged.[736]

### Our final decision

5.331 We have retained the good practice steps set out in paragraph 5.319 in this statement.

5.332 We have amended our good practice step on fact-checking and labelling to include evidence on the importance of context for displaying information about AI-generated content, as suggested by stakeholders. We have additionally included reference to Ofcom's latest research on deepfakes and attribution measures in our good practice step on watermarking and metadata and added a specific mention of the harm of deepfake intimate image abuse.

---

[730] Response(s) to our February 2025 consultation: The Cyber Helpline, p.7; Welsh Government p.4.
[731] Response(s) to our February 2025 consultation: Meta Platforms Inc., p.11; [✂].
[732] Response(s) to our February 2025 consultation: Centre for Protecting Women Online, p.16.
[733] Response(s) to our February 2025 consultation: Pinterest, p.6.
[734] Response(s) to our February 2025 consultation: Women's Aid Federation Northern Ireland, p.7; Engendering Change, p.2; Ofcom Stakeholder Roundtable, Belfast, 8 May 2025; Collective Shout, p.20.
[735] Response(s) to our February 2025 consultation: Refuge Annex, p.29; [✂]; [✂].
[736] Response(s) to our February 2025 consultation: British and Irish Law, Education, and Technology Association (BILETA), p.20.

5.333 We have not made any changes to our good practice step on reporting channels. It is important to make reporting channels findable and accessible. We cover estimated costs for providers in the impact assessment (**Annex A3**).

5.334 While we recognise that providing estimated time periods for a response to a report may be useful for setting user expectations and accountability for the service, we have decided not to provide prescriptive suggestions on what this time period should be for different harms. This is due to the multiple variables that a suggested time period for a response would have to account for, such as the size and type of the service and the type of harm reported. We have instead included a reference to the benefit of setting user expectations with estimated timelines for report responses in the new case study on transparency in the reporting process in **Action 8** (**Case study 19)**. We have also added in the word 'timely' into the introduction to **Action 9**.

5.335 We have not made any changes in **Action 9** related to stakeholder feedback on providers making data or trends on enforcement action public. Please see paragraphs 5.124-5.126 in this statement, where we discuss our decision on feedback on information sharing practices.

# A1. Other stakeholder feedback

A1.1 In this section, we set out and explain our decisions related to stakeholder feedback on the following topics:

a) **Topic 1:** Scope of the Guidance and the statutory framework

**b) Topic 2:** Accessibility and design of the Guidance

**c) Topic 3:** Stakeholder engagement

**d) Topic 4:** Specialist services and education

**e) Topic 5:** Other issues

## Scope of the Guidance and the statutory framework

### Summary of stakeholder feedback

A1.2 We received a range of feedback from stakeholders related to the scope of the Guidance and the statutory framework.

A1.3 A small number of stakeholders queried why harms were, or were not, in scope of various duties under the Act, including one queried primary priority content or priority content distinctions,[737] and another called for additional kinds of content and activities to be added the Illegal Harms Register of Risks.[738]

A1.4 One stakeholder also called for Ofcom to expedite the report about reporting and complaints procedures, as required by section 160 of the Act.[739]

A1.5 Clean Up the Internet said that Ofcom's guidance about user identity verification, as required by section 65 of the Act, must consider the misuse of accounts by perpetrators of online gender-based harms and how these risks can be mitigated.[740]

A1.6 In addition to the feedback we received about extending Protection of Children Codes to adults, as set out in paragraph 3.60 in this statement, stakeholders also commented on other Codes, for example commenting on segmentation of the CSAM measures, strengthening CSEA measures,[741] calling for strengthened how Codes address gender-based harms more generally.[742]

A1.7 One stakeholder commented that for platforms subject to the DSA for example, the recommendation to enable users to opt out of complaint communications may directly conflict with their legal requirements to provide the complainant with the statements of reasons for the resolution of the complaint. They also considered this opt-out would "require significant modification or exemption logic, introducing further complexity and legal risk." [743]

[737] Response(s) to our February 2025 consultation: Galop, p.2.; CyberSafe Scotland, p.5
[738] Response(s) to our February 2025 consultation: LGB Alliance, p.2.
[739] Response(s) to our February 2025 consultation: South West Grid for Learning, p.7.
[740] Response(s) to our February 2025 consultation: Clean Up the Internet, p.4.
[741] Response(s) to our February 2025 consultation: Collective Shout, p.20-21; NSPCC, p.26.
[742] Response(s) to our February 2025 consultation: Commissioner for Children and Young People (NICCY), p.9.
[743] Response(s) to our February 2025 consultation: Hammy Media Ltd / xHamster, p.5.

A1.8 Finally, several stakeholders called on Ofcom to have a sustained investment in safer online education and media literacy for both children and parents.[744] One Stakeholder said that Ofcom should produce guidance for parents about their children using social media and to run a campaign to educate users on geolocation sharing.[745]

### Our response

A1.9 The classification of content as primary priority content / priority content that is harmful to children, and decisions about which types of content fall under Schedule 7 (Priority Illegal Harms) are matters for Parliament, as is the scope of Ofcom's duty under section 54 of the Act, which specifically requires Ofcom to produce guidance "for providers of Part 3 services".

A1.10 We will produce the report about reporting and complaints procedures within two years of when section 160 of the Act comes into force.

A1.11 As regards to the responses concerning other areas of our work, including Ofcom's guidance on user identity under section 65 of the Act and our decisions in the Illegal Harms and Protection of Children Statements, we will consider these additional suggestions and comments as relevant and appropriate as part of any future work in those areas and seek up to date views from stakeholders through future consultations. We are unable to consider changes to any of our foundational steps in relation to this Guidance, as the foundational steps reflect measures in the Codes and risk assessment guidance which we have already consulted on and published through separate processes.[746]

A1.12 In response to feedback about media literacy, we agree that media literacy is an important component of improving users' ability to use, understand and create media. As part of our media literacy work, we have published draft recommendations designed to help a broad range of services to take active steps to empower the public by giving them the skills and information needed to critically and safely engage with the content they see.[747]

## Accessibility and design of the Guidance

### Summary of stakeholder feedback

A1.13 A small number of stakeholders asked Ofcom to provide more information on which services must implement the foundational steps, as well as information mapping each foundational step to its relevant Code of Practice and Guidance,[748] or noted that the "multi-layered structure" requiring cross referencing with other documentation could be difficult to navigate.[749] Meta Platforms Inc asked that Ofcom publish a table summarising the foundational steps and good practice steps set out in the Guidance.[750]

---

[744] Response(s) to our February 2025 consultation: Clean Up the Internet, p.4; The four Welsh Office of Police and Crime Commissioners, p.2; Women in Tech Policy Network, p.2; White Ribbon UK, p.1-2; Commissioner for Children and Young People (NICCY), p.15; Kira, B. Asser, Z. Ruiz, J, p.13; Engendering Change, p.2; [✂].

[745] Response(s) to our February 2025 consultation: Bolt Burden Kemp LLP, p.4-5.

[746] We published our Illegal Harms consultation in November 2023 (and have since published our final statement in December 2024) and our Protection of Children consultation in May 2024 (and have since published our final statement in April 2025).

[747] See section 11 of the Communications Act 2003. See Ofcom's Consultation on recommendations for online platforms, broadcasters and services.

[748] Response(s) to our February 2025 consultation: Kira, B. Asser, Z. Ruiz, J, p.8; [✂].

[749] Response(s) to our February 2025 consultation: Kira, B. Asser, Z. Ruiz, J, p.6-7.

[750] Response(s) to our February 2025 consultation: Meta Platforms Inc, p.12.

A1.14 Several stakeholders suggested how Ofcom might provide support for services to implement the Guidance, including commissioning specialist training by experts for services on how to implement the Guidance effectively,[751] providing toolkits, design templates and workshops for smaller service providers,[752] and tailored Guidance for different types and sizes of services.[753]

A1.15 Several stakeholders called on Ofcom to simplify the Guidance and ensure it is accessible for providers and users, including children, parents and carers.[754] [755]

A1.16 The Cyber Helpline suggested we include a summary of the rights assessment in the foreword of the Statement "to reassure stakeholders that measures have been scrutinized for compliance with rights and found to be justified."[756]

A1.17 Plan International UK said that the Guidance should be available across a number of languages, including English and Welsh, to support women and girls for whom English may not be their first language.[757] One stakeholder argued that the Guidance should ask services to ensure that interfaces, prompts, language, and support are matched to a child user's age, cognitive ability and emotional maturity .[758]

## Our response

A1.18 Our proposed structure with actions, foundational steps and good practice steps is aimed at ensuring that the Guidance can be applied by a broad range of services and that it covers a broad range of harms. The nine actions are built on a 'safety-by-design' approach to encourage providers to embed safety for women and girls online into the design and operation of their services. The steps within each action bring together our existing Codes and guidance for providers under illegal harms and protection of children, with additional steps that providers can take to go further.

A1.19 We set out additional information about foundational steps in the Guidance at a Glance document, including where the foundational steps appear in other Ofcom documents, such as our Illegal Content Codes of Practice and our Protection of Children Codes of Practice and where they have different application according to service type, size of service and risk.

A1.20 We acknowledge the importance of accessibility for civil society organisations and users, including parents, carers and children. We also recognise that this Guidance is meant to be relevant for services of different size and type. We have made some amendments to the Guidance to improve accessibility:

a) We have restructured the case studies to ease understanding (as explained in paragraphs 5.20-5.22 in this statement) and ensure they have applicability to services of different size and type.

b) We have made changes to **Chapter 2** (as explained in paragraphs 3.17 in this statement) to more clearly explain the harm areas.

---

[751] Response(s) to our February 2025 consultation: Refuge, p.9.
[752] Response(s) to our February 2025 consultation: Parity, p.13.
[753] Response(s) to our February 2025 consultation: Ukie, p.11; Ofcom / Young People's Action Group Roundtable, 7 July 2025.
[754] Response(s) to our February 2025 consultation: [✂]; Harrison, J., p.2; Scottish Government, p.1; The four Welsh Office of Police and Crime Commissioners, p. 5; Children First, p.8.
[755] Ofcom / Young People's Action Group Roundtable, 7 July 2025.
[756] Response(s) to our February 2025 consultation: The Cyber Helpline, p.10.
[757] Response(s) to our February 2025 consultation: Plan International UK, p.17.
[758] Response(s) to our February 2025 consultation: Do-Ngoc, T., Carmel, E, p.2.

A1.21 We also acknowledge the importance of making this Guidance available to users across the UK and we have published a version of the Guidance in Welsh.

# Stakeholder engagement

## Summary of stakeholder feedback

A1.22 A few stakeholders welcomed Ofcom's multi-stakeholder engagement approach to the consultation.[759] Some suggested that Ofcom engage with representatives from law enforcement[760],stakeholders representing marginalised communities,[761] and those with lived experiences especially children and young people.[762]

A1.23 One stakeholder suggested that Ofcom establish an advisory group that includes civil society experts and services to discuss guidance implementation, emerging forms of abuse and best practice development.[763] Another suggested that Ofcom establish a platform where companies can share best practice, innovations, impact of activities and solutions to barriers that they have identified.[764]

A1.24 Several civil society and individual stakeholders raised concerns that Ofcom's engagement with women and girls-focused civil society organisations created an "echo chamber" that excluded dissenting views.[765]

A1.25 Flux Digital Policy encouraged Ofcom to work with other domestic regulators to ensure regulatory coherence, including the Advertising Standards Authority (ASA).[766] One stakeholder noted that Ofcom should engage with the Department for Science, Innovation and Technology's Office of Digital Identity Attributes, as well as digital identity providers and professional / trade organisations to understand how accredited identity providers meet privacy requirements and can support the inclusion for those without documents.[767]

A1.26 Bumble encouraged Ofcom to collaborate with international regulators to promote higher norms and standards to address gender-based harms,[768] while another stakeholder indicated that the Global Online Safety Regulators Network can help drive best practice outside of the UK.[769]

## Our response

A1.27 We recognise the importance of ongoing and accessible dialogue to inform this Guidance and can confirm that we undertook various engagement activities with a range of stakeholders during the consultation period to ensure they were able to provide feedback on the draft

[759] Response(s) to our February 2025 consultation: Bumble, p.1; Meta Platforms Inc, p.1; NSPCC, p.8
[760] Response(s) to our February 2025 consultation: The Four Welsh Office of Police and Crime Commissioners, p.3; Association of Police and Crime Commissioners, p.2.
[761] Response(s) to our February 2025 consultation: Women's Aid Federation of England, p.4; Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.4; Ofcom / Translucent Meeting 25 March 2025
[762] Response(s) to our February 2025 consultation: Do-Ngoc, T., Carmel, E, p.6.
[763] Response(s) to our February 2025 consultation: Refuge, p.7.
[764] Response(s) to our February 2025 consultation: The four Welsh Office of Police and Crime Commissioners, p.5.
[765] Response(s) to our February 2025 consultation: Evans, M. I, p. 9; Moxon, S.P, p.4; Parity, p.15; [✂]; [✂].
[766] Response(s) to our February 2025 consultation: Flux Digital Policy, p.2.
[767] Response(s) to our February 2025 consultation: Yoti, p.3.
[768] Response(s) to our February 2025 consultation: Bumble, p.3.
[769] Response(s) to our February 2025 consultation: Women in Tech Policy Network, p. 3.

guidance. Among others, this included people with lived experience, young people, and smaller civil society organisations, including those representing men and boys (as explained in paragraphs 2.12-2.14 in this statement).

A1.28 As noted in paragraph 3.84 in this statement, we will continue to engage with key stakeholders, including services, civil society, academia and public bodies, to continue to build our evidence and drive the implementation of the Guidance.

A1.29 In addition, we are aware of the global and domestic initiatives that interact with our work on improving women and girls' safety online and we have sought to gain feedback on regulatory coherence in line with our wider work with the Global Online Safety Regulators Network as well as our regular engagement with domestic regulators and the Government.

## Specialist services and education

### Summary of stakeholder responses

A1.30 We also received feedback raising concerns with the lack of funding and resourcing for civil society organisations and advocated for services to fund online gender-based harms research and work,[770] including via the introduction of a tech tax on services.[771]

A1.31 Stakeholders raised the importance of wider ongoing efforts to prevent and tackle gender-based violence in schools, workplaces and the justice system.[772] For example, we heard that funding cuts to youth support services can lead at-risk and isolated young men and boys who may look to harmful online spaces which can foster resentment and anger.[773] Further, Are, C., raised concerns with the lack of sex education in schools and society.[774] The Commissioner for Children and Young People (NICCY) noted the Committee of Public Accounts' inquiry on Tackling Violence Against Women and Girls, highlighting the particular concerns in relation to "children as young as 11 [being] both victims and perpetrators of sexual violence online" and calls for the Government to address this. NICCY asked Ofcom to state "how it will ensure that this Guidance can act as a suitable response to the matters raised by the Committee of Public Accounts"'.[775]

### Our response

A1.32 We recognise that civil society organisations are limited in resource and funding. As set out in **Action 1**, we note that it is good practice for services engaging with expert organisations to provide appropriate compensation for any work carried out. However, matters concerning the funding and resourcing of third-party organisations are outside the scope of Ofcom's remit, as is taxation, which is a matter for Government and Parliament.

A1.33 In response to the Young Women's Movement and Are, C., we recognise the risks posed by gender-based harms can extend beyond the scope, expertise and remit of our role as the

[770] Response(s) to our February 2025 consultation: The Cyber Helpline, p.9.
[771] Response(s) to our February 2025 consultation: End Violence Against Women and Girls Coalition (EVAW), p.15.
[772] Response(s) to our February 2025 consultation: Ofcom / Young People's Action Group Roundtable, 7 July 2025.
[773] Response(s) to our February 2025 consultation: Ofcom / Men and Boys Roundtable, 29 May 2025.
[774] Response(s) to our February 2025 consultation: Are, C, p.1.
[775] Response(s) to our February 2025 consultation: Commissioner for Children and Young People (NICCY), p.12.

online safety regulator. Therefore, we recognise the need to work together with a wide range of stakeholders to tackle the root causes of online gender-based harms.

A1.34 In response to NICCY's feedback, we consider that this Guidance is intended to assist providers to address the risk of online gender-based harms, including those raised by the Committee of Public Accounts such as sexual violence. However, we also acknowledge that the Guidance is just one part of the wider landscape aimed at making a difference. We will continue to work with other organisations in the public, private and charitable sectors who share our common goal to create a safer life online for women and girls. We consider this Guidance to complement existing efforts across society to address online gender-based harms, including work done in schools, government and by civil society.

