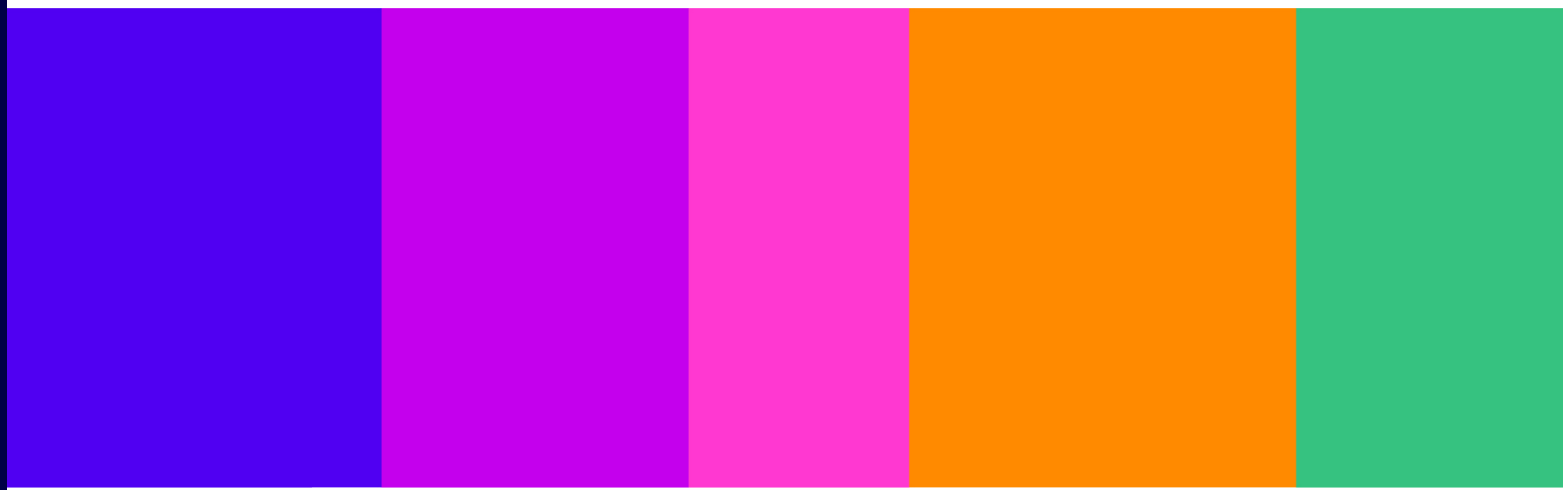
Consultation Document

A safer life online for women and girls: practical guidance for tech companies

Consultation

Published 25 February 2025
Closing date for responses: 23 May 2025

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



Contents

Section

Annex

Foreword

Life online allows us to stay connected, learn new skills and build positive communities. But for women and girls, too often, our online world can be a hostile and dangerous place. Online spaces can facilitate online domestic abuse, silence women who wish to express themselves, and create communities where misogynistic views thrive.

Tech companies play a crucial role in how harms to women and girls proliferate online. The decisions they make have the power and opportunity to create a safer life online for women and girls. While some sites and apps have taken some steps to protect women and girls, the fact is many have not.

In 2023, the UK Parliament passed the Online Safety Act (the 'Act'). For the first time, online services, including social media, gaming services, dating apps, discussion forums and search services have new responsibilities to protect people in the UK from illegal content and content harmful to children, including harms that disproportionately affect women and girls.

- The Act requires tech firms to assess the risk of illegal harms occurring on their service, including controlling or coercive behaviour, stalking and harassment, and intimate image abuse. They have a duty to protect all users from this material, taking down illegal material once they become aware of it.
- The Act also requires tech firms to assess the risk of harm to children from harmful content, including abusive and hateful content, violent content and pornography. They have a duty to take appropriate action to protect children from this kind of content.

To help services meet these duties, Ofcom has already published final Codes and guidance on how we expect tech firms to tackle illegal content, and we'll shortly publish our final Codes and guidance on the protection of children. Once these duties come into force, Ofcom's role will be to hold tech companies to account, using the full force of our enforcement powers where necessary.

But beyond enforcing these core legal duties, the Act also requires Ofcom to produce additional, dedicated industry guidance setting out how providers can take action against harmful content and activity that disproportionately affects women and girls, in recognition of the unique risks they face.