# Other issues

## Summary of stakeholder responses

A1.35 Heriot-Watt University – University of Edinburgh noted that the Guidance lacks information on how services' responsibilities map onto the criminal justice process.[776] Women's Aid Federation of England suggested that we add a good practice from the VAWG Code of Practice[777] on effective protections put in place by service providers to ensure flagging and court orders are not used for malign purposes by Government agencies or law enforcement of any kind to remove content they find objectionable which is neither illegal nor harmful.[778]

A1.36 SouthWest Grid for Learning said that while the draft guidance encouraged proactive moderation, it did not address what happens when platforms fail to act in clear cases of non-consensual intimate images. It called for the creation of a government-supported nonconsensual intimate image registry to enable "verified abusive content" to be "flagged, actioned and removed". It referenced similar existing mechanisms for CSAM in support of this argument and called on Ofcom to signal to the Government and industry that long term parity with CSAM enforcement requires national infrastructure for verified non-consensual intimate image content.[779]

A1.37 One stakeholder also raised concerns that "Ofcom's overall approach risks creating an implicit hierarchy where certain illegal content, notably Child Sexual Abuse Material (CSAM), is treated with greater urgency and resourcing than other illegal content and activities that disproportionately affect women and girls."[780]

A1.38 Ukie highlighted their use of an age rating system for content that is harmful to children.[781] The Commissioner for Children and Young People (NICCY) shared feedback from the NICCY Youth Panel/Engagement Forum that social media services should have women only sections.[782]

[776] Response(s) to our February 2025 consultation: Heriot-Watt University – University of Edinburgh, p.7.
[777] Carnegie UK, The End Violence Against Women Coalition, Glitch, NSPCC, Refuge, 5Rights, Woods, L. and McGlynn, C., 2022. Violence Against Women and Girls (VAWG) Code of Practice [accessed 20 October 2025]. The VAWG Code of Practice was developed for industry by a civil society coalition.
[778] Response(s) to our February 2025 consultation: Women's Aid Federation of England, p.12.
[779] Response(s) to our February 2025 consultation: SouthWest Grid for Learning, p.13.
[780] Response(s) to our February 2025 consultation: Kira, B., Asser Z., Ruiz, J., p.4.
[781] Response(s) to our February 2025 consultation: Ukie, p.4.
[782] Response(s) to our February 2025 consultation: Commissioner for Children and Young People (NICCY), p.12.

A1.39 The Jo Cox Foundation recommended that Ofcom include a suggestion for platforms to share basic information about political systems and identifying mis-information during election times.[783]

## Our response

A1.40 In response to the feedback from Heriot-Watt University – University of Edinburgh and Women's Aid Federation of England, we do not consider that this Guidance is an appropriate vehicle to comment on service providers' responsibilities or interactions with regards to the criminal justice process.

A1.41 In response to the South West Grid for Learning's feedback, we note that service providers have a duty to swiftly take down illegal content once they become aware of it. Ofcom's consultation on additional safety measures includes a proposal for certain service providers to use hash matching to detect intimate images that have been shared without consent, so they can be removed, and we have included this as good practice in the Guidance under **Action 6**. We consider the creation of national infrastructure to be a matter for Government.

A1.42 In response to the feedback about our approach to different types of content, we consider that the Illegal Harms Codes, and the proposed measures in the consultation on additional safety measures – such as hash matching for intimate image abuse – demonstrate Ofcom's commitment to ensuring that illegal content and activities that disproportionately affect women and girls are tackled effectively by services.

A1.43 In response to Ukie's feedback, the Act does not empower Ofcom to put in a place a 'content rating system'. Our role is to tackle the root causes of online content that is illegal and harmful for children, by improving the systems and processes that services use to address them. As set out in the Protection of Children Statement, we have aimed to establish a baseline level of protection for children of all ages, while encouraging providers to consider children's ages when deciding whether to take more protective actions for priority content and non-designated content. We noted that providers should put in place the strongest protections where the benefits to children are greatest and support children to have age-differentiated online experiences, in recognition of the rights and evolving capacities of children as they age. We are however clear that stronger protections for younger children should not leave older children unprotected.

A1.44 In response to the Commissioner for Children and Young People (NICCY) feedback on social media, Ofcom is not empowered to require providers to establish separate service sections for different groups of users (although it is open to them to do this if they think this will best serve their users).

A1.45 In response to the Jo Cox Foundation's feedback, we note that election disinformation is outside of the scope of the Guidance but we recognise, in **Chapter 2**, that women and girls in public life are targeted by organised gendered mis- and disinformation campaigns which weaponise false narratives to achieve social, political or economic aims.

[783] Response(s) to our February 2025 consultation: The Jo Cox Foundation, p.2.

# A2. Legal annex

## Ofcom's General Duties

A2.1 The Communications Act 2003 ("CA 2003") places a number of duties on Ofcom that we must fulfil when exercising our regulatory functions, including our online safety functions. Section 3(1) of the CA 2003 states that it shall be our principal duty, in carrying out our functions:

- To further the interests of citizens in relation to communication matters; and
- To further the interests of consumers in relevant markets, where appropriate by promoting competition.

A2.2 In performing that principal duty, we are required to have regard to principles set out in the CA 2003 under which regulatory activities should be transparent, accountable, proportionate, consistent and targeted only at cases in which action is needed, as well as any other principles appearing to us to represent best regulatory practice (section 3(3) of the CA 2003).

A2.3 In carrying out our functions Ofcom is required to secure, in particular, the adequate protection of citizens from harm presented by content on regulated services, through the appropriate use by providers of such services of systems and processes designed to reduce the risk of such harm (section 3(2)(g) of the CA 2003).

A2.4 Section 3(4A) of the CA 2003 further provides that in relation to matters to which section 3(2)(g) is relevant, we must have regard to the following as they appear to us to be relevant in the circumstances:

- the risk of harm to citizens presented by content on regulated services;
- the need for a higher level of protection for children than for adults;
- the need for it to be clear to providers of regulated services how they may comply with their duties under the Act;
- the need to exercise our functions so as to secure that providers may comply with such duties by taking or using measures, systems or processes which are proportionate to the size or capacity of the provider and the level of risk of harm presented by the service;
- the desirability of promoting the use by providers of technologies which are designed to reduce the risk of harm to citizens presented by content on regulated services and the extent to which providers demonstrate, in a way that is transparent and accountable, that they are complying with their duties.

A2.5 Section 3(4) of the CA 2003 sets out other matters to which Ofcom must, to the extent they appear to us relevant in the circumstances, have regard, in performing our duties. In line with these duties in preparing the Guidance we have considered: the desirability of promoting competition and encouraging investment and innovation in relevant markets; the vulnerability of children and of others whose circumstances put them in need of special protection; the needs of persons with disabilities, the elderly and of those on low incomes; the desirability of preventing crime and disorder; the opinions of consumers and of members of the public generally; and the different interests of persons in the different parts of the United Kingdom and of the different ethnic communities within the United Kingdom.

## Statement of Strategic Priorities for Online Safety

A2.6 On 2 July 2025, the Government's Statement of Strategic Priorities for Online Safety ("SSP") was designated, after previously being laid in draft before Parliament.[784]

A2.7 This sets out the Government's desired outcomes which Ofcom must have regard to when exercising its regulatory functions and outlines, as one of five priorities, the importance of 'safety by design' in tackling violence against women and girls.

A2.8 Ofcom responded to this by way of letter dated 25 July 2025.[785] We have had regard to the SSP, and in particular the Government's commitment to tackling the abuse faced by women and girls online, when making our final decision concerning the Guidance.

## Media Literacy Duties

A2.9 We also draw upon Ofcom's media literacy duties under section 11 of the CA 2003 (as amended by the Act). Ofcom's media literacy duties are set out under section 11 of the CA 2003.

A2.10 The Act amended our media literacy duties to require Ofcom to take such steps as we consider most likely to be effective in heightening the public's awareness and understanding of the ways in which they can protect themselves and others when using regulated services, in particular by helping them to:

- understand the nature and impact of harmful content and the harmful ways in which regulated services may be used, especially content and activity disproportionately affecting particular groups, including women and girls;
- reduce their and others' exposure to harmful content and to the use of regulated services in harmful ways, especially content and activity disproportionately affecting particular groups, including women and girls;
- use or apply—
  - features included in a regulated service, including features mentioned in section 15(2) of the Act, and
  - tools or apps, including tools such as browser extensions, so as to mitigate the harms mentioned in the second bullet.
- establish the reliability, accuracy and authenticity of content;
- understand the nature and impact of disinformation and misinformation, and reduce their and others' exposure to it;
- understand how their personal information may be protected.

A2.11 Ofcom must perform this duty by pursuing activities and initiatives, commissioning others to pursue activities and initiatives, taking steps designed to encourage others to pursue activities and initiatives and making arrangements for the carrying out of research. We can also perform this duty in other ways.

A2.12 The Act also created a new duty for Ofcom to take such steps as we consider most likely to encourage the development and use of technologies and systems for supporting users of

[784] Department for Science, Innovation & Technology, 2 July 2025, Final Statement of Strategic Priorities for Online Safety.
[785] Ofcom, 25 July 2025, Letter to Government on the Statement of Strategic Priorities for Online Safety.

regulated services to protect themselves and others in relation to the matters set out in this section.[786]

# Summary of relevant duties under the Act

A2.13 In the following sections, we summarise the provisions of the Act which are relevant to service providers for the purposes of this Guidance.

## Safety duties relating to illegal content

A2.14 The Act imposes duties of care on providers of regulated user-to-user services and providers of regulated search services[787] in relation to, among other things, "illegal content".[788]

A2.15 Providers of regulated user-to-user services and regulated search services have specific safety duties to effectively mitigate and manage risks of harm from illegal content.[789] User-to-user services also have duties to effectively manage the risk of the service being used for the commission or facilitation of the defined priority offences identified in the Act. For a more detailed summary of the safety duties about illegal content, please see Ofcom's Overview of Illegal Harms section of our Illegal Harms Statement as well as the Legal Annex at Annex 2.

A2.16 Service providers need to understand what amounts to illegal content in order to carry out their risk assessment, as set out in the 'Risk assessment duties' section, and comply with their safety duties. Ofcom's Illegal Content Judgements Guidance will help providers to assess whether content is illegal.

## Children's safety duties

A2.17 Part 3 services that are 'likely to be accessed by children' are subject to duties relating to the protection of children from content that is legal but is harmful to them (known as 'content that is harmful to children'[790]).[791]

A2.18 The duties on user-to-user services include using proportionate systems and processes designed to prevent children encountering primary priority content that is harmful to children. These duties also involve protecting children in age groups judged to be at risk of harm from priority content and non-designated content.[792] The duties on search services include using

[786] Section 11(1B) CA 2003. This includes technologies and systems which: provide further context to users about content they encounter; help users to identify, and provide further context about, content of democratic importance present on regulated user-to-user services; signpost users to resources, tools or information raising awareness about how to use regulated services so as to mitigate the harms mentioned in the second bullet above.
[787] Part 2 of the Act provides definitions related to these services.
[788] Under section 59 of the Act, 'illegal content' is defined as "content that amounts to a relevant offence".
[789] Section 10 and 27 of the Act.
[790] As defined in section 60 of the Act.
[791] As set out in sections 11-13 and 20-21 for regulated user-to-user services and sections 28-30 and 31-32 for regulated search services.
[792] Primary priority content is defined in section 61 of the Act. In summary it comprises pornographic content and content which encourages, promotes or provides instructions for: (a) suicide; (b) an act of deliberate self-injury; and (c) an eating disorder or behaviours associated with an eating disorder. Priority content is defined at section 62 of the Act. In summary it comprises abusive content and content which incites hatred based on specified characteristics; violent content; bullying content; and content relating to dangerous stunts or challenges or physically harmful substances. It also includes 'non designated content' as defined in section

proportionate systems and processes designed to minimise the risk of children encountering such content. For a more detailed summary of the safety duties about content that is harmful to children, please see Ofcom's Overview section of our Protection of Children Statement as well as the Legal Annex at Annex 4.

## Duties about content reporting and complaints

A2.19 In addition to these duties, providers of regulated user-to-user and search services have additional duties in relation to illegal content and protection of children which are relevant to the Guidance: content reporting[793] and complaints procedures.[794]

A2.20 Section 7 of the Act states that all providers of regulated user-to-user services must comply with these duties (and the other duties set out under section 7(2)). Section 24 similarly states that providers of regulated search services must comply with these duties (and the other duties set out under section 24(2).

## Risk assessment duties

A2.21 Providers of regulated user-to-user and search services have a duty to carry out a suitable and sufficient illegal content risk assessment[795] at the times set out in Schedule 3 to the Act. These services must take appropriate steps to keep an illegal content risk assessment up to date, including when Ofcom makes a significant change to a relevant risk profile. They are also under an obligation to carry out a further suitable and sufficient illegal content risk assessment, before making any significant changes to any aspect of a service's design or operation - this further illegal content risk assessment must relate to the impact of that proposed change.

A2.22 Providers of regulated user-to-user and search services that are likely to be accessed by children have a duty to carry out a suitable and sufficient children's risk assessment[796] at the specific times set out in Schedule 3 to the Act. The risk assessments must cover certain matters, must be kept up to date, including when Ofcom makes a significant change to a relevant risk profile, and before making any significant changes to any aspect of a service's design or operation.

## Transparency duties

A2.23 The Act also sets out that where Ofcom has designated a relevant service as either Category 1 or Category 2B (user-to-user services) or Category 2A (search services or combined services), the service will appear on Ofcom's register of categorised services.[797] Once a year, Ofcom must issue every such provider with a transparency notice requiring them to produce a transparency report about that service.[798]

---

60(2)(c) of the Act which is content of a kind which presents a material risk of significant harm to an appreciable number of children in the UK (subject to certain exclusions).

[793] Section 20 and section 31 of the Act.

[794] Section 21 and section 32 of the Act.

[795] Section 9 and 26 of the Act.

[796] Section 11 and 28 of the Act.

[797] Section 95(2) of the Act.

[798] Section 77 of the Act.

## User empowerment duties

A2.24 These duties will apply to Category 1 services. As noted in Ofcom's updated roadmap on online safety implementation, subject to the outcome of our representations process, we plan to publish the categorisation register and consult on the additional duties that apply to categorised services around July 2026.

A2.25 As set out in section 14 of the Act, Category 1 services will have to conduct 'a suitable and sufficient assessment' related to adult user empowerment content.

A2.26 Section 16 of the Act describes the content that these duties will apply to and includes regulated user-generated content that promotes suicide, self-harm and eating disorders, as well as content that is abusive or incites hatred against listed characteristics.

A2.27 Under section 15 of the Act, Category 1 services will have to include in a service, to the extent that it is proportionate to do so, features which adult users may use or apply if they wish to increase their control over content or users. These features are those that:

- reduce the likelihood of the user encountering content;[799]
- alert the user to content present on the service;[800]
- prevent non-verified users from interacting with content from that user;[801] and
- reduce the likelihood that verified users encounter content from non-verified users.[802]

A2.28 Category 1 services must additionally:

- ensure such features are made available to all adult users and are easy to access;[803]
- give registered adult users the earliest possible opportunity to take a step indicating they wish to retain or change the default setting of the feature (whether that is that the feature is applied or not applied by default);[804]
- include clear and accessible provisions in the terms of service specify which user control features are available and how users may take advantage of them;[805]
- summarise in the terms of service the findings of the most recent assessment of a service under section 14;[806] and
- include in a service features which adult users may use or apply if they wish to filter out non-verified users.[807]

## Duties concerning freedom of expression and privacy

### Freedom of expression

A2.29 Service providers have specific duties under sections 22(2) (user-to-user) and 33(2) (search) of the Act to have particular regard, when deciding on, and implementing, safety measures and

[799] Section 15(3) of the Act.
[800] Section 15(3) of the Act.
[801] Section 15(10) of the Act.
[802] Section 15(10) of the Act.
[803] Section 15(4) of the Act.
[804] Section 15(5) of the Act.
[805] Section 15(7) of the Act.
[806] Section 15(8) of the Act.
[807] Section 15(9) of the Act.

policies,[808] to the importance of protecting users' right to freedom of expression within the law.

A2.30 Under section 22, Category 1 services will have additional duties in relation to freedom of expression, including the duty to prepare and publish impact assessments of contemplated and adopted safety measures and policies in relation to freedom of expression, as well as to keep the impact assessment updated. Those services will have a further duty to specify in a publicly available statement the positive steps that the provider has taken in response to an impact assessment to protect users' right to freedom of expression within the law.

### Privacy

A2.31 Service providers have specific duties under sections 22(3) (user-to-user) and 33(3) (search) of the Act in relation to privacy. These provisions place obligations on providers, when deciding on, and implementing, safety measures and policies, to have particular regard to the importance of protecting users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of the service (including, but not limited to, any such provision or rule concerning the processing of personal data).

A2.32 Under section 22, Category 1 services have additional duties to prepare and publish impact assessments of contemplated and adopted safety measures and policies in relation to privacy impacts, as well as to keep the impact assessment updated. Those services will have a further duty to specify in a publicly available statement the positive steps that the provider has taken in response to an impact assessment to protect users' right to privacy.

[808] Section 22(8) sets out that, in relation to user-to-user services, "safety measures and policies" means measures and policies designed to secure compliance with any of the duties set out in—section 10 (illegal content), section 12 (children's online safety), section 15 (user empowerment), section 20 (content reporting), or section 21 (complaints procedures). Section 33(4) sets out that, in relation to search services, safety measures and policies" means measures and policies designed to secure compliance with any of the duties set out in—section 27 (illegal content), section 29 (children's online safety), section 31 (content reporting), or section 32 (complaints procedures).

# A3. Impact assessments

## Costs and risks impact assessment

A3.1 Impact assessments provide a valuable way of assessing the options for regulation and showing why the chosen option(s) was preferred. They form part of best practice policy making. This is reflected in section 7 of the CA 2003, which requires Ofcom to carry out and publish an assessment of the likely impact of implementing a proposal which would be likely to have a significant impact on businesses or the general public, or when there is a major change in Ofcom's activities. As a matter of policy, Ofcom is committed to carrying out impact assessments in the large majority of our policy decisions and has discretion as to the substance and form of an impact assessment. Our impact assessment guidance sets out our general approach to how we assess and present the impact of our decisions.[809]

A3.2 Our Guidance aims to provide service providers with advice on how they can meet their relevant duties under the Act, as well as additional advice on the voluntary good practice steps they could take to tackle online gender-based harms.

A3.3 We assess the impact of our Guidance in the following sections. Where we set out how service providers can consider the measures recommended in the wider online safety regime to tackle online gender-based harms ('foundational steps'), we note that the impacts of these measures have already been assessed in the Illegal Content and Protection of Children Codes and guidance on Risk Assessments and Transparency Reporting. In this impact assessment, we therefore focus on the potential impact of service providers engaging with the Guidance and taking the good practice steps.

## Our provisional assessment

A3.4 At consultation, our proposed view was that the draft guidance was unlikely to impose a significant burden on service providers. We explained that this was because the Guidance does not mandate any new requirements but instead strongly encourages the take up of the good practice steps set out.

A3.5 Nevertheless, we recognised that service providers may incur some costs. In particular, there may be some small costs from engaging with the Guidance (e.g. staff time), by familiarising themselves with the Guidance and considering the actions and good practice step it sets out. There may also be additional, more substantial costs (e.g. one-off and ongoing costs) for providers that take the good practice steps. We expected that these costs would vary according to the size, complexity, and services' existing systems and processes.

## Stakeholder feedback

A3.6 Some stakeholders welcomed and/or provided general support for our impact assessment.[810] However, others argued that the impact assessment could go further in its consideration of the potential benefits and costs.

[809] Ofcom, Impact assessment guidance, 2023.

[810] Response(s) to our February 2025 Consultation: Barker, K., p. 15; Children's Commissioners for England's Office, p.6; Flux Digital Policy, p.7; Image Angel, p.9; Internet Matters, p.21-22; Institute for Strategic Dialogue

A3.7 Some were concerned that our impact assessment had not accounted for, or that more consideration could be provided for, the benefits to users (e.g. women and girls).[811]

A3.8 Others argued that more consideration could be given to the potential indirect impacts and wider impacts to society. For example, two academic respondents suggested that we should consider the potential cost reductions that could arise to service providers (e.g. reduction in long-term moderation costs) if taking the good practice steps.[812] A small number of stakeholders suggested that we should consider the potential wider costs to other parties and society, such as in terms of healthcare and law enforcement resources, if service providers choose not to take the good practice steps.[813]

A3.9 Trade bodies suggested that more consideration should be provided for how smaller service providers are often likely to be disproportionately impacted when taking new measures, relative to large service providers.[814]

A3.10 A small number of stakeholders suggested that the impact assessment could include quantification of the potential costs to providers from taking the good practice steps,[815] with Internet Matters specifically suggesting that we include a calculation of the Business Net Present Value (BNPV). techUK considered that the lack of quantification puts the onus on providers to calculate the costs of measures.[816]

A3.11 Some stakeholders also questioned the intended value and impact of the Guidance in light of our view in the consultation that the draft guidance was unlikely to impose a significant burden on service providers as it does not mandate any new requirements.[817]

## Our response

A3.12 We maintain our view that the Guidance is unlikely to impose a significant cost burden on providers, including smaller service providers. This is because we consider that all providers will have the flexibility to take the non-mandatory good practice steps in a cost-effective way, that is proportionate to their size and risk.

A3.13 In response to the stakeholder feedback received, we have further developed our impact assessment to recognise the potential direct and indirect benefits and costs, as well as potential wider impacts on society, associated with service providers taking the good practice steps.

### Direct impact

A3.14 If taken effectively, we expect the steps to have a range benefits. This includes more transparency on how firms are addressing online gender-based harms to help users make

(ISD), p.13; The Cyber Helpline, p.10; The four Welsh Office of Police and Crime Commissioners, p.7; and Welsh Women's Aid, p.10-11.

[811] Response(s) to our February 2025 Consultation: Engendering Change, p.3; [✂]; Suzy Lamplugh Trust, p.13-14; and Women's Aid Federation of England, p.15.

[812] Response(s) to our February 2025 Consultation: Barker, K., p. 16; and Heriot-Watt University - University of Edinburgh, p. 13.

[813] Response(s) to our February 2025 Consultation: [✂]; and Suzy Lamplugh Trust, p.13-14.

[814] Response(s) to our February 2025 Consultation: Online Dating & Discovery Association (ODDA), p.2; Ukie, p2-6.

[815] Response(s) to our February 2025 Consultation: Internet Matters, p.21-22; [✂];

[816] Response(s) to our February 2025 Consultation: techUK, p.10.

[817] Response(s) to our February 2025 Consultation: Lucy Faithfull Foundation, p.6; Marie Collins Foundation, p.5; Suzy Lamplugh Trust, p.13-14.

informed decisions, better harm prevention to reduce the scale and impact of gender-based harms on women and girls, and improved support for women and girls targeted by harms. As noted in **Section 3**, we expect these benefits to extend to any user experiencing the harms set out, not just women and girls.

A3.15 Service providers who choose to engage with the Guidance will incur some small costs in reading and familiarising themselves with its contents and considering how they might take forward its actions and recommendations. These costs are likely to vary across service providers, depending on the extent they engage with the Guidance.

A3.16 Service providers that take the good practice steps may incur more substantial costs in the form of one-off and ongoing costs. We expect these costs will vary according to the size and complexity of services and also depend on the existing systems and processes services may already have in place.

A3.17 We expect a service provider will only take the good practice steps if it considered the potential costs to be proportionate to the expected online safety benefits to users. We acknowledge the Online Dating and Discovery Association (ODDA) and Ukie's comments that smaller service providers could be disproportionately impacted when introducing new measures. Upon further consideration, we explicitly acknowledge in the Guidance where we consider a good practice step may be prohibitively costly for smaller service providers to take. For example, we note that certain engagement methods with experts and oversight mechanisms (**Action 1, Case studies 3** and **4**) are likely most proportionate for larger providers.

A3.18 In **Table 2**, we provide some consideration of the potential direct costs to service providers, as well as the potential benefits to users, for examples of good practice step set out across the actions in the Guidance.

| Actions | Example of good practice | Potential benefits | Potential direct costs |
|---|---|---|---|
| **Ensure governance and accountability processes address online gender-based harms** | This could include setting policies that are designed to tackle online gender-based harms. | Having clear, specific, and proactive policies could create safer spaces for women and girls on services. | Staff costs associated with developing new polices, or updating existing policies, and introducing these policies to clearly tackle online gender-based harms. |
| **Conduct risk assessments that focus on harms to women and girls** | This could include conducting user research such as surveys, to better understand users' preferences and experiences of risk. | Insights from the surveys could then be used to develop safety tools and monitor the experiences of users engaging with the service. | Costs associated with engaging with external experts, to design and conduct surveys, to better understand the experiences of online users, including survivors and victims. |
| **Be transparent about women and girls' online safety** | This could include sharing information about the prevalence of different | Could provide users and others (e.g. civil society organisations) with additional information to | Staff costs associated with determining the information that can be shared on the prevalence |

| Actions | Example of good practice | Potential benefits | Potential direct costs |
|---|---|---|---|
| | forms of online gender-based harms. | understand which harms disproportionately affect women and girls. | of online gender-based harms, and on the effectiveness of measures in place. |
| **Conduct abusability evaluations and product testing** | This could include using red teaming for abusability testing. | Could create safer environments for women, girls, and other users at heightened risks of online gender-based harms. | Costs associated with planning and conducting red team exercises, including paying for the input of any external experts, and the computing power needed to perform the exercises. |
| **Set safer default settings** | This could include setting strong and customisable defaults around privacy. | Enables users to have the highest safety option as default, but also the flexibility and control to customise defaults if they wish to. | Staff costs; systems infrastructure costs; and product and user experience design and testing costs associated with developing and introducing user defaults. |
| **Reduce the circulation of content depicting, promoting or encouraging online gender-based harms** | This could include designing recommender systems that promote content diversity and variety and reducing the prominence of misogynistic abuse and sexual violence from recommender feeds. | Could enable the identification and reduction in circulation of content that encourages misogynistic abuse and sexual violence. | Staff and systems infrastructure costs associated with reviewing and extending automated content moderation systems to identify content that could be harmful. |
| **Give users better control of their own experiences** | This could include allowing users to signal what content they do not want to see, and what content they want to see more of. | Could allow users that are at heightened risk of harm (e.g. public figures or those experiencing stalking or coercive control) to curate what safety looks like for them. | Staff costs; systems infrastructure costs; and product and user experience design and testing costs associated with developing and introducing tools that can provide users with greater control over the content they see. |
| **Enable users who experience online gender-based harms to make reports** | This could include allowing users to track and manage their reports and tailor their | Could encourage more users to report content and help users to provide the information a service | Staff costs; systems infrastructure costs; and product and user experience design and testing costs associated with developing and |

| Actions | Example of good practice | Potential benefits | Potential direct costs |
|---|---|---|---|
| | experience throughout the complaints process. | needs to make an appropriate decision. | introducing a system where users can track and manage reports. |
| **Respond appropriately when online gender-based harms occur** | This could include taking enforcement action against users who continually violate a provider's terms of service. | Supports survivors and victims by minimising the risk of future harmful behaviours from perpetrators. | Staff costs associated with determining what an appropriate form of action may be and when it may come into effect, and systems infrastructure and product and user experience design and testing costs associated with its introduction. |

**Table 2: Potential benefits to users and costs to service providers associated with the good practice steps**

A3.19 We have also considered the feedback we received from stakeholders that potential costs to service providers should be quantified. We do not think it would be meaningful to estimate the potential costs to service providers of taking our good practice steps. Our good practice steps are not prescriptive. Therefore, service providers have the flexibility to take these steps in a range of ways with consideration for their size, complexity and existing systems and processes. This means costs are likely to vary widely across service providers and we do not consider developing a broad cost range to account for this variation is likely to provide much clarity to individual service providers.

A3.20 In response to comments raised by Internet Matters, we acknowledge that it is good practice to quantify the potential impacts where possible and proportionate to do so. However, we note that calculating a BNPV[818] is not feasible in this context, as we would not be able to quantify all the potential direct benefits and costs that could result from a service provider taking the good practice steps. In particular, it would be challenging to monetise the potential wide-reaching benefits associated with the good practice steps that aim to create a safer life online for women and girls.

## Other impacts

### Indirect impacts

A3.21 In response to the feedback received by Professor Kim Barker and Heriot Watt University – University of Edinburgh, we acknowledge that the good practice steps could indirectly affect the ongoing costs of some providers' existing systems and processes. For example, where the good practice steps are effective at discouraging and preventing online-gender based harms from occurring, this could reduce the costs of providers reactively dealing with these harms through their content moderation and/or reporting and complaints functions. However, we also note that some of the good practice steps could increase the ongoing costs of providers' existing systems and processes. For example, where they aim to encourage users to report

[818] A financial metric that measures the difference between expected benefits and expected costs in present value terms.

their experiences of online-gender based harms, this could increase the costs associated with dealing with reports.

A3.22 We also acknowledge that the introduction of the good practice steps could make users feel safer when engaging on services. In turn, this could increase user numbers or engagement and, depending on the business model of the service, could increase revenues for those services.

### Impact on the wider market

A3.23 In response to other feedback on the potential wider costs to other parties and society, we also acknowledge the potential cost savings that could arise to wider society, as a result of providers taking the good practice steps, especially to public services and law enforcement resources that play an important role in supporting victims and survivors of online-gender based harms.

A3.24 Additionally, we recognise the potential impact the good practice steps could have if effective at encouraging more innovation among service providers, and in the range of measures used to address online gender-based harms.

# Rights impact assessment

A3.25 As a public authority, Ofcom must act in accordance with its public law duties to act lawfully, rationally and fairly, and it is unlawful for Ofcom to act in a way which is incompatible with the ECHR.[819]

A3.26 Of particular relevance to Ofcom's functions under the Act are the right to freedom of expression (Article 10 ECHR) and the right to privacy (Article 8 ECHR). We have had particular regard to these rights when developing the Guidance, to ensure that the actions and good practice steps we recommend are appropriate and proportionate to create a safer life online for women and girls, and do not disproportionately infringe these or other ECHR rights. Any interference with these ECHR rights must be prescribed by law; pursue a legitimate aim and be necessary in a democratic society. The interference must be proportionate to the legitimate aim pursued and corresponding to a pressing social need. The relevant legitimate aims that Ofcom may act in pursuit of, in the context of our duty under section 54 of the Act, include the prevention of crime and disorder, public safety and the protection of health or morals, and the protection of the rights and freedoms of others. Other rights which may also be relevant to our functions under the Act are the right to peaceful enjoyment of one's possessions (Article 1 of Protocol No. 1 ECHR), the right to freedom of thought, conscience and religion (Article 9 ECHR) and the right to freedom of assembly and association (Article 11 ECHR).

A3.27 In developing the Guidance, we have carefully analysed where we have identified the potential for interference with ECHR rights, to make sure any such interference is proportionate.

## Our provisional rights assessment

A3.28 We noted that in carrying out our rights assessment of our proposals, we had addressed the relevant rights impacts on users, services and other persons and had considered the extent to which our proposals may interfere with certain rights in the ECHR as set out in Schedule 1 of the HRA 1998. Where a right is engaged, the interference may be justified where it is:

- in accordance with the law;
- the law in question pursues a legitimate aim and it is proportionate to that aim; and
- there is a pressing social need.

A3.29 We noted the specific obligations on Ofcom under the Act in relation to protecting the right of individuals to freedom of expression within the law and protecting the privacy of users when setting out measures in a code of practice.[820] Our view was that the draft guidance drew upon measures already set out in the Illegal Content Codes and Risk Assessment Guidance and draft Protection of Children Codes and Risk Assessment Guidance, where those obligations have been considered in detail. We therefore did not separately consider any relevant impacts in relation to those 'foundational steps'.

[819] Section 6 of the Human Rights Act 1998.

[820] Paragraph 10(1) of Schedule 4 to the Act states '*Measures described in a code of practice which are recommended for the purpose of compliance with any of the relevant duties must be designed in the light of the principles...and (where appropriate) incorporate safeguards for the protection of the matters mentioned in those principles.'* Paragraph 10(2) sets out that those principles are the importance of protecting the right of users and (in the case of search services or combined services) interested persons to freedom of expression within the law, and the importance of protecting the privacy of users.

A3.30 Our approach was therefore to consider rights impacts of the actions and good practice steps set out in the draft guidance.

A3.31 In relation to the right to freedom of expression under Article 10 ECHR, we noted that any interference with this right must be proportionate to the legitimate aim pursued and corresponding to a pressing social need. We also noted that the relevant legitimate aims that Ofcom may act in pursuit of in the context of our duty under section 54 of the Act to provide this Guidance include the prevention of crime and disorder, public safety and the protection of health or morals, and the protection of the rights and freedoms of others.

A3.32 We explained that overall, we consider that the actions and good practice steps we proposed to include in the draft guidance represented a fair balance between securing adequate protections for women and girls from harm (and their rights in respect of this) and the ECHR rights of users, other interested persons and services, as relevant. We considered that any interference with the right to freedom of expression was proportionate to the legitimate aims pursued and placed weight on all the specific evidence of harm set out in our February 2025 consultation. We carefully considered whether other, less intrusive good practice recommendations would be appropriate that might adequately mitigate the harms faced by women and girls on regulated services.

A3.33 We made clear that we recognised that online harms, including hate and abuse targeted at women and girls based on their gender, can have an inhibiting effect on them and the way they engage and express themselves online. We recognised that existing evidence showed many women and girls limit their online speech due to concerns over abuse, harassment and other forms of harm and that this could manifest in several ways including not posting or engaging in debate, limiting the expression of their thoughts, or in some cases, coming off platforms altogether.

A3.34 We considered that, in tackling gender-based harms, service providers can have a significant impact on the online experiences of women and girls, including positively impacting their ability to express themselves freely. Therefore, we considered it proportionate to the aim of creating a safer life online for women and girls that the good practice recommendations we made may have resulted in service providers taking actions that restrict what some users who share and engage with harmful content, such as abuse and harassment against women and girls, could do online.

A3.35 We also considered Article 8 ECHR which sets out the right to respect an individual's private and family life. We explained that some of our good practice proposals would involve the collection and processing of personal data and that the ICO has a range of data protection compliance guidance which we encouraged service providers to consult. We said that our good practice proposals made it clear that service providers should follow data protection law and (where applicable) ICO guidance, so that they comply with data protection legislation. To assist service providers, we incorporated references to applicable ICO guidance on data protection legislation in the draft guidance. At paragraph A2.15 of the consultation, we provided examples of this.

A3.36 We considered that the good practice steps proposed were proportionate to the aim of the Act which is for Ofcom to produce guidance for service providers to assist them to protect women and girls in relation to risks from content and activity which disproportionately affects them and for reducing such risks.

## Stakeholder feedback and Ofcom's response

A3.37 We received a number of comments related to this rights assessment in response to our February 2025 consultation. We have assessed this feedback and have set out our response, before setting out our overall conclusions below. The key themes of stakeholder feedback, explored in greater detail in the paragraphs which follow, are:

- Positive feedback on the rights assessment, including that the rights assessment struck the right balance between the protection of different rights under the ECHR;
- Concerns that Ofcom should reference the UN Convention on Rights of a Child ("UNCRC") and conduct a Children's Rights Impact Assessment;
- Concerns that the rights assessment should focus more on the rights of women and girls, including other rights under the ECHR and international law;
- Freedom of expression and concerns about over-moderation by providers;
- Concerns that the draft guidance was discriminatory in breach of Article 14 ECHR[821] in that it unfairly focused on women and girls to the exclusion of men and boys;
- The rights assessment should consider additional factors or information; and
- Privacy and data protection.

A3.38 Numerous stakeholders commented on the rights implications of specific actions, good practice steps and case studies in the draft guidance. This feedback is discussed and our responses outlined in **Section 5** of this statement.