Building on foundational protections

Women and girls will benefit from these foundational protections but tackling the broader risks they face requires a holistic approach looking beyond illegal content. This draft Guidance sets out ambitious and practical ways to tackle problems which facilitate online domestic abuse, silence women who wish to express themselves, create communities where misogynistic views thrive, and sometimes affect women's ability to do their jobs.

More needs to be done to meet the specific needs of vulnerable victims and survivors of domestic abuse, beyond the removal of illegal content. The pile-on culture that is so prominent on social media can amount to harassment and prevent women from exercising their ability to express themselves freely online or, sometimes, even from doing their jobs. Misogynistic speech is often not illegal, but, at scale, it can normalise harmful beliefs in boys and men, and impact women and girls' experiences both online and offline. Image-based abuse has increased exponentially as a result of image generating AI tools, with one helpline reporting more than a 100% increase in reports in 2023 from the previous year.

Our draft Guidance identifies a total of **nine areas** where technology firms should do more to improve women and girls' online safety by taking responsibility, designing their services to prevent harm and supporting their users.

It promotes a safety-by-design approach, demonstrating how providers can embed the concerns of women and girls throughout the operation and design of their services, as well as their features and functionalities. This approach envisages tech firms taking greater responsibility at all levels for women and girls' online safety, taking steps to prevent harm through safer design and having effective mechanisms to support women and girls and respond when harm does occur. Under each of the nine actions, we highlight the foundational steps we have already set out through our work on illegal harms, protection of children and transparency reporting. In addition, we draw on practical, real examples to show how tech companies can go further if they are serious about addressing the range of harms women and girls face online. Within this draft Guidance, the nine proposed actions are:

Taking responsibility

1. Ensure that governance and accountability processes address online gender- based harm, for example by consulting subject matter experts and setting policies that prohibit these harms.
2. Conduct risk assessments that focus on harms to women and girls, for example by engaging with survivors and victims and conducting user surveys.
3. Be transparent about women and girls' online safety, for example through sharing information about the prevalence of harms on a service and the effectiveness of safety measures.

Preventing harm

4. Conduct abusability evaluations and product testing, for example by using red teaming to identify ways malicious actors may try to use service features to perpetrate harm.
5. Set safer defaults, for example by 'bundling' default settings together to make it easier for women experiencing pile-ons to secure their accounts.
6. Reduce the circulation of online gender-based harm, for example by using hash matching to detect and remove intimate images shared without consent.

Supporting women and girls

7. Give users better control over their experiences, for example by providing the option to block multiple accounts at once.
8. Enable users who experience online gender-based harm to make reports, for example by building reporting systems designed in a way that is supportive and accessible for those experiencing domestic abuse.
9. Take appropriate action when online gender-based harm occurs, for example by taking action against users who repeatedly violate the service's policies.

Taken together, these actions combine the legal responsibilities tech firms now have to protect their users with innovative good practices and deliver a new and ambitious vision for women and girls' online safety.

Tackling online gender-based harms is a complex task

This draft Guidance balances difficult challenges. First, these harms cover both illegal and legal content. While illegal content needs to be taken down, we also need to protect the ability of users to

express themselves freely online. Crucially, this includes the need to secure the ability of women and girls to speak out and have their voices heard, without being silenced by abuse.

Second, online anonymity can make it easier for perpetrators to post hateful and threatening content, but it can also ensure that some users – including those at risk of domestic abuse and stalking – maintain their privacy and stay safe online.

Third, online apps and sites are different, and people's experiences on these services vary substantially. Our research shows that factors like, gender, age, race, and ethnicity, and socio-economic status can influence someone's experience online. This includes how often they go online, what platforms they use, and the harms they may experience. While a feature or functionality of a service may be positive for many users, it may also increase the distinct and disproportionate risks faced by women and girls. Tech companies need to invest in understanding how their platforms affect the experiences of women and girls and take the actions that will have the most impact. That's why they need to be a part of this conversation.

Finally, these harms – and the online spaces that enable them – change rapidly. Perpetrators are quick to exploit new tools and find new ways to uphold and enable longstanding forms of misogyny, sexism and gender-based violence. Our vision for women and girls' online safety is dynamic and responsive to both well-established and novel patterns of harm.

In developing this draft Guidance, we've spoken to survivors and victims, as well as frontline organisations, to hear directly from those impacted and listen to what changes they want to see. Their first-hand experience of these issues must be heard if we are to create meaningful change. We are working closely with specialists on women and girls' safety, and we have facilitated discussions between industry, civil society, researchers, law enforcement and other experts to discuss these challenges from a range of perspectives.