A3.39 Stakeholders also provided comments about the rights assessment and other impact assessments more generally. The University of York said that the impact assessments should mark the start of a detailed process of 'assessing, publicising and preventing' online harms.[822] The Institute for Strategic Dialogue (ISD) said that the impact assessments should include commitments to: track disaggregated data on implementation and platform responses (e.g. by gender, race, role in public life), regularly review the Guidance's real-world impact, and integrate these insights into Ofcom's broader transparency and enforcement framework under the Act.[823]

### Positive feedback about the rights assessment

#### Stakeholder feedback

A3.40 A number of stakeholders said they welcomed the rights assessment and considered that Ofcom had given appropriate consideration to the different rights impacts under the draft guidance,[824] stating that the provisional assessment represented "a thoughtful and well-grounded approach" and that it correctly identified that freedom of expression is a qualified

[821] Article 14 ECHR as set out in the HRA 1998 states "the enjoyment of the rights and freedoms set forth in the European Convention on Human Rights and the Human Rights Act shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status".

[822] Response(s) to our February 2025 consultation: University of York, p.11.

[823] Response(s) to our February 2025 consultation: Institute for Strategic Dialogue (ISD), p.15.

[824] Response(s) to our February 2025 consultation: Children's Commissioner for England's Office, p.6; The Cyber Helpline, p.10; The four Welsh Office of the Police and Crime Commissioners, p.7; The Jo Cox Foundation, p.3; Mayor of London, p.12; The Minderoo Centre for Technology and Democracy at the University of Cambridge, p.6; Office of the Derbyshire Police and Crime Commissioner, p.5; Barker, K., p.14.

right that must be balanced against the rights of others.[825] The Cyber Helpline said it was pleased to see a "robust rights assessment" which contextualised the draft guidance as "enabling a wider exercise of rights by curbing abuse, but also by giving users more control over their environment". It said it believed the draft guidance appropriately safeguarded ECHR rights and agreed that any interference with those rights was proportionate. The Women's Aid Federation of England agreed with the provisional rights assessment that any interference with freedom of expression in the draft guidance was proportionate to the legitimate aim of protecting the rights of others and promoting public safety.[826] It supported Ofcom's recognition in the rights assessment of the chilling effect that online harms have on women.[827] The Minderoo Centre for Technology and Democracy at the University of Cambridge agreed with Ofcom's position in the rights assessment and stated that ensuring a safer life for women and girls is fundamentally a question of human rights.[828]

A3.41 Some stakeholders made additional suggestions connected to the rights assessment. For example, the Cyber Helpline suggested that Ofcom consider publishing a summary of the rights assessment in the foreword to the Guidance to "reassure stakeholders that measures have been scrutinized for compliance with rights and found to be justified."[829] The Mayor of London said they welcomed Ofcom's impact and rights assessments but suggested that Ofcom could adopt a broader scope of "impact" that recognises not only the immediate consequences of exposure to harmful content but also its long-term, systemic and cultural effects. They said that research led by the Violence Reduction Unit shows that repeated exposure to violent or misogynistic content can shape social norms, increase desensitisation, and foster fear and that these effects are often gendered and racialised.[830]

### Our response

A3.42 We agreed that it would be helpful to stakeholders to add in a statement on Ofcom's consideration of rights in the Guidance itself. We have included this in **Chapter 1** of the Guidance.

A3.43 We consider that the Guidance recognises the long-term, systemic and cultural effects of users' exposure to harmful content as well as the immediate harmful consequences. In particular, we discuss this in **Section 4** of this statement where we recognise the impacts of pile-ons and coordinated harassment on women in public life and the chilling impact this has on women and girls' participation more broadly. We also explain the range of new evidence we received at consultation about how misogynistic abuse and sexual violence manifests and its impact on users, and the promotion of such content to men and boys. We explain that we have added relevant evidence related to harms from sexual violence, including new evidence on the role of recommender systems in promoting pornographic content depicting sexual violence. In **Section 4,** we also recognise the intersectional impacts of content and activity on women and girls and explain that we have added new evidence in the Guidance focusing on

---

[825] Response(s) to our February 2025 consultation: Professor Kim Barker, p.14.
[826] It stated, "with one in three (36%) UK women having experienced online abuse, representing over 11 million women, there is a clear and immediate need to protect their rights and safety. The Special Rapporteur on violence against women has previously explored online violence against women and girls from a human rights perspective and found that technology-facilitated gender-based violence hinder women's and girls' enjoyment of human rights and ability to achieve gender equality. This is mirrored in UN Women and the World Health Organisation's proposed definition of technology-facilitated violence against women."
[827] Response(s) to our February 2025 consultation: The Women's Aid Federation of England, p15.
[828] Response(s) to our February 2025 consultation: The Minderoo Centre for Technology and Democracy, p.7.
[829] Response(s) to our February 2025 consultation: The Cyber Helpline, p.10.
[830] Response(s) to our February 2025 consultation: Mayor of London, p.12.

overlaps between relevant harms, incorporating stakeholder feedback on how misogynistic abuse and sexual violence intersects with homophobia, transphobia and racism.

## Ofcom should reference the UNCRC and conduct a Children's Rights Impact Assessment

### Stakeholder feedback

A3.44 Several stakeholders suggested that Ofcom should consider the rights of children separately, including by reference to the UNCRC and conducting a Children's Rights Impact Assessment ("CRIA").[831]

A3.45 The Northern Ireland Commissioner for Children and Young People (NICCY) said they would have welcomed Ofcom undertaking a CRIA and for this to be detailed as a good practice step for providers to take in the Guidance. The response pointed out that paragraphs 38 and 39 of General Comment No. 25[832] makes recommendations in relation to CRIAs and safety by design industry standard. It also suggested referencing Articles from the UNCRC[833] as part of the evidence informing the four harm areas in the Guidance, as this "would send out a clear message to the technology companies that tackling violence against girls online is not optional but part of their legal and corporate responsibilities to children, under the UNCRC."[834] Children First made a similar comment highlighting Article 19 of the UNCRC, which says that Governments must do all they can to ensure that children are protected from all forms of violence. They said that General Comment No. 25 should be used as a starting point for Ofcom and the UK and Scottish Governments when considering the approach to encouraging take up of the Guidance.[835]

A3.46 Ofcom's Advisory Committee for Scotland, NICCY and Cybersafe Scotland also encouraged Ofcom to undertake a CRIA, with the Advisory Committee for Scotland also suggesting that a Wellbeing Assessment should be undertaken.[836] Several stakeholders said that the suggestion to conduct a CRIA had also been raised in relation to Ofcom's consultation on the Protection of Children Codes. Cybersafe Scotland encouraged companies to conduct 'best interest' rights-based assessments based on the UNCRC. They said that, for companies providing digital services to children in Scotland, rights-based impact assessments should be a legal requirement. Other stakeholders said that the rights assessment should have a stronger focus on children's rights. One individual said that the impact assessment should specifically include young people, identifying whether initiatives have influenced behaviour of young men and boys and, if so, how.[837] The Age Check Certification Scheme said that the right to digital protection and participation must be secured through the enforcement of age-appropriate experiences.[838] Thao-Ngoc, T. and Carmel, E., in their comments on the rights assessment,

---

[831] Response(s) to our February 2025 consultation: The Age Check Certification Scheme, p.3; Children First, p.9; The Northern Ireland Commissioner for Children and Young People (NICCY), p.13-15; Cybersafe Scotland, p.7; Ofcom Advisory Committee for Scotland, p.5; and Name Withheld 3, p.2.

[832] United Nations, 2021, General comment No. 25 (2021) on children's rights in relation to the digital environment [accessed 10 November 2025].

[833] Article 19: Protection from violence, abuse and neglect; Article 34: Protection from sexual exploitation and abuse; and Article 39: Recovery and reintegration

[834] NICCY referenced the following document: UNICEF, 2012, Children's Rights and Business Principles [accessed 10 November 2025].

[835] Response(s) to our February 2025 consultation: Children First, p.9.

[836] The stakeholders noted the following guidance: Scottish Government, 2024. Child rights and wellbeing impact assessment external guidance and templates, p.5 [accessed 10 November 2025].

[837] Response(s) to February 2025 consultation: Name Withheld 3, p.3.

[838] Response(s) to February 2025 consultation: Age Check Certification Scheme, p.3.

suggested making lived experience and child-centred design central to understanding platform dynamics by formally integrating the voices of those with lived experience, especially children and young people, into the design, implementation, and ongoing evaluation of safety measures.[839]

### Our response

A3.47 We have considered stakeholders' calls for greater focus on children's rights. As set out in our Protection of Children Statement,[840] our view is that the UK Parliament made it clear during the legislative process that the spirit of the UNCRC is reflected in the Act, including by amending the CA 2003 to reference the higher standard of protection for children.[841] On that basis, we remain of the view that the appropriate approach for us to assess rights impacts is to consider these in light of the applicable requirements under UK law, which encompasses and reflects relevant aspects of the UNCRC and General Comment No.25 (2021). We note the following issues relevant to the Guidance and consideration of rights of children:

a) In addition to adults, the Guidance will directly impact children and young people up to age 18 who the UNCRC is intended to protect. Girls, together with women, are a focus of the Guidance, but as explained in this statement we consider that it will also have positive impacts for men and boys even though the focus of Ofcom's duty to produce guidance is on content and activity disproportionately affecting women and girls, as established by Parliament and outlined in section 54 of the Act.

b) We recognise the importance of the UNCRC to the Guidance, including in particular Freedom of expression (Article 13); Freedom of thought, belief and religion (Article 14), Freedom of association (Article 15), Privacy (Article 16), Encouraging the development of appropriate guidelines for the protection of the child from information and material injurious to his or her well-being (Article 17). We consider that the Guidance protects these fundamental rights.

c) As referenced throughout this statement, we have specifically sought the views of young people on the Guidance to ensure that their views are included. This includes the roundtables we held with organisations that represent men and boys and the Young People's Action Group. In addition, we sought the views of young people and organisations which represent them during our regional engagement with stakeholders on the draft guidance. This upholds the general principle to involve children and young people in decisions that will affect them. As explained in our letter responding to the Government's Statement on Strategic Priorities for Online Safety, children's voices and experiences continue to play a crucial role in our policy work.[842]

d) We have incorporated the views of children and young people following our discussions with them into the Guidance.[843]

---

[839] Response(s) to our February 2025 consultation: Do-Ngoc, T, Carmel, E., , p.6.

[840] See paragraph 2.47 of Volume 1 Overview scope and regulatory approach to our Protection of Children Statement, 24 April 2025

[841] Section 3(4A)(b) of the CA 2003, as amended by section 91 of the Act.

[842] Ofcom, 25 July 2025, Letter to Government on the Statement of Strategic Priorities for Online Safety.

[843] See, for example, Section 4 of the statement where we draw on evidence received in relation to the impact of misogynistic content on men and boys, following the roundtable with men and boys' organisations, and Chapter 4 of the Guidance where this evidence was expressly referenced. This also led to us making changes to Chapter 1 of the Guidance. This recognises that abusive misogynistic content is often pushed towards boys - boys often find this content upsetting and it can normalise harmful narratives and beliefs of masculinity.

- We have considered relevant published research that involved and collected the views of children and young people. This research is noted throughout the Guidance.[844]

## Rights assessment should focus more on the rights of women and girls, including other rights under the ECHR and international law

### Stakeholder feedback

A3.48 A number of stakeholders told us that they considered that the rights assessment did not afford appropriate weight to the rights of women and girls.[845] Some added separately, together with other stakeholders, that the rights assessment did not refer to international law and jurisprudence of the Strasbourg Court which they argued would strengthen the rights assessment.[846]

A3.49 The Online Safety Act Network ('OSAN') said that while the summary of the approach to fundamental rights in the legal annex to the consultation and provisional rights impact assessment reflected the Court's approach, it did not go far enough into the detail of the jurisprudence. They said that their understanding of the jurisprudence of the European Court of Human Rights is that Ofcom "probably has more room to manoeuvre in terms of the balance of abusers' freedom of expression rights with the rights to freedom from torture/inhuman and degrading treatment and the right to private life of victims". OSAN said that it is arguable that as a public body, Ofcom is "under some positive duties in this regard which would certainly support its position if not suggest it go further." [847]

A3.50 OSAN annexed a paper to their response, authored by Professor Lorna Woods OBE, in support of this submission ('the Paper').[848] The Paper outlined jurisprudence of the Strasbourg Court in detail. The Paper raises a number of factors which it said should lead to Ofcom taking a more proactive approach to the rights of women and girls, noting that it considered there is space for Ofcom to "be more courageous" in its protection of the Article 8 ECHR rights of women and girls.[849]

A3.51 First, it noted that a discussion of Article 17¸ which prohibits the destruction of and excessive limitation on the rights and freedoms set in the ECHR, was not included in the provisional

---

Following the roundtable with the Young People's Action Group (YPAG), we added supporting information to Case study 10 on the importance of media literacy interventions in schools, communities and at home to combat misogynistic abuse and sexual violence.

[844] See, for example: Domestic Abuse Commissioner, 2025. Victims in their own right? Babies, children and young people's experience of domestic abuse; Internet Matters, 2023. "It's really easy to go down that path": Young people's experiences of online misogyny and image-based abuse; Girlguiding, 2024. Girls' Attitudes Survey 2024; National Education Union, 2023. Working with boys and young men to prevent sexism and sexual harassment; Ringrose, J., Regehr, K. and Whitehead, S, 2021. Teen Girl' Experiences Negotiating the Ubiquitous Dick Pic: Sexual Double Standards and the Normali…, *Sex Roles,* 85(558); Schmidt, F., Varese, F., Larkin, A., & Bucci, S. (2023). The Mental Health and Social Implications of Nonconsensual Sharing of Intimate Images on Youth: …*Trauma, Violence, & Abuse*, 25 (3), 2158-2172; Women's Aid, 2023. Influencers and Attitudes: How will the next generation understand domestic abuse?. We also note our Children's Register of Risk which contains a wide range of research in this respect.

[845] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (EVAW) Annex 1, p.17. End Violence Against Women Coalition (EVAW) Annex 2, p.5; Online Safety Act Network (OSAN), p.3; Online Safety Act Network (OSAN) Annex; Popa-Wyatt, M., p.3; Popa-Wyatt, M. Annex, p.5; Refuge, p.6.

[846] Response(s) to our February 2025 consultation: Children First, p.9; Equality Now, p.6; EVAW, Annex 1 and 2; OSAN, p.3 and Annex; Professor Kim Barker, p.9; and Women's Aid Federation of England, p.15.

[847] Response(s) to our February 2025 consultation: Online Safety Act Network (OSAN), p.3.

[848] Response to February 2025 consultation: Online Safety Act Network (OSAN), Annex.

[849] Response(s) to our February 2025 consultation: Online Safety Act Network (OSAN) Annex p.12.

rights assessment. It noted that under Article 17, specific content and activity would not be afforded the protection of Article 10 ECHR, although it emphasised that Article 17 would apply to content and activity "'only in the most serious cases" and that a wide use of Article 17 was not recommended because of the risks to freedom of expression, which in principle extends to protecting the shocking and offensive.[850] However, it argued that some of the content relevant to the Guidance – content that "aims at inciting violence or hatred or is targeted towards destroying the rights and freedoms of others" - would not receive the protection of Article 10 ECHR given that a direct incitement to violence is not required to trigger Article 17 which it said was evidenced by the jurisprudence referred to. It said it would seem likely that this would apply to death threats, especially when combined with other aspects (e.g. encouraging a pile on or doxxing), and considered that certain types of misogynistic content may cross also that threshold of seriousness. Second, it argued that there is a greater margin of appreciation for preventative measures where the rights of women and girls are engaged.[851] Third, it highlighted the positive obligations of the state to protect women and girls from harm.[852] It stated in relation to the draft guidance, that given much of the speech falling into the four categories of harm will be "speech attracting little protection (if any)" and "the matters that Ofcom seeks to protect go to the core of Article 8 ECHR" a stronger statement, not just about the space available to Ofcom to work in, but also about the positive obligations, would have been desirable. It added, "While freedom of expression should never be cavalierly dismissed, there is space here for Ofcom to be more courageous in its protection of the Article 8 rights of women and girls."[853]

A3.52 The Paper noted that many of the good practice proposals did not require the removal of content and were therefore less intrusive. It said, for example, that requiring governance mechanisms and providing user empowerment tools did "not directly affect speech" and that reviews of recommender tools "might limit reach but do not stop speech".[854]

A3.53 The British and Irish Law, Education and Technology Association (BILETA) noted "the complexities inherent in balancing freedom of expression with online content moderation are longstanding and largely unresolved" but welcomed the explicit consideration of these rights and their assessment in the draft guidance, specifically noting the importance of ensuring women and girls can exercise these rights safely. BILETA encouraged Ofcom to provide "further clarification and detail" as to how the Guidance intends to overcome the issue of reluctance of women and girls to actively participate online and exercise their right to freedom of expression due to concerns about potential abuse, and harm "including the increasing threat of malicious deepfakes like non-consensual intimate imagery and targeted online harassment". It noted that the provisional rights assessment commented on this, but that strengthening this aspect of the Guidance to empower women and girls to exercise their

[850] Response(s) to our February 2025 consultation: Online Safety Act Network (OSAN) Annex,p.4
[851] Response(s) to our February 2025 consultation: Online Safety Act Network (OSAN) Annex, p.5- 10.
[852] Response(s) to our February 2025 consultation: Online Safety Act Network (OSAN) p.10-12. This point was also noted by Professor Lorna Woods in Annex 1 to the EVAW response: "The other thing is that the guidance, and Ofcom's analysis in general across the board, is silent on, is the extent to which there are positive rights to protect people's human rights in their relationships with others. In some circumstances, the courts have said the public bodies are obliged to intervene. Admittedly, the case law here is less clear on how a body like Ofcom might be subject to positive obligations, but it is striking that there's no consideration of the issue.", p.18.
[853] Response(s) to our February 2025 consultation: Online Safety Act Network (OSAN) Annex, p.12.
[854] Response(s) to our February 2025 consultation: Online Safety Act Network (OSAN) Annex, p.7.

free speech online and contribute to their chosen platforms would "support the mission of ensuring online safety for women and girls as active digital citizens."[855]

A3.54 The response also recommended further guidance on how moderation practices and "free speech considerations" should interact with automated content moderation systems, given the potential for bias in these systems to either fail to detect harmful content targeting women and girls or unfairly censor their speech. [856]

A3.55 BILETA also commented on the Supreme Court decision in the case of *For Women Scotland Ltd v Lord Advocate* [2025] UKSC 16, suggesting that this had "sparked increased online discourse regarding the judgment, potentially impacting both trans and cis women depending on their perspectives on the ruling and trans rights Centre for Mental Health". They noted that this is a highly contentious issue and exemplifies the delicate balance that must be struck between competing rights and free speech considerations, both offline and online, a balance that remains under debate.[857]

A3.56 End Violence Against Women and Girls Coalition (EVAW) joint response to Ofcom's draft guidance said that the rights assessment should be strengthened to explicitly state how online abuse breaches the human rights of women and girls under Article 8 and 10 ECHR, and also Article 2 (right to life) and Article 3 (freedom from torture).[858] It also said that Ofcom should elaborate on how it balances conflicting rights, recognising that not all speech is equal, and some speech falls outside protection.[859] The Paper acknowledged the importance and relevance of these rights, although it also appreciated that not all content and activity the draft guidance focused on would reach the level of severity required to trigger Article 3.[860] Refuge recommended that the Guidance clearly state that freedom of expression does not justify violence or abuse and that ensuring safe online participation is essential to protecting the right to free expression for women and girls.[861] Popa-Wyatt, M. said that the rights assessment must reframe freedom of expression not merely as a right that might be infringed by moderation, but as a right that is undermined by unchecked abuse, adding that women and girls' expressive freedom is curtailed every time they are harassed off platforms or silenced by threats.[862]

A3.57 Women's Aid Federation of England referenced several aspects of international human rights law that it considered supported this position.[863] It supported Ofcom's recognition in the provisional rights assessment of the chilling effect online harms are having on women,

---

[855] Response(s) to our February 2025 consultation: BILETA, p.21.
[856] Response(s) to our February 2025 consultation: BILETA, p.22.
[857] Response(s) to our February 2025 consultation: BILETA, p.22.
[858] Response(s) to our February 2025 consultation: End Violence Against Women Coalition (EVAW) Annex 2, p.5.
[859] Response(s) to our February 2025 consultation: EVAW, Annex 2, p.5.
[860] Response to our February 2025 consultation, OSAN, Annex, p.8.
[861] Response(s) to our February 2025 consultation: Refuge, p.6.
[862] Response(s) to our February 2025 consultation: M. Popa-Wyatt, p.3.
[863] It stated, "The Human Rights Council resolution 31/13 recognises that human rights protected offline must also be protected online. Particular rights that may be impacted by technology-facilitated abuse include: The right to live free from gender-based violence; The right to freedom of expression and access to information; The right to privacy and data protection; The right to access and use digital technologies; The right to participate in public and political life. The United Nations' General Assembly's Resolution 71/199 also recognises that violations of the right to privacy online have particular effects on women and children, and those who are vulnerable or marginalised. This was reaffirmed by the Human Rights Council in resolution 34/7."

referencing research undertaken by Amnesty International.[864] However, it pointed Ofcom to a blog post on the Online Safety Act Network website,[865] linking to the Paper, "for more detail on legislation in this area."

A3.58 The Minderoo Centre for Technology and Democracy at the University of Cambridge added that both UN Women and the Council of Europe Convention on preventing and combating violence against women and domestic violence, identify online violence against women and girls as crucial factors that can limit women's public participation and their right to express themselves[866] and that online harms can therefore also represent a threat to the right to freedom of expression of women and girls.[867]

### Our response

A3.59 We have considered OSAN's response, including the Paper, in detail. We note the references to international human rights law and jurisprudence contained within the Paper, and referred to by other stakeholders including Children First, EVAW, Equality Now, Barker, K., and Women's Aid Federation of England. We agree that the right to freedom of expression is not absolute and that expression that promotes or justifies violence, hatred, xenophobia or another form of intolerance is not normally protected under Article 10 ECHR. We also agree that there are different categories of protected speech under Article 10 ECHR, with some speech receiving a greater degree of protection than others.[868] As explained below, the scope of harms in the draft guidance was broader than the Guidance and therefore our provisional assessment had to consider the broader impacts on freedom of expression rights. We consider that we have afforded sufficient weight to the rights of women and girls under the HRA 1998, including their Article 8 ECHR rights. We have also considered the rights of women and girls under Articles 2 and 3 in relation to abuse and other harms they may experience from online content and activity that disproportionately affects them, although we consider that these

---

[864] The response referred to, "Amnesty International research that found over three quarters (76%) of women who have experienced abuse or harassment on social media have changed the way they use the platform, with almost a third (32%) of women saying they have stopped posting content that expressed their opinion on certain issues. In the Victim Commissioner's report on the impact of online abuse, more than half of respondents agreed the abuse made them withdraw from the world, both online (51%) and offline (58%). When asked what they wanted from internet companies when reporting online abuse, respondents shared that the most important outcomes was for the abuse to stop (48%), for the abuser to be prevented from continuing (57%), and the abuser to be removed from social media (44%). One survey of almost 4,000 women found that 40% are worried about image-based abuse happening to them, rising to 58% of disabled women. These fears deeply impact our right to freedom of expression."

[865] Online Safety Act Network, 2025. Ofcom's draft guidance on protecting women and girls. [accessed November 19 2025].

[866] UN Women, 2022. Accelerating Efforts to Tackle Online and Technology-Facilitated Violence Against Women and Girls [accessed 19 November 2025]; Council of Europe, Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention), CETS No. 210, opened for signature May 11, 2011, entered into force August 1, 2014. [accessed 19 November 2025].

[867] Response(s) to our February 2025 consultation: The Minderoo Centre for Technology and Democracy at the University of Cambridge, p.6.

[868] These issues were raised by Professor Lorna Woods as noted in the transcript contained in Annex 1 to the EVAW coalition response to the consultation when she said, "*not all speech is equal, even within expression falling within Article 10. There is a priority given to freedom of expression where political speech is an issue, but lower protections or lower oversight for artistic speech, and then commercial speech. Ofcom's guidance doesn't recognise these different types of speech and nor does it engage with the fact that some speech falls outside protection entirely when it is aimed at undermining the objectives of the Convention or the rights of others. I think some of the activities that can be characterised as speech because they are just online would be undermining the rights of others. If we look at a rape and coercive control, and similar sorts of things, it is hard to see that they're not undermining the rights of others.*" (p.18).

specific rights would be unlikely to be engaged in many cases. We do not consider that the Paper changes the overall approach we have taken to the Guidance or our assessment of rights.

A3.60 We agree with the position in the Paper that content which incites violence or hatred or destroys the rights and freedoms of others would not receive the protection of Article 10 ECHR. We have expressly referenced this in a statement in **Chapter 2** of the Guidance,[869] together with contextualising the right to criticise certain views or opinions under Article 10 ECHR in line with case law. Taking into account other stakeholder feedback from service providers and other users on potential interference with the right to freedom of expression, we have clarified the scope of harms covered by the Guidance which we consider will reduce the risk of over-moderation by services which impacts on the right to freedom of expression of users and other people who might view online content. The harms within the scope of the Guidance are now clearly content and activity which is either illegal or is covered by the protection of children duties under the Act. We consider that this is in line with the submissions made in the Paper. It strengthens the position that the Guidance is targeted at a pressing social need to protect the rights of women and girls in relation to a set of clearly defined harms, in accordance with definitions provided within the Act, Ofcom's Illegal Content Judgements Guidance, and the Children's Harms Guidance. This pressing social need was recognised by Parliament by including section 54 in the Act. This has enabled us to take a more targeted approach to the good practice steps focused on, while also providing information as to how these relate to the harms within the scope of the Guidance, which provides important context for service providers. Our statement explains where we have made changes to strengthen the Guidance with this focus in mind.[870]

A3.61 The Guidance recognises the harms in scope of the Guidance may have a chilling effect on women's and girls' rights, including their rights to freedom of expression. It also includes a statement on Ofcom's consideration of rights.[871] In **Chapter 2** of the Guidance, we note that the right to freedom of expression is not absolute and cite relevant ECHR case law in support of this.[872]

A3.62 In making these changes to the Guidance, we also note that Parliament has set out that the duty on Ofcom in section 54 of the Act is to produce Guidance for service providers, rather than to set out enforceable requirements. However, we consider that the changes we have made will assist providers to use the Guidance more effectively, which will in turn improve the online experiences of women and girls and uphold their fundamental rights.

A3.63 We acknowledge the positive obligations on the State to protect the fundamental rights of women and girls. We consider that the positive obligations to protect these rights are inherent

[869] See page 18. We also note the following case law and ECHR paper: Perinçek v. Switzerland [GC], 2015, § 230; Zemmour v. France, 2022, § 49; European Court of Human Rights, Key Theme – Article 10 Hate Speech.
[870] For example, in Chapter 2, we have broadened two categories of harm focusing on illegal content and activity. We received feedback that 'online domestic abuse' was too narrowly defined. We have amended this category to 'stalking and coercive control' covering the offences of stalking and coercive and controlling behaviour. We have also expanded the category of 'image-based sexual abuse' to recognise the offence of self-generated indecent images by children in addition to the offences intimate image abuse and cyberflashing. In addition, we have added case studies on a broader range of service types and focusing on different users to demonstrate efficacy of good practice to different services and different ways in which harm can manifest. This can be seen in Case study 1 where we discuss how providers can capture the specific harm of stalking within their terms of service.
[871] See Chapter 1 of the Guidance.
[872] See Chapter 2 of the Guidance.

to the framework of the Act, including Ofcom's duty to carry out our functions so as to secure the adequate protection of citizens from harm presented by content on regulated services,[873] and the duty in section 54, which is specifically aimed at securing greater protections for people in the UK from harms that disproportionately affect women and girls. We therefore do not think it is necessary to show that a particular harm infringes users' (including women and girls') human rights in order to show that they should be protected from that harm.

A3.64 We also agree with comments made in the Paper that Article 17 would only be engaged in the most serious cases where the content or activity in question would undermine the fundamental values of the ECHR. Even though we have made amendments to clarify the scope of harms in the Guidance is limited to illegal content or content that is harmful to children, Article 17 will not be applicable to all the types of content and activity covered by the Guidance. We have therefore considered the proportionality of good practice steps given the pressing social need they are intended to address, and carefully balanced the rights of women and girls or other users who may be subjected to harms with the rights of others, including service providers and other users of online services. This includes, in particular, where good practice measures cover harms that are not criminal in nature and confer protection on adults as well as children. Examples of this include certain harms within scope of the misogynistic abuse and sexual violence and pile-ons and coordinated harassment harm areas, which may not meet the criminal threshold. While we acknowledge, in line with what we have said in the Illegal Content Judgements Guidance and Guidance on Content Harmful to Children, we would not normally expect content falling within scope of these harm areas to include the type of content that would attract a high degree of protection under Article 10 ECHR, we have carefully considered the balance of rights in relation to these areas and consider that, given the evidence of harm in relation to these areas, adults as well as children should have the opportunity to benefit from good practice in the Guidance relating to them. We have taken care to set out in the Guidance which good practice steps are applicable to the harm areas, and these harm areas in particular.

A3.65 As we explain below, we consider that the good practice steps will benefit a broader range of people beyond women and girls, should providers take the steps set out. We have explained the approach we have taken in relation to the feedback suggested by stakeholders, and the reasons for the good practice steps in the Guidance, throughout this statement.

A3.66 In response to BILETA's comments, the Guidance intends to address concerns about women and girls exercising their fundamental rights including in relation to participation online by including abuse, non-consensual intimate image abuse and harassment in the key harm areas set out in **Chapter 2** of the Guidance, with good practice steps and case studies which are targeted around those harms. We address stakeholder feedback on the case of *For Women Scotland Ltd v Lord Advocate* [2025] UKSC 16 in **Section 3** of this statement. In relation to BILETA's request for further content moderation interactions with freedom of expression, this is addressed in **Section 5** of this statement where we explain the reasons for our decision related to **Action 6** and 'automated detection' together with responses to other stakeholder comments raising freedom of expression and other concerns about content moderation practices.

[873] Section 3(2)(g) of the CA 2003.

## Freedom of expression and concerns about over-moderation by providers

### Stakeholder feedback

A3.67 A number of stakeholders commented that the draft guidance and rights impact assessment did not afford sufficient weight to the Article 10 ECHR right to freedom of expression of users and providers,[874] with some of these responses focusing more on the rights of men and boys who are users of those services. For example, one stakeholder argued, "Ofcom say in their consultation paper that people must not be silenced. In this way censorship can be seen as a harm. However, whereas they make this claim in relation to women; they are themselves silent, when it comes to seeing censoring men as a potential harm."[875] The same stakeholder raised concerns that Ofcom did not consider freedom of expression in the provisional rights impact assessment "other than setting out what the legislative framework says, what their proposed actions are, and simply stating they are compatible."[876]

A3.68 The Free Speech Union also queried "what exactly is 'misogynistic speech' and who gets to define it?" They said that while few people would deny that misogyny exists as a social problem, the term is both broad and subjective, stretching from the "unambiguously hateful to the merely provocative or politically unfashionable." It raised concerns that the language in the draft guidance "blurs the boundary between unlawful content and lawful expression that is simply considered undesirable by the regulator. Combined with the repeated assertion that firms 'should do more', this framing imposes a moral expectation that goes beyond the law, exerting pressure on providers to pre-emptively restrict lawful content."[877] LGB Alliance made a similar comment that "while the guidance seeks to address 'abusive, hateful or threatening content', it would be helpful if these terms could be clearly defined so as not to force service providers to punish users for legal expression."[878] Stakeholders also referred to a lack of clarity around "misgendering",[879] while The Free Speech Union said that the Guidance must recognise that "gender critical beliefs…must not be treated as a form of misogyny" and that gender critical speech is both politically contested and legally protected.[880] The Free Speech Union also noted that Article 10 ECHR requires that lawful political expression, particularly on matters of public interest, be given the highest level of protection. Their response referred to the case of *R v Casserly* [2024] EWCA Crim 25, which they said evidenced the principle that 'the greater the value of the speech in question, the weightier must be the justification for interference'. The response also noted that "Article 10 protects not only well received expression, but also that which offends, shocks or disturbs" and referenced the case of *Kwiecien v Poland* (2007) 48 EHRR 7 at [43].[881]

A3.69 Parity argued that several of the good practice steps promoted automated content moderation, proactive takedowns, and design-level filtration, yet failed to offer sufficient safeguards for due process or clarity on enforcement standards. It argued that "broad references to 'gender-based harms' in content moderation and user reporting systems may chill lawful speech, especially where definitions remain vague or ideologically loaded". It said this created a number of risks including mischaracterisation of dissenting views on gender,

---

[874] Response(s) to our February 2025 consultation: [✂]; The Free Speech Union, p.4; Name Withheld 2, p.4 M.I Evans, p.10; Parity, p.5; S.P Moxon, p.7; [✂].
[875] Response(s) to our February 2025 consultation: Name Withheld 2, p.4.
[876] Response(s) to our February 2025 consultation: Name Withheld 2, p.6.
[877] Response(s) to our February 2025 consultation: The Free Speech Union, p.1-2.
[878] Response(s) to our February 2025 consultation: LGB Alliance, p.2.
[879] Response(s) to our February 2025 consultation: The Free Speech Union p.4; LGB Alliance p.2.
[880] Response to our February 2025 consultation, The Free Speech Union, p.5 and 6.
[881] Response to our February 2024 consultation, The Free Speech Union, p.5 and 6.

abuse, or policy debates as 'gender-based harms'; censorship of controversial but lawful content, disproportionately affecting men or gender-critical voices; and a lack of transparency around what qualifies as 'harm,' leading to subjective or ideologically motivated enforcement. It added, "in the absence of strong procedural protections, such as user appeals, clear definitions, and transparent moderation logs, the practices risk fostering a censorship-prone environment and may actively harm free speech and equality under the law". It made suggestions for the Guidance and impact assessments, including that Ofcom should broaden stakeholder engagement to include voices from a wider range of affected groups, including organisations representing men and boys, LGBTQ+ users, and others at high risk online; replace "ideologically charged" terms like "gender-based harms (against women and girls)" with evidence-based, inclusive terminology that reflect "real-world harm profiles" and "ensure that content regulation frameworks do not infringe lawful speech or promote discriminatory platform policies".[882] Other stakeholders such as Evans, M.I.; Moxon, S.P.; [✂] and [✂] provided similar comments.