We've analysed research reports, design prototypes, and academic literature on how harms manifest and how to intervene. And we've also spoken to tech companies who have shared with us what they are already doing to create safer spaces for women and girls.

This draft Guidance is a call to action for those working within tech companies

They are in a unique position of power to shift a system that can allow misogyny, sexism, and gender-based violence to go unchecked in online spaces to one which fosters trust with the millions of women and girls in the UK.

Through this consultation, we are inviting tech companies, civil society, researchers and other stakeholders to help strengthen our proposals. We want to see more evidence about what could work, and hear about more examples of what can be done. We are asking tech companies to come to the table to speak with us alongside experts and survivors to explain how they are going to take action.

Following this consultation, we intend to publish the final Guidance by the end of this year. After that we will continue to work closely with regulated companies to find out what steps they are taking to protect women and girls. We will also continue to work with researchers and civil society organisations, and to learn from women and girls themselves about their experiences online. We will publish an assessment of what tech companies are doing – or not doing – to create a safer life online for women and girls around 18 months after finalising the Guidance, to shine a light on industry practice and help women and girls make informed choices about the services they use.

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 Improving women and girls' online safety is a strategic priority for Ofcom. As the online safety regulator, we will focus our efforts on ensuring providers make their services safe for women and girls online. This includes giving practical guidance on how services can be made safer, as well as supporting women and girls to make informed decisions about the services they use. We understand that securing women and girls' safety is a societal challenge;[1] however, we firmly believe there is more service providers can – and should – do.

1.3 The Act makes providers of regulated user-to-user and search services ('services')[2] – including social media, search, and adult services – legally responsible for keeping users safe online. This includes clear requirements on online services to address illegal harms such as intimate image abuse, and to protect children from harmful content, including pornographic and abusive content.

1.4 To help services meet these duties, Ofcom is required to publish various Codes of Practice and guidance documents. We have moved swiftly to begin implementing the Act, and are publishing these documents in phases. The duties also come into force at different times. We published the Illegal Content Codes and Risk Assessment Guidance in December 2024, setting out how services must approach their new duties relating to illegal harms. In January 2024, we published our statement on age assurance and children's access assessments. In April 2025, we will publish the Protection of Children Codes and Risk Assessment Guidance, looking at how services should approach their new duties relating to content that is harmful to children. We will also publish our Transparency Guidance in Spring 2025.[3] We are ready to take enforcement action if providers do not act promptly to comply with their duties.

1.5 In addition to these requirements, the Act also states that Ofcom must produce dedicated guidance on how providers can address content and activity that disproportionately affects women and girls.[4] This includes a wide range of illegal and legal harms that threaten, silence, abuse, monitor, coerce and otherwise harm women and girls online, curtailing their safety and ability to express themselves freely.

---

[1] We are aware of a significant number of global and domestic initiatives focusing on improving women and girls' safety online. This includes governmental initiatives, international partnerships and other programmes. For example, in the UK, see plans set out by the Northern Ireland, Welsh and Scottish Governments, as well as the UK Government's mission to 'halve violence against women and girls in the next decade.' [accessed 11 February 2025].

[2] 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'.

[3] For more information, see Ofcom's progress update implementing the Online Safety Act. [accessed 29 January 2025].

[4] Section 54 of the Act.

1.6 Our proposed guidance is the subject of this consultation and is available at Annex A (draft Guidance).

Legal context

1.7 Under section 54 of the Act, Ofcom is required to produce guidance for Part 3 service providers[5] which focuses on 'content and activity' that 'disproportionately affects women and girls'.

1.8 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. [6] It also says that the guidance may, among other things, (a) contain advice and examples of best practice for assessing risks of harm to women and girls from such content and activity; and (b) refer to provisions contained in Ofcom's Codes of Practice that relate to the duties of Part 3 service providers and which are particularly relevant to the protection of women and girls from this content.[7] In this way, the Act is permissive in terms of what we can include in the guidance - it does not restrict us to including guidance containing only (a) and (b).

1.9 Before producing the final Guidance, we are required to consult the Domestic Abuse Commissioner, the Commissioner for Victims and Witnesses and such other persons as we consider appropriate.[8] We are also required to consult on revised or replacement guidance.[9]

1.10 In Annex 1, we set out the relevant legal context and explain our general duties and the matters we are required to have regard to in carrying out our functions, our media literacy duties and Ofcom's duty to carry out our functions compatibly with the Human Rights Act 1998, including the right to freedom of expression and 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.