A3.70 The Classification Office raised concerns that social media companies may be more risk-averse when it comes to content moderation and that a risk-averse approach has the potential to infringe people's right to freedom of expression. It said, for example, services may systematically remove content that is discussing gender-based harms rather than perpetuating it.[883] BILETA made a similar comment concerning the risk of over-removal of content.[884]

A3.71 Meta Platforms Inc. also stressed that users have the fundamental right to engage in discourse on potentially controversial topics, as long as they do not violate platform policies and urged Ofcom to adopt a flexible approach when guiding services to reduce potentially disagreeable content circulation and acknowledge the unique challenges and opportunities presented by different services and technologies.[885]

### Our response

A3.72 We have discussed above the approach we have taken to the Article 10 ECHR rights of all affected individuals, including users, and service providers in relation to the content and activity within scope of the Guidance.

A3.73 As we have explained, we have made amendments to the Guidance to address stakeholder concerns about over-reach and over-moderation due to the harm areas in the draft guidance being too broad in scope. These changes include:

- Amending the harm area of 'online misogyny' to 'misogynistic abuse and sexual violence'. Only content and activity which is either illegal or primary priority content / priority content that is harmful to children under the Act will be within scope of this category. It focuses on misogynistic content and activity that is abusive and hateful towards women and girls and/or violent (including sexual violence). This definition ties directly to the most harmful types of content and activity, as set out under the Act.[886] We consider this approach is proportionate to address the impact of the harm.

---

[882] Response(s) to our February 2025 consultation: Parity, p.16.
[883] Response(s) to our February 2025 consultation: The Classification Office, p.4.
[884] Response(s) to our February 2025 consultation: BILETA, p.14.
[885] Response(s) to our February 2025 consultation: Meta Platforms Inc., p.8.
[886] As explained in Section 4 of the statement, this approach clarifies and refocuses the harm area to capture content that depicts or invokes sexual violence, including some types of pornography and extreme

- Drawing clearer links between the harm areas in **Chapter 2** of the Guidance with providers' duties under the Act relating to illegal harms or the protection of children to enable providers to consult clear definitions of content and activity which Ofcom has already set out as part of implementing the online safety regime.
- Drawing clearer links between good practice steps and one or more of the four harm areas focused on. We set these in context with amended case studies which are focused on harms occurring on different service types and impacting different people of different backgrounds. One the one hand, we explain in **Section 5** of this statement that providers could, for example use good practice steps related to user controls (**Action 7**) to address misogynistic abuse and sexual violence. This gives adults choice over the kind of content and activity they are exposed to and enables them to restrict their exposure to this content if they wish. On the other hand, we recommend deploying good practice that proactively identifies and removes content (per the 'Removal' good practices under **Action 6**) only to illegal content.
- Providing clarification in response to stakeholder feedback that 'gender critical beliefs' are protected by law, although we note that some forms of misgendering, as set out in the Children's Harms Guidance, are abusive and/or hateful and can constitute harassment.[887] We also expressly reference the principle set out in Handyside v UK in the Guidance, in response to stakeholder feedback: "Freedom of expression constitutes one of the essential foundations of such a [democratic] society, one of the basic conditions for its progress and for the development of every man. …. it is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no 'democratic society'."

A3.74 Further, service providers have specific duties under sections 22(2) and 33(2) of the Act to have particular regard, when deciding on and implementing safety measures and policies, to the importance of protecting users' right to freedom of expression within the law. Under section 22, Category 1 services will have additional duties in relation to freedom of expression, including the duty to prepare and publish impact assessments of contemplated and adopted safety measures and policies in relation to freedom of expression, as well as to keep the impact assessment updated. Those services will have a further duty to specify in a publicly available statement the positive steps that the provider has taken in response to an impact assessment to protect users' right to freedom of expression within the law. We consider that these duties will provide further safeguards to protect against stakeholder concerns regarding freedom of expression. We have added these duties as a 'foundational step' under **Action 1** of the Guidance.

A3.75 We also note that in accordance with its own rights to freedom of expression, a service provider has the right to decide the kinds of content it allows its users to upload, share, or generate on its service, provided it complies with the duties in the Act. We consider that the changes we have made to clarify the scope of harms covered by the Guidance, and the further

---

pornography. In line with feedback on the risks to sex workers, our approach intentionally does not capture all forms of pornography. In taking this approach, we have had careful regard to freedom of expression under Article 10 of the Convention, both in terms of adult users generating, uploading or sharing legal pornographic content and adult users being able to access such content.

[887] In Chapter 2, we also note that some forms of content and activity, such as criticising public figures, are protected by human rights law, to maintain a free and democratic society. For example, people have the right to criticise women politicians or other women in public life because they disagree with their actions or views.

context added to good practice steps and case studies, will allow providers to exercise this right while bearing in mind the risks of harm to women and girls from the most serious forms of content and activity which affect them.

## Concerns about discrimination against men and boys in breach of Article 14 ECHR

### Stakeholder feedback

A3.76 Several stakeholders raised concerns about the draft guidance being discriminatory in that it focuses on women and girls to the exclusion of men and boys, which they said infringed the right to freedom from discrimination of men and boys under Article 14 ECHR.[888] These responses made connected arguments that this may risk the infringement of the right to freedom of expression of men and boys. One response said that Ofcom "has simply declined to recognise even the possibility that online content even may be gender-neutral, never mind more harmful to men and boys."[889] Parity argued that "ideologically charged terms like "gender-based harms (against women and girls)" should be replaced with "evidence-based, inclusive terminology that reflects real-world harm profiles."[890] Other stakeholders made similar points.[891] One individual stated that Ofcom needs to protect all users whether they are male or female, saying that "as a process" section 54 of the Act "is very insufficient because it will only identify unequal harms between two groups, and only those which go in one direction".[892] Another stakeholder argued that although section 54 of the Act does not expressly reference harm to men and boys, to fail to address this would be to discriminate against men and boys in terms of protection from harm, "in contravention of the UK's obligations under the Sex Discrimination Act, Equality Act, and Human Rights Act."[893]

### Our response

A3.77 It is important to recognise that Parliament has set a duty for Ofcom to publish Guidance in relation to the online safety of women and girls, as set out in section 54 of the Act. The Guidance pursues a legitimate aim recognised by Parliament and, for the reasons set out in this assessment, we consider that the recommendations set out are proportionate to the aim pursued.

A3.78 Notwithstanding this, we do not consider that the Guidance, or the approach to the Guidance, represents an infringement of men and boys' rights under Article 14 ECHR. The following issues must be considered:

- Whether there has been a difference in treatment of persons in analogous or relevantly similar situations – or a failure to treat differently persons in relevantly different situations?
- If so, is such difference – or absence of difference – objectively justified? In particular, (a) does it pursue a legitimate aim; and (b) are the means employed reasonably proportionate to the aim pursued?[894]

---

[888] Response(s) to our February 2025 consultation: Moxon, S.P. p. 7; [✂];Evans, M.I.,p.10; [✂];
[889] Response(s) to our February 2025 consultation: Moxon, S.P., p. 7.
[890] Response(s) to our February 2025 consultation: Parity, p.16.
[891] Response(s) to our February 2025 consultation: [✂]; Evans, M.I. p.11; Name Withheld 1; Name Withheld 2, p.1; Moxon, S.P., p. 5; [✂].
[892] Response(s) to our February 2025 consultation: Name Withheld 2, p.3.
[893] Response(s) to our February 2025 consultation: [✂].
[894] European Court of Human Rights, Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention, paragraph 56

A3.79 As explained in **Section 3** of this statement, we do not consider that aims, purpose and substance of the Guidance represent a difference in treatment of women and girls compared with men and boys. We have addressed stakeholder feedback on this issue in detail in **Section 3** which explains 'who the Guidance is intended to support'. We also address this issue in our Equality Impact Assessment. As numerous consultation responses on this issue recommended, we have undertaken engagement with organisations representing men and boys and have considered their feedback before finalising the Guidance. This is explained throughout this statement. We have also added specificity to the Guidance to move away from broad references to 'gender-based harms' to focus on specific harms when discussing good practice steps which are particularly relevant to those harms. We still use the collective term 'gender-based harms' where appropriate. Throughout **Chapter 2** of the Guidance, we have referred to harms which impact upon men and boys. As explained in **Section 3** of our statement, we remain of the view that the good practice steps in the Guidance will benefit, and should be afforded to, all users, improving their experiences online. Ofcom's Codes of Practice, which set out ways in which providers can comply with enforceable duties under the Act, will also protect the interests of men and boys. The good practice steps set out in the Guidance represent a set of voluntary steps providers can take to protect all users.

A3.80 Not all differences in treatment – or failure to treat differently persons in relevantly different situations – constitute discrimination, but only those devoid of "an objective and reasonable justification". To the extent that the Guidance does represent a difference in treatment, Ofcom has a statutory duty under section 54 of the Act to produce guidance which focuses on harms which disproportionately impact women and girls. According to established case-law, Article 14 ECHR does not prohibit a member State from treating groups differently in order to correct "factual inequalities" between them; and in certain circumstances a failure to attempt to correct such inequality through different treatment may in itself give rise to a breach of Article 14 ECHR.[895] In **Section 4** of this statement we have explained the evidence we have relied on when deciding which harms the Guidance should focus on which have a disproportionate effect on women and girls. Any difference in treatment can therefore be objectively and reasonably justified. We have addressed stakeholder concerns about the privacy and freedom of expression rights of all individuals impacted by the Guidance, as well as providers' right to freedom of expression, as part of this rights assessment. We do not consider that the Guidance will affect the enjoyment of men and boys' human rights.

## The rights assessment should consider other additional factors or information

### Stakeholder feedback

A3.81 The Institute for Strategic Dialogue (ISD) said it "welcomed" Ofcom's inclusion of a rights assessment. However, it provided feedback that the impact assessments generally would benefit from "greater specificity, mainstreamed intersectional framing, and more robust engagement with the structural drivers of online VAWG, particularly regarding platform design and algorithmic systems". It said that the discussion on balancing rights in the rights assessment was "limited and abstract" and recommended a clearer articulation of the specific groups whose expression is most at risk due to online abuse, "such as women, girls, journalists, politicians, and activists, and marginalised communities e.g. LGBTQ+ and queer communities." It said that failure to act on systemic violence against women and girls can

[895] European Court of Human Rights, Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention, paragraph 44.

amount to "a de facto suppression of expression and participation, particularly for already marginalised groups".[896]

A3.82 Heriot-Watt University - University of Edinburgh commented that one of the factors listed in the provisional impact assessment in consideration of whether an infringement of a right is proportionate is whether it is "in accordance with the law" but that the rights assessment "does not comprehensively set these out". It noted that "firms are not just subject to the Online Safety Act and Human Rights legislation".[897]

A3.83 Image Angel said it believed that all of the impact assessments at consultation "could go further in recognising the unique vulnerabilities of women, girls, and sex workers in the digital economy -particularly on adult platforms". It noted "the critical role of forensically capable, survivor-informed technology in mitigating these harms."[898]

A3.84 The Office of the Derbyshire Police and Crime Commissioner reiterated the importance of embedding intersectionality more explicitly throughout the Guidance and impact assessments. They said that this will help ensure that the diverse experiences of women and girls – particularly those from marginalised communities – are fully considered and addressed.[899]

### Our response

A3.85 In response to ISD and other stakeholders on the importance of embedding intersectionality, we have explained our approach in **Section 3** 'who the Guidance is intended to support' to groups, including minority groups, whose right to freedom of expression is most at risk. We agree with stakeholders that many different people can experience the harms we focus on in the Guidance, and that a wide range of factors can impact risk and vulnerability. We have reflected this in the Guidance[900] and discuss relevant impacts in our equality impact assessment. In explaining our approach to pile-ons and coordinated harassment in **Chapter 2** of the Guidance, we acknowledge the impact on women in public life and have reframed this harm area to primarily focus on them, and the chilling impact this has on women and girls' participation more broadly.

A3.86 In response to Heriot-Watt University - University of Edinburgh, 'in accordance with the law' in our provisional rights assessment set out part of the legal test for justifying interferences with a right under the HRA 1998. We acknowledge that service providers are subject to a variety of legal duties. However, Ofcom must act in accordance with its powers and duties in accordance with the Act and other legislation set out in the Legal Annex (**Annex A2**) to this document, as well as having regard to established jurisprudence on these issues.

A3.87 In response to Image Angel, the Guidance recognises impacts on women on adult services and their rights. As we explain in **Sections 4** and **5** of this statement, we have taken into account evidence from stakeholders concerning these impacts and rights when finalising the Guidance. **Chapter 1** of the Guidance refers to specific evidence about the unique risks faced by these users.

---

[896] Response(s) to our February 2025 consultation: Institute for Strategic Dialogue (ISD), p.14 and 15.
[897] Response(s) to our February 2025 consultation: Heriot-Watt University - University of Edinburgh, p13.
[898] Response(s) to our February 2025 consultation: Image Angel, p.11.
[899] Response(s) to our February 2025 consultation: The Office of the Derbyshire Police and Crime Commissioner, p.4.
[900] For example, Action 2 good practice.

## Privacy and data protection

A3.88 We discuss feedback we received concerning the Article 8 ECHR rights of women and girls in the section above. This section focuses on feedback we received concerning the interwoven issues of all users' right to privacy and data protection. These two related issues were often conflated in stakeholder feedback, and we have therefore addressed as one section.

### Stakeholder feedback

A3.89 The ICO provided detailed feedback in its response to the consultation related to chapters, actions, good practice steps and case studies. Feedback on these specific points is addressed in **Section 5** of this statement. The ICO referred to the joint statements made with Ofcom[901] which recognise that online safety and data protection interact in a variety of ways and set out the overall ambition to ensure coherence across online safety and data protection requirements and promote compliance with both regimes. The ICO said that it recognised the importance of consistent messages to businesses, and it would continue working hand in hand with Ofcom to ensure that all users can enjoy a safe and privacy-respectful online experience. It noted that it was "pleased that Ofcom has incorporated references to data protection in several chapters of the draft guidance". It suggested the following overarching improvements and clarification:[902]

- Given that most good practice steps are likely to involve the processing of personal information, a general reminder of the need to comply with data protection law at the start of the Guidance would help ensure that services take the necessary steps when handling personal information.
- The Guidance should refer services to the ICO's guide to UK GDPR which offers guidance on carefully assessing the necessity and proportionality of personal information processing, determining the minimum amount of personal information required to achieve the intended purpose, and selecting the most appropriate lawful basis for processing.
- More clarity in the Guidance about the status of the good practice steps and their relationship to compliance with the duties of the Act as this would provide services with clearer information to enable them to make an informed choice about whether the legal obligation lawful basis is appropriate for their processing.
- The Guidance could usefully refer services to the ICO's guidance on lawful bases and remind them that under data protection law they will need to ensure that they have a lawful basis for their processing under Article 6 UK GDPR.
- It would be beneficial for Ofcom to remind services that, as data controllers, they remain accountable for their obligations under data protection law when implementing any of the steps set out in the Guidance, including if they implement the steps as set out in the case studies.
- The ICO's Age Appropriate Design Code (the Children's Code) explains how service providers can ensure that they appropriately safeguard children's personal data. Signposting to the ICO's Children's Code in the Guidance will help service providers who are subject to compliance with the Act and data protection law.

[901] Ofcom and ICO, 2025. Online safety and data protection: a joint statement by Ofcom and the Information Commissioner's Office; Ofcom and ICO, 2024. Online safety and data protection: A Joint Statement by Ofcom and the Information Commissioner's Office on Collaboration on the Regulation of Online Services.
[902] Response(s) to our February 2025 consultation: Information Commissioners Office (ICO), p.2-3.

A3.90 Other stakeholders noted that users (including young people and adults caring for them) must have access to clear information about how their data is used.[903]

A3.91 BILETA referred to the "critical need to proactively evaluate the potential consequences of the proposed guidance and AI-driven safety tools on the fundamental rights, data privacy, and equality of women and girls." It pointed out that increasing reliance on extensive datasets for content moderation and deepfake detection introduces substantial privacy and bias concerns, highlighting the need for Data Protection Impact Assessments. [904]

A3.92 One individual noted that the approach taken in the provisional rights assessment appeared to "offload the responsibility for privacy onto the Information Commissioner's Office". They raised concerns that "the nine actions would see providers monitoring legal content, because the approach taken is to cut further into freedom of expression, and classify more legal content as harmful. That has huge implications for privacy, and Ofcom simply haven't considered it." They said that, in their opinion, "the huge impact on privacy is unpalatable."[905]

A3.93 Do-Ngoc, T. and Carmel, E. said that Ofcom should provide clearer guidance for platforms on how to avoid reinforcing surveillance harms, particularly for women and girls in minoritised communities. They noted that while they considered that content moderation and other platform safety interventions are necessary, this must not lead to the "over-policing or surveillance of already marginalised groups". This response said that the Guidance should explicitly state that providers' data collection and monitoring practices must uphold privacy rights and be subjected to vigorous human rights assessments. It noted that this is especially important given that racially minoritised women, LGBTQ+ communities, and those from low-income backgrounds, are more likely to experience both digital harms and disproportionate surveillance.[906]

### Our response

A3.94 We have addressed the ICO's overarching points by adding to **Chapter 1** of the Guidance. We have explained the approach to clarifying the link between good practice steps and duties under the Act in **Section 3** of the statement. We have implemented the specific suggestions for chapters, actions, good practice and case studies as discussed in **Section 5** of this statement. We did not consider it to be necessary to reference case studies specifically when providing a statement at the outset of the Guidance that providers remain accountable for their obligations under data protection law when implementing any of the steps set out in the Guidance.

A3.95 In response to BILETA's suggestion regarding Ofcom proactively evaluating AI driven safety tools, we have referenced ICO guidance where relevant within the Guidance to ensure that service providers have a holistic understanding of their online safety and data protection

[903] Response(s) to our February 2025 consultation: Do-Ngoc, T. and Carmel, E., p.7.
[904] Response(s) to our February 2025 consultation: BILETA, p.22. It stated "For instance, in the context of deepfake detection—a significant threat involving non-consensual intimate imagery and online harassment predominantly targeting women and girls—a Fundamental Rights Impact Assessment like the one required under Article 27 of the EU AI Act would scrutinize whether the deployment of detection technologies could infringe upon rights such as freedom of expression, non-discrimination, data protection, or privacy."
[905] Response(s) to our February 2025 consultation: Name Withheld 2, p.5 and 6.
[906] Response(s) to our February 2025 consultation: Do-Ngoc, T. and Carmel, E., p.7.

duties. Further, we have included, in the Guidance, reference to protections against concerns about privacy, bias and freedom expression in relation to algorithmic systems.[907]

A3.96 As noted above in relation to freedom of expression, section 22(3) (user-to-user) and section 33(3) (search) of the Act place obligations on providers, when deciding on, and implementing, safety measures and policies, to have to have particular regard to the importance of protecting users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of the service (including, but not limited to, any such provision or rule concerning the processing of personal data). As explained above, Category 1 services have additional duties under section 22 to prepare and publish impact assessments of contemplated and adopted safety measures and policies in relation to privacy impacts, as well as to keep the impact assessment updated. Those services will have a further duty to specify in a publicly available statement the positive steps that the provider has taken in response to an impact assessment to protect users' right to privacy. We consider that these duties will provide further safeguards to protect against stakeholder concerns regarding privacy impacts. We have included reference to these duties as a "foundational step" within **Action 1** of the Guidance.

A3.97 We address our approach to the scope of the Guidance, including content that is not illegal, above in relation to freedom of expression concerns. We consider that the narrowing of the scope and greater clarity around how good practice steps apply to particular harms will minimise the impacts on freedom of expression and privacy.

A3.98 We have incorporated appropriate protections in relation to the privacy rights of users into the Guidance, incorporating amendments and signposting to ICO Guidance as suggested by the ICO. This will ensure that service providers are aware of the relevant law and guidance when dealing with issues impacting users' privacy and data protection rights. We consider that this appropriately safeguards against concerns raised by stakeholders that providers must uphold data protection and privacy rights.

## Our overall conclusion on rights

A3.99 In developing the Guidance, and taking into account stakeholder feedback on these issues, we have carefully considered whether the recommendations made would constitute undue interference with users' and interested persons' fundamental rights, such as their rights to privacy, freedom of expression, and freedom from discrimination (Articles 8, 10, and 14 ECHR). We have further carefully considered whether the recommendations would constitute undue interference with the right to freedom of thought, conscience and religion and freedom of association (Articles 9 and 11 ECHR) and the right to peaceful enjoyment of one's possessions (Article 1 of Protocol No. 1 ECHR). In addition, we have considered whether the recommendations in the Guidance would constitute interference with services' freedom of expression rights. Our assessment is they do not. We confirm our view in the provisional assessment that the Guidance draws upon measures already set out in the Illegal Content Codes and Risk Assessment Guidance and Protection of Children Codes and Risk Assessment

[907] See Action 2 of the Guidance where we include a good practice step that services can evaluate algorithmic systems such as content moderation and recommender systems for a variety of risks in relation to bias and discrimination. We also note in the foundational steps under Action 6, user-to-user services should also ensure that children's recommender feeds exclude or limit the prominence of content harmful to children, which may also involve undertaking algorithmic assessments.

Guidance, where those obligations have been considered in detail. We therefore have not separately considered any relevant impacts in relation to those 'foundational steps.'

A3.100 We continue to recommend that providers apply the good practice steps set out in the Guidance to adults as well as children. As we have explained, we have also decided not to narrow the scope of the Guidance in certain areas to only include illegal harms. We have carefully considered responses from stakeholders related to freedom of expression; however, we consider it to be proportionate and in line with section 54 of the Act for the Guidance to retain information about the impacts of these harms areas which span both illegal content and content harmful to children. This is in line with evidence that this content and activity disproportionately affects women and girls and evidence about the impacts on their human rights. Given the clearer scope of harms the Guidance applies to, the specificity added to **Action 6** concerning removal of content to align with the most serious harms, and the further contextual changes we have made to the Guidance as we have described above including statements about the application and safeguarding of rights, we consider that this is proportionate in light of the legitimate aims the Guidance pursues. We have explained throughout **Section 5** how we expect our recommendations to benefit women and girls in terms of protecting them from these harms, as well as other groups who experience these harms. Taking into account those benefits, we consider any interference with the rights of others that might result from the inclusion of the good practice steps (including the case studies) is proportionate in the context of the Guidance and the harms it seeks to address. In particular, we note the Guidance does not require providers to take any particular good practice step – providers will assess the most suitable course of action depending on the nature of their service, taking into account the interests of their users.

A3.101 We consider that our approach appropriately balances the Article 8 ECHR rights of all users, including women and girls, who are at risk of being impacted by the harms set out in the Guidance, as well as their right to engage and express themselves freely. In relation to other issues concerning privacy and data protection rights of all users, we consider that these issues are inextricably linked, and these are therefore assessed together. We remain of the view that, some of our good practice proposals, illustrated by case studies, are likely to involve the collection and processing of personal data of users. Having considered feedback from ICO on our proposals, we have considered further impacts on the privacy and data protection rights of users and addressed these in the ways explained above and throughout **Section 5** of this statement. Providers that process personal data in taking the good practice steps set out in the Guidance will need to comply with relevant data protection legislation and should refer to relevant guidance from the ICO, as explained throughout the Guidance. Overall, where providers comply with data protection laws, we consider that the privacy impact of the good practice steps is limited and proportionate to the aims and benefits of the Guidance.

## Equality impact assessment

A3.102 Section 149 of the EA 2010 imposes a duty on Ofcom, when carrying out its functions, to have due regard to the need to eliminate discrimination, harassment, victimisation and other prohibited conduct related to the following protected characteristics: age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex and sexual orientation. The EA 2010 also requires Ofcom to have due regard to the need to advance equality of opportunity and foster good relations between persons who share specified protected characteristics and persons who do not.

A3.103 Section 75 of the Northern Ireland Act 1998 ('the 1998 Act') also imposes a duty on Ofcom, when carrying out its functions relating to Northern Ireland, to have due regard to the need to promote equality of opportunity and have regard to the desirability of promoting good relations across a range of categories outlined in the 1998 Act. Ofcom's Revised Northern Ireland Equality Scheme explains how we comply with our statutory duties under the 1998 Act.[908]

A3.104 To help us comply with our duties under the EA 2010 and the 1998 Act, we assess the impact of our proposals on persons sharing protected characteristics and in particular whether they may discriminate against such persons or impact on equality of opportunity or good relations.

A3.105 When thinking about equality we consider the potential impacts more broadly and not just in relation to those groups of persons that share protected characteristics identified in equalities legislation (see paragraph 4.7 of our impact assessment guidance[909]).

A3.106 In particular, section 3(4) of the CA 2003 also requires us to have regard to the needs and interests of specific groups of persons when performing our duties, as appear to us to be relevant in the circumstances. These include:

- the vulnerability of children and of others whose circumstances appear to us to put them in need of special protection;
- the needs of persons with disabilities, older persons and persons on low incomes; and
- the different interests of persons in the different parts of the UK, of the different ethnic communities within the UK and of persons living in rural and in urban areas.

A3.107 We examine the potential impact our policy is likely to have on people, depending on their personal circumstances. This also assists us in making sure that we are meeting our principal duty of furthering the interests of citizens and consumers.

## Our provisional equality impact assessment

A3.108 We set out that we had carefully considered the impacts of our proposals on individuals with protected characteristics and any other potential risks of discrimination, as well as impacts on equality of opportunity and fostering good relations. We also considered wider impacts on other groups, such as people from different socio-economic groups and vulnerable groups, including children.

A3.109 We set out that the 'foundational steps' outlined in the draft guidance reflect Codes measures and information from our risk assessment guidance, that we have already set for service providers. We explained that these codes measures had already undergone equality impact assessments and we decided that they were likely to have a positive impact on persons with protected characteristics, so we did not re-assess their impact.

A3.110 We assessed the 'good practice steps' outlined in the draft guidance and did not envisage that they would have a detrimental impact on any particular group of people. We stated that we expect the foundational and good practice steps to improve online safety for all groups, extending beyond women and girls who are the specific focus of the draft guidance, to other individuals with protected characteristics and vulnerable groups, in line with the broader aims of the Act.

[908] Ofcom, 2025. Revised Northern Ireland Equality Scheme for Ofcom.
[909] Ofcom, 2023. Impact assessment guidance.

A3.111 We stated that our proposals aimed to empower users, improve equality of opportunity and foster positive interactions between users. We considered this would benefit other groups of people beyond women and girls (who are the primary focus). For example, we considered that our proposals for good practice to address online gender-based harms in transparency reporting could improve users' understanding of how service providers address these types of harms. We also considered our proposal for good practice in relation to safer defaults, such as bundling settings for services with many features or frequent updates, were valuable for those at risk of coercive and controlling behaviour and stalking, as they would ensure users always have the most secure and private options. We considered that they could also increase accessibility for younger and older users and those with disabilities by reducing complexity, simplifying navigation and making it easier for users to make choices about their settings. We noted that other proposals relating to abusability evaluations and product testing encouraged providers to understand diverse user experiences and create an inclusive online environment. We suggested that red teaming may take into account abuse such as threats and harassment toward individuals with protected characteristics and help prevent it. We concluded that, overall, we expected a wide range of users to benefit from implementing our good practice proposals.

A3.112 We noted that no single method is completely free of bias and our draft guidance was designed to help service providers mitigate potential adverse impacts on particular groups. While our initial analysis did not identify any adverse effects, we considered it did identify some potential risks, which could occur as an unintended consequence of our proposals, or if they were implemented without consideration of users with protected characteristics. We considered these risks in setting out our proposals for good practice steps and believed that they could generally be mitigated as set out in the following paragraphs.

A3.113 We considered that the complexity of some good practice steps might negatively impact service usability, particularly for younger users and those with disabilities. For example, creating dedicated reporting and review channels for online gender-based harms could increase choice overload. We also recognised a risk of excluding certain groups if features are not well-designed. To mitigate these risks, we emphasised the importance of service providers implementing these practices in a way that is inclusive, user-friendly and considerate of users' emotional and cognitive states. We pointed to the draft guidance, where we proposed this could be achieved through gender-inclusive, accessible and regularly reviewed terms of service and community guidelines which respond to trends in online gender-based harms. We also proposed that, additionally, through service design and prevention, service providers can prevent harm before it occurs by testing products to identify potential routes for abuse and making necessary changes.

A3.114 We acknowledged that certain good practice steps may risk being misused by malicious actors. For example, good practice proposals around fact-checking and labelling for gendered disinformation could result in false positives related to gender identity and sexual orientation content, as malicious actors might exploit reporting features to trigger these processes. To mitigate this risk, we suggested service providers implement robust verification processes and provide a clear appeal mechanism, as suggested in the draft guidance.

A3.115 We concluded that, overall, possible risks could be mitigated as explained and were outweighed by the benefits of providers implementing our recommendations. We stated that, the draft guidance is designed to engage, inform and reduce online gender-based harms and therefore considered that our proposals would have a generally positive impact on individuals with protected characteristics. We also recognised that there may be opportunities to further advance equality of opportunity and foster good relations between persons who share

protected characteristics and persons who do not. We indicated that we would continue to assess the potential impacts of our good practice proposals as our evidence base and understanding improve over time.

## Stakeholder feedback

A3.116 We received feedback that the equality impact assessment should focus more strongly on intersectionality.[910] We also received feedback to consider intersectionality across the Guidance: several stakeholders called on us to focus more on marginalised women's experience and/or intersectional risks, particularly for women and girls from minority ethnic groups and/or with disabilities, and provided evidence about how harms manifest in these contexts.[911]

A3.117 For example, the Commissioner for Children and Young People (NICCY) said it "would have welcomed more of a focus on the intersectionality of girls' vulnerabilities in both the good practice steps and case studies and references to Section 75 duties" of the 1998 Act.[912] The Women's Aid Federation of England recommended that "transparency documentation" "include specific data on the experiences of marginalised groups, including communities with multiple marginalisations, for example, disabled women."[913] BILETA noted algorithms, as well as automated filters or word lists, should be tested for unintended bias to ensure that content by women of colour isn't misclassified as harassment or hate speech.[914] They also noted that algorithmic impact assessments should include "rigorous bias assessments" to address the "statistical breakdowns in the accuracy of deepfake detection models across different racial groups" and recommended that the Guidance include guidance on conducting thorough impact assessments to address bias.[915]

A3.118 In addition, several stakeholders called on us to focus more good practice steps on girls.[916]

A3.119 We also received feedback that we should place greater emphasis on the experiences of LGBTQ+ people, particularly transgender people.[917] Galop also raised concerns that "social

---

[910] Response(s) to our February 2025 consultation: Barker, K., p.16; Harrison, J., p.14-15; Image Angel, p.9-10; Institute for Strategic Dialogue (ISD), p.13; [✂]; Office of the Derbyshire Police and Crime Commissioner, p.4.
[911] Response(s) to our February 2025 consultation: Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales, p.4; Galop, p.1; Glitch, p.1; Equality Now, p.1; Office of Derbyshire Police and Crime Commissioner, p.4; Women's Aid Federation of England, p.4; Antisemitism Policy Trust, p. 1-2; End Violence Against Women Coalition, p.3; Girlguiding, p.4; End Violence Against Women Coalition (Annex 2), p.4; [✂]; Kira, B., Asser, Z, Ruiz, J, p. 2; Mayor of London, p.6; Scotland Nations Workshop
[912] Response(s) to our February 2025 consultation: Commissioner for Children and Young People (NICCY), p.11.
[913] Response(s) to our February 2025 consultation: Women's Aid Federation of England, p.17.
[914] Response(s) to our February 2025 consultation: British and Irish Law, Education and Technology Association (BILETA), p.6,8, 12, 20.
[915] Response(s) to our February 2025 consultation: British and Irish Law, Education and Technology Association (BILETA), p.23.
[916] Response(s) to our February 2025 consultation: Barker, K. p.9; Domestic Abuse Commissioner for England and Wales and Victims' Commissioner for England and Wales p.6; NSPCC, p.13; Internet Matters, p.17; Plan International UK, p.15; British and Irish Law, Education and Technology Association (BILETA), p.2; Northern Ireland Commissioner for Children and Young People, p.11; Girlguiding, p.6-8.
[917] Response(s) to our February 2025 consultation: Galop, p.2-5; [✂]; Do-Ngoc, T., Carmel, E., p.1 [✂]; Institute for Strategic Dialogue, p.5; Cyber Helpline, p.1; Parity, p.11; NSPCC, p.7; Minderoo Centre for Democracy & Technology, p.2; Equality Now, p.1; Office of the Derbyshire Police and Crime Commissioner, p.4; Evans, M.I., p.6; [✂]; Equality Now, p.1; Name Withheld 3; Ofcom / Translucent Meeting, 26 March 2025.

media platforms can sometimes conflate LGBTQ+ content as harmful, therefore limiting access to specialist LGBTQ+ information, support and community networks".[918]

A3.120 In addition, several stakeholders raised concerns that the equality impact assessment and the draft guidance did not consider men and boys**.**[919] Several stakeholders noted Ofcom's responsibilities in relation to our role as a public authority, and our duties under the EA 2010 and HRA 1998. They said this requires Ofcom to consider harms to men and boys.[920] For example, Parity asked that Ofcom's assessments consider "the full spectrum of gender-based and gender-neutral harms using transparent methodologies and disaggregated data". [921] They also noted that Ofcom should engage with "organisations representing men and boys, LGBTQ+ users and others at high risk online", which we address in **Section 3.** They also asked us to "replace ideologically charged terms like 'gender-based harms (against women and girls)' with evidence-based inclusive terminology that reflects real world harm", which we address in **Section 3.**

A3.121 As noted in **Section 3**, some individuals and organisations also provided evidence that men and boys experience gender-based harms and detailed the particular risks they face online. They argued this should be further explored in the Guidance, or that because men and boys are affected (in some cases disproportionately) the harm areas should not be the focus of the Guidance.[922]

A3.122 One stakeholder suggested that we should "explicitly state that data collection and monitoring practices must uphold privacy rights and be subjected to rigorous human rights impact assessments". They argued that this is especially important given that racially minoritised women, LGBTQ+ communities, and those from low-income backgrounds are more likely to experience both digital harms and disproportionate surveillance. [923]

## Our response

A3.123 As noted in **Section 3**, we agree that different people can experience the harms we focus on in the Guidance and that a wide range of factors can impact risk and vulnerability. As noted in A3.102-A3.104, the equality impact assessment helps us comply with our duties under the EA 2010 and the 1998 Act.

A3.124 In **Chapter 2**, we have retained our position that online gender-based harms are systemic and intersectional. In **Chapter 3**, we have retained the good practice step under **Action 1** recommending that providers should consider intersectionality of harms in their governance and decision-making processes. In **Chapter 4**, we set out how a provider can improve its automated moderation tools to detect intersectional forms of online abuse affecting Black women (**Case study 14**).