Approach to the Guidance

1.11 We consider the Guidance to be an opportunity to set out practical steps for providers. To do this, we set out a foundation of safety by bringing together relevant Codes measures and guidance from across Illegal Harms, Protection of Children and (only as applicable to a defined set of providers) transparency. We also go further, including additional examples of good practice that represent an ambitious vision for a safer life online for women and girls. In this draft Guidance, we take a safety-by-design approach, demonstrating how providers can embed the concerns of women and girls throughout the operation and design of their

[5] Section 4(3) of the Act provides that a 'Part 3 service' means a regulated user-to-user service or a regulated search service.
[6] 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.
[7] The relevant Codes of Practice for this purpose are those under Section 41 (see s.54(2)(b)) of the Act.
[8] Section 54(3) of the Act.
[9] Section 54(3) of the Act.

services, features and functionalities. Specifically, we ask providers to take action in nine areas:

Figure 1: Nine action areas in Chapter 3, Chapter 4, and Chapter 5 of the draft Guidance

1.12 By taking action in these areas, service providers can meaningfully create safer environments for women and girls. These services play an important role in how we all communicate, and providers have a responsibility to ensure users have fair and safe experiences. Designing services with the safety of women and girls in mind is critical for securing longer-term engagement and fostering trust with a significant portion of their customer base. Our Online Nation 2024 report suggests that women spent more time online than men across all adult age groups. We also expect that, for ad-funded services, demonstrating they are taking action can reassure advertisers that their advertising spend is being placed in a way that does not undermine brand value.

1.13 We also recognise the importance of an ongoing and accessible dialogue to build out this draft Guidance. In developing the draft Guidance, we ran two stakeholder workshops to support our interpretation of the available evidence and expand our evidence base further. Overall, over 40 organisations participated. This provided an opportunity to bring together

a breadth of specialist experts on online gender-based harms across the UK and beyond to ensure that we could consider these perspectives early in the process of developing the draft Guidance.

1.14 The first workshop, held on 16 September 2024, focused on 'Discovery', where we sought a wide range of views on what we should include and consider in the draft Guidance. This was attended by public bodies, civil society, academia, and law enforcement.[10] The second workshop, held on 19 November 2024, focused on 'Testing', where we asked for feedback and evidence to stress-test our direction of travel. This was attended by public bodies, civil society, academia, law enforcement, and services.[11]

1.15 During the consultation period, we hope to gain further insights about what providers are currently doing in this space, as well as expert views, so the final Guidance can set out an ambitious and actionable vision of a safer life online for women and girls. Once finalised, we have a range of tools we can use as the online safety regulator, including through information gathering, supervisory engagement and our own published reports, to encourage providers to take up the recommendations included in the final Guidance.

1.16 As part of this, we intend to publish an assessment which will spotlight how providers are addressing women and girls' safety 18 months after finalising the Guidance. This will include reviewing the uptake of the Guidance, and gathering feedback from women and girls in the UK about how their experiences have – or have not – changed. We would intend for this report to shine a light on which services are prioritising women and girls' safety, helping users to make informed choices about how they use online services.

1.17 We will also continue our ongoing engagement with civil society, academics, industry and other experts to gather evidence and strengthen our understanding of online gender-based harms.

Our proposed objectives for the Guidance

1.18 We want this Guidance to give service providers a detailed and holistic framework for understanding harms to women and girls online, and to set out an ambitious vision for women and girls' online safety. We propose three objectives for the Guidance.

1.19 First, we want the Guidance to be a resource which summarises the ways different types of content and activity affect women and girls online, drawing together our evidence base on specific areas set out in Illegal Harms, Protection of Children, as well as additional sources looking at the issue in the round. This approach is explained in detail in paragraphs 2.6-2.16.

---

[10] Organisations that attended the first workshop include: Centre for Protecting Women Online; Children's Commissioner; End Violence Against Women Coalition; Executive Office, Northern Ireland; HateAid; Nexus; Centre for Digital Citizens, Northumbria University; North West Regional Organised Crime Unit; NSPCC; Online Safety Act Network; Refuge; Suzy Lamplugh Trust; SWGfl; UCL Gender + Tech Research Lab; Victims' Commissioner; Welsh Women's Aid; Zero Tolerance.