A3.125 In addition, we have made changes in the Guidance to further highlight intersectionality. In **Chapter 2**, we have included additional evidence that women and girls with additional factors,

---

[918] Response(s) to our February 2025 consultation: Galop, p.1.
[919] Response(s) to our February 2025 consultation: Evans, M.I., p.4-6, 9; Parity, p.5-10, 14; Men and Boys Coalition Charity, p.1; Moxon, S.P., p.4-8; Name Withheld 1, p.1-3; Name Withheld 2, p.5-6; [✂]; [✂].
[920] Response(s) to our February 2025 consultation: Evans, M.I., p.2; Parity, p.4; Moxon, S.P., p.4; Name Withheld 2, p.6; [✂]; [✂].
[921] Response(s) to our February 2025 consultation: Parity, p.16.
[922] Response(s) to our February 2025 consultation: Evans, M.I., p.1; Parity, p.1**;** Men and Boys Coalition Charity, p.4; [✂]; [✂].
[923] Response to our February 2025 Consultation: Do-Ngoc, T., Carmel, E., p.8.

including age, race, ethnicity, socio-economic status, sexual orientation, gender identity, disability and religion, experience heightened and specific risk and impacts of harm.[924]

A3.126 Under **Action 1,** the new **Case study 3** on engaging with subject-matter experts notes that service providers should meet with organisations that represent specific groups at risk of harm – such as groups representing LGBTQ+ or immigrant survivors and victims – to include intersectional experiences of abuse. Under **Action 2**, we have retained the case study on gender-sensitive risk assessment (**Case study 5**) and noted that both girls and boys with multiple protected characteristics experience unique and compounding risks in their risk assessments.

A3.127 In response to Galop's concerns about the misinterpretation of LGBTQ+ content as harmful , we note in **Case study 4** on external oversight for content moderation under **Action 1** that an example of misapplication of content moderation policies can be the removal of non-prohibited content can include images of LGBTQ+ couples kissing.

A3.128 As set out **Section 2,** we have also engaged with a wide range of stakeholders in different formats, including hosting roundtables with organisations representing men and boys and young people. In **Section 4** (from paragraph 4.18), we explain our response to stakeholder feedback querying our approach and evidence base on identifying harms that 'disproportionately affect' women and girls. In short, we confirm our approach set out at consultation to group content and activity that disproportionately affects women and girls into four key harm areas to outline the different ways harms manifest. We also clarify our position that 'disproportionately affects' can mean that women and girls are more likely to experience online gender-based harms or that the impact on women and girls is distinct. In addition, we also note that under-reporting— including among men and boys —may affect our understanding of who experiences online gender-based harms, and to what extent, and have included examples in **Chapter 2** about how men and boys are impacted by harms. For example:

a) We have incorporated additional evidence, including evidence provided by respondents, about how misogynistic abuse manifests and we also recognise that this harm effects men and boys.[925]
b) We note that pile-ons and coordinated harassment can be perpetrated against men and boys, as well as women and girls. However, research demonstrates that this harm has a disproportionate impact on women in public life and the kinds of content they are targeted with are often misogynistic and sexually violent.[926]
c) We also note that there are some types of image-based sexual abuse that disproportionately affect men, such as sextortion.[927]

A3.129 In addition, we have also amended the draft case study 11 on gender-sensitive recommender systems to focus on young boys' exposure to content depicting misogynistic abuse and sexual violence on a video-sharing service (now **Case study 10**).

---

[924] See, for example, UNESCO, 2023. Exposing Technology-Facilitated Gender-Based Violence in an Era of Generative AI; Gray, K. L. (2011). INTERSECTING OPPRESSIONS AND ONLINE COMMUNITIES: Examining the experiences of women of color in Xbox Live. *Information, Communication & Society*.
[925] See, for example, Ofcom, 2025. Online Experiences Tracker – Wave 8; Feine, J., Gnewuch, U., Morana, S. and Maedche, A., 2020. Gender bias in chatbot design, *Chatbot Research and Design*; Men and Boys Roundtable, 29 May 2025.
[926] See, for example, Ofcom, 2025. Online Experiences Tracker – Wave 8;
[927] See, for example, Revenge Porn Helpline (Papachristou, K.), 2025. Revenge Porn Helpline 2024 Report.

A3.130 We address feedback regarding the use of the term "gender-based harms" in paragraph 4.14 in this statement.

A3.131 As set out in the Rights Assessment (from paragraph A3.47) we have taken a number of steps to ensure that the Guidance includes evidence on the experiences of children and young people online.

A3.132 In response to the feedback from Do-Ngoc, T. and Carmel, E. we note in the rights assessment that we have incorporated appropriate protections as regards the privacy rights of users into the Guidance, incorporating suggestions from the ICO. This will ensure that service providers are aware of the relevant law and guidance when dealing with issues impacting users' privacy and data protection rights. We consider that this appropriately safeguards against concerns raised by stakeholders that providers must uphold data protection and privacy rights.

A3.133 In response to the feedback from the Institute for Strategic Dialogue (ISD) and the University of York, we note in **Section 3** of this statement our plans to publish a report in the first half of 2027 to share information about what services are doing to address online gender-based harms. As set out in **Section 2** of this Statement, we also expect to update the Guidance to reflect changes to Ofcom's implementation of the Act, such as any new Code measures we introduce or changes we make to existing ones, as well as to reflect emerging online gender-based harms and technologies.

## Our overall conclusion on equality impacts

A3.134 We are confirming our provisional assessment and we set out further considerations and examples below. In developing the Guidance, and taking into account stakeholder feedback on these issues, we have carefully considered the impacts of our recommendations in the Guidance on individuals with protected characteristics and any potential risks of discrimination, as well as impacts on equality of opportunity, and fostering good relations. We have also considered wider impacts on other groups, such as people from different socio-economic groups and vulnerable groups, including children, as well as people in the different parts of the UK, of the different ethnic communities within the UK and of persons living in rural and in urban areas. We provide examples of the positive impacts on these groups at paragraph A3.138 in this statement.

A3.135 As noted in the provisional assessments, the 'foundational steps' outlined in the Guidance reflect Codes measures and information from our risk assessment guidance we have already set for service providers elsewhere. These steps have undergone previous equality impact assessments, which concluded that they are likely to have a positive impact on persons sharing protected characteristics. We did not consider any to have a detrimental impact on those groups.

A3.136 We do not envisage that the remainder of the Guidance would have a detrimental impact on any particular group of people. We note the focus of the Guidance, as required by section 54 of the Act, is on content and activity "which disproportionately affects women and girls." We acknowledge that gender-based harms are intersectional and different people can experience the harms we focus on in the Guidance, and that a wide range of factors can impact risk and vulnerability, including protected characteristics. We have explained our approach above and consider the addition of intersectional considerations in the Guidance, including when describing the harm areas, good practice, and case studies to adequately address these issues. We also recognise that the harms in the Guidance affect men and boys. As set out in our response to stakeholder feedback both here and in the rights assessment, we consider that

the Guidance, and our approach to the Guidance, is compliant with Ofcom's obligations, including under the EA 2010, the Northern Ireland Act 1998 and the HRA 1998.

A3.137 Taken together, we are confirming our provisional view that we expect the Guidance to improve online safety for all groups, extending beyond women and girls who are the specific focus of the Guidance, to other individuals with protected characteristics, in line with the broader aims of the Act.

A3.138 We remain of the view that our good practice steps aim to empower users, improve equality of opportunity and foster positive interactions between users, benefitting different groups of people as set out in paragraph A3.134 in this statement. For example:

a) The good practice step that services should set policies that directly address online gender-based harms prevalent on their service can help reduce misogynistic abuse and sexual violence, such as misogynoir or deliberate persistent misgendering and therefore improve users' experience.

b) The good practice step of using external assessors to monitor the threat landscape, including local partners with regional and cultural knowledge with expertise in highly contextual risk areas such as stalking and coercive control will help ensure that the issues local to different ethnic communities within the UK and to communities in rural and urban areas are considered.

c) The good practice step to address online gender-based harms by improving transparency can improve users' understanding of how service providers address these types of harms. In addition, the good practice step on publishing information and findings in a clear and accessible way to a range of audiences by producing versions of reports tailored to different audiences including children and young people will help ensure that all users can engage with the information.

d) The good practice step to clearly and comprehensively explain default settings, bundles, and account access options to users can make important safety information more accessible for everyone. Services can explain their settings through visual elements, audio-visual elements, or interactive elements. This can benefit children, some disabled people, or people who are unable to read the language a service is provided in.

e) The good practice steps aimed at reducing the circulation of online gender-based harms can foster good relationships between different groups of people by downranking content that spreads disinformation about vulnerable groups and by reducing the prominence of content containing misogynistic abuse and sexual violence. The steps also encourage service providers to consider media literacy interventions that may be necessary to address particular harms or the needs of children and vulnerable groups.

A3.139 Overall, we expect a wide range of users to benefit from implementing our good practice proposals.

A3.140 As noted in our provisional assessment, we note that no single method is completely free of bias and our Guidance is designed to help service providers mitigate potential adverse impacts on particular groups. While our analysis did not identify any adverse effects, it did identify some potential risks, which could occur as an unintended consequence of our proposals, or if they are implemented without consideration of users' identities. We have considered these risks in setting out our proposals for good practice steps and the considerations in each case study and believe that they can be generally mitigated when applied appropriately.

A3.141 For example, the good practice step that services should share information regarding what kinds of posts might trigger downranking, de-prioritisation, or exclusion for transparency could improve transparency and accountability which can be helpful to groups such as LGBTQ+ and people of certain political opinions[928] who may see their content downranked. However, services should carefully consider the benefits and risk of notifying users as malicious users could use this information to bypass safety measures or ensure content harmful to groups of individuals is allowed to proliferate.

A3.142 In addition, the good practice step recommending that services engage with subject-matter experts, particularly those with experience of supporting survivors and victims, when designing privacy and security settings could lead to providers relying on the views of subject matter experts as individuals who may hold personal biases. However, services can mitigate this risk by engaging with a variety of stakeholders.

A3.143 Overall, we retain our position of the provisional assessment that any possible risks can be mitigated in the ways we have explained and are outweighed by the benefits of providers implementing our recommendations. The Guidance is designed to engage, inform and reduce online gender-based harms. We therefore consider that our recommendations will have a generally positive impact on individuals with protected characteristics. As set out in the provisional assessment, we also recognise that there may be opportunities to further advance equality of opportunity and foster good relations between persons who share protected characteristics and persons who do not. We expect our evidence base and understanding to improve over time, and we will continue to assess the potential impacts of the Guidance.

## Welsh language assessment

A3.144 The Welsh Language (Wales) Measure 2011 made the Welsh language an officially recognised language in Wales. This legislation also led to the establishment of the office of the Welsh Language Commissioner who regulates and monitors our work. Ofcom is required to take Welsh language considerations into account when formulating, reviewing or revising policies which are relevant to Wales (including proposals which are not targeted at Wales specifically but are of interest across the UK).[929]

A3.145 Where the Welsh Language Standards are engaged, we consider the potential impact of a policy proposal on (i) opportunities for persons to use the Welsh language; and (ii) treating the Welsh language no less favourably than the English language. We also consider how a proposal could be formulated as to have, or increase, a positive impact, or not to have adverse effects or to decrease any adverse effects. The following sections provide our Welsh language impact assessment.

[928] As set out in section 75(1) of the Northern Ireland Act 1998, in carrying out our functions relating to Northern Ireland we are required to have due regard to the need to promote equality of opportunity between persons of different religious belief, political opinion, racial group, age, marital status or sexual orientation; men and women generally; persons with a disability and persons without; and persons with dependents and persons without. In addition, as set out in section75(2), without prejudice to the obligations under section 75(1), in carrying out our functions in relation to Northern Ireland we are required to have regard to the desirability of promoting good relations between persons of different religious belief, political opinion or racial group. For more information, see Ofcom, 2025. Revised Northern Ireland Equality Scheme for Ofcom.

[929] See Standards 84-89 of Hysbysiad cydymffurfio (in Welsh) and compliance notice (in English). Section 7 of the Welsh Language Commissioner's Good Practice Advice Document provides further advice and information on how bodies must comply with the Welsh Language Standards.

## Our provisional Welsh language assessment

A3.146 We noted that the 'foundational steps' outlined in the draft guidance reflected codes measures and information from our risk assessment guidance that we had already set for service providers elsewhere. We noted that these foundational steps have already undergone previous Welsh impact assessments, as part of previous consultations and statements on implementing those aspects of the regime, which concluded that our proposals are likely to have positive effects or increased positive effects on opportunities to use Welsh and treating Welsh no less favourably than English, with no known adverse effects.

A3.147 We noted that we had assessed the 'good practice steps' in the draft guidance. We noted that we recommended that providers should have regard to the needs of their user base in considering what languages are needed when developing their policies (in **Action 1**), user surveys (in **Action 2**), information about account access (in **Action 5**), and when designing their reporting processes (in **Action 8**). We stated that, to this extent, we considered that our proposals were likely to have positive effects or increased positive effects on opportunities to use Welsh and the treatment of Welsh no less favourably than English. We concluded that we did not consider that any adverse effects would be likely to arise as a result of our proposals.

## Stakeholder feedback

A3.148 Several stakeholders suggested that the Guidance should explicitly require safety features such as reporting tools and user support tools be available in Welsh.[930] We received similar feedback regarding content moderation systems and processes.[931] For example, the University of Portsmouth suggested that the Guidance explicitly require safety features such as reporting tools, content moderation systems and user support be available in Welsh, and that providers develop Welsh-language moderation capacity either in house or through partnerships. It also proposed that platforms include Welsh-language users in their risk assessments and publicly report on how effectively they serve those users, aligning the Guidance with the Welsh Language (Wales) Measure 2011 and promoting linguistic equality online.[932] In addition, the Minderoo Centre for Technology and Democracy at the University of Cambridge noted that "content moderation in non-English languages, including Welsh, received less attention across the board" and that considerations about content moderation across language boundaries are absent from the Guidance.[933]

A3.149 One stakeholder noted that "service providers should be at liberty to choose the languages in which they wish to provide their service, and if they feel unable to appropriately monitor and review user content in other languages, reject that user content."[934]

A3.150 The four Welsh Office of Police and Crime Commissioners[935] said that the Guidance should be available in Welsh.

---

[930] Response(s) to our February 2025 consultation: Equality Now p.1-2; Harrison, J., p.16; [✂]; NSPCC, p.28,
[931] Responses to our February 2024 consultation: Harrison. J. p.16, The Minderoo Centre for Technology and Democracy at the University of Cambridge p6-7.
[932] Response(s) to our February 2025 consultation: University of Portsmouth, p.13.
[933] Response(s) to our February 2025 consultation: The Minderoo Centre for Technology and Democracy at the University of Cambridge p6-7.
[934] Response(s) to our February 2025 consultation: Name Withheld 1, p. 2-3.
[935] Response(s) to our February 2025 consultation: The four Welsh Office of Police and Crime Commissioners, p.9.

A3.151 Several stakeholders asked if we had undertaken assessments about language accessibility for other commonly spoken minority languages in the UK, with several stakeholders specifically mentioning Gaelic.[936]

## Our response

A3.152 In response to feedback that the Guidance should explicitly require safety features as well as content moderation systems and processes be available in Welsh, we have stated that services should have regard to the needs of their UK user base in considering what languages are needed to ensure safety information is accessible to their user base,[937] which may include Welsh.

A3.153 In response to the comments related to Welsh language moderation capacity, we consider that providers must already be able to appropriately monitor and review content on their services as part of their duties under the Act, regardless of the language of the content. We have added a consideration under **Action 6** / **Case study 14** (Automated detection of misogynoir content and results) that providers should have regard to the needs of their UK user base in considering what languages are needed to ensure that its automated systems are accurate at detecting harmful content in multiple languages.

A3.154 In response to the feedback on risk assessments, we are unable to amend foundational steps through the Guidance as the foundational steps reflect measures in the Codes and risk assessment guidance which we have already consulted on, finalised and published through separate processes.

A3.155 We have published a Welsh version of the Guidance alongside the English version.

A3.156 In response to the feedback about the scope of the Welsh Language assessment and other UK languages, we note that we already consider the different interests of persons in the different parts of the UK, including languages spoken across the UK, as part of the equality impact assessment.

## Our overall conclusion on Welsh language impacts

A3.157 We are confirming our provisional assessment and we set out further considerations below. We have reviewed stakeholder feedback in our provisional assessment and have carefully assessed the Guidance. We have recommended that providers should have regard to the needs of their user base in considering what languages are needed when developing their policies (see **Action 1**), developing their user surveys (see **Action 2**), ensuring that published information and findings are accessible (see **Action 3**), providing information about account access (see **Action 5**), applying automated content moderation tools (see **Action 6**) and when designing their reporting processes, their off service-incident reporting processes and when providing supportive information (see **Action 8**). With this considered we are confirming our provisional view that our proposals are likely to have positive effects or increased positive effects on opportunities to use Welsh and treating Welsh no less favourably than English.

A3.158 As noted in our provisional impact assessment, the 'foundational steps' outlined in the Guidance reflect codes measures and information from our risk assessment guidance that we had already set for service providers elsewhere. These foundational steps have already

[936] Response(s) to our February 2025 consultation: Institute for Strategic Dialogue (ISD), p.15; Name Withheld 3, p.3-4; Women's Aid Federation of England p.18, Ofcom Advisory Committee for Scotland, p.6.
[937] See Actions 1, 5, 6 and 8 of the Guidance.

undergone previous Welsh impact assessments that have been through the process of public consultation and a final assessment has been published responding to stakeholder feedback. These final assessments concluded that the foundational steps are likely to have positive effects or increased positive effects on opportunities to use Welsh and treating Welsh no less favourably than English, not highlighting any known adverse effects.