[11] Organisations that attended the second workshop include: 5Rights; Beyond Equality; Microsoft; Bumble; CEASE; Centre for Protecting Women Online; Cranstoun; Digital Rights Foundation; End Violence Against Women Coalition; Everyone's Invited; Executive Office, Northern Ireland; Google/YouTube; Institute for Strategic Dialogue; Match; Meta; Nexus; Centre for Digital Citizens, Northumbria University; NSPCC; Online Safety Act Network; Reddit; Refuge; Southall Black Sisters; Suzy Lamplugh Trust; SWGfl; Twitch; UCL Gender + Tech Research Lab; University of Portsmouth; University of Warwick; Victim's Commissioner; White Ribbon NI; Women's Aid NI; Women's Aid Scotland; Women's Support Project.

1.20 Second, we intend for the Guidance to set out practical and achievable recommendations that providers can implement to improve women and girls' safety in ways that go beyond the measures we have already set out in Codes and risk assessment guidance. We intend to use this consultation process to continue facilitating conversations between ourselves, service providers, civil society organisations, researchers, survivors and victims, safety tech organisations, public sector bodies, and other experts about the proposals we have set out and how to take these further. We hope to gather additional insights and highlight emerging issues. This approach is described in detail in paragraphs 2.17-2.82.

1.21 Third, we see the Guidance as an opportunity to demonstrate to industry the pressing need to improve women and girls' online safety, and to provide them with the support and encouragement needed to take action. As explained in paragraphs 2.83-2.89, we want to leverage our role as the online safety regulator to highlight specific providers that are taking meaningful and bold action – and, in turn, spotlight those providers that are not.

1.22 This consultation document explains how we have developed the draft Guidance in line with these proposed objectives.

Who does the Guidance apply to?

1.23 Part 3 of the Act places duties on providers of regulated user-to-user services and providers of regulated search services to identify, mitigate and manage the risks of harm from illegal content and activity, as well as content and activity harmful to children. These services include a wide range of platforms including social media, gaming, discussion forums, pornography services,[12] dating services and online marketplaces. The ways that harms targeting women and girls manifest on these services can vary and the kinds of interventions available to address those harms evolve rapidly.

1.24 While we expect many of the proposals in the draft Guidance to be relevant for all services, our focus – both in terms of developing our proposals and our future engagement – will be on those services with the highest reach or highest risk for online gender-based harms.

1.25 We recognise that online gender-based harms do not happen in isolation on such 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,[13] as well as Bluetooth,[14] which is commonly used for cyberflashing.[15] Where relevant, we make reference in the draft Guidance to how these technologies are being used to facilitate or amplify online harm. We also expect that some

[12] 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. [accessed 11 February 2025].

[13] 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 3 January 2025]; eSafety Commissioner, 2024. Technology, gendered violence and Safety by Design. [accessed 3 January 2025].

[14] 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.

[15] Law Commission, 2021. Modernising Communications Offences: A final report. [accessed 11 February 2025].

of the information we provide in the draft Guidance may assist providers of these technologies to improve safety.

What this document covers

1.26 We are issuing this public consultation on the draft Guidance and invite comments from all interested parties, including the two named statutory consultees, the Domestic Abuse Commissioner and the Commissioner for Victims and Witnesses, as well as civil society organisations, regulated service providers and other industry participants.

1.27 This consultation document provides the necessary background and context that stakeholders should be aware of when reading the draft Guidance and responding to the consultation. It covers:

- Background, including the provisions of the Act which are relevant to this Guidance;
- Our proposed approach to the draft Guidance, including the scope, structure, content and how we propose to monitor and update the draft Guidance;
- The relevant legal framework, including Ofcom's wider duties;
- Our assessments of the impact of our draft Guidance (including our impact assessment under Section 7 of the Communications Act 2003, equalities impact assessment and Welsh language impact assessment); and
- How to respond to this consultation.

Next steps

1.28 We are inviting stakeholders' views on our draft Guidance. The deadline for responses is 23 May 2025.

1.29 Once we have considered all responses, we will publish a statement explaining our final decisions on the Guidance, alongside the final Guidance itself. We expect this to be by the end of 2025.

2. Proposed approach

Warning: this chapter contains content that may be upsetting or distressing.

2.1 This section explains the objectives we hope the draft Guidance will help to secure:

a) giving providers a detailed and holistic framework for understanding harms to women and girls online;
b) setting out practical and ambitious steps providers can take to secure women and girls' online safety; and
c) encouraging service providers to take action to achieve a safer life online for women and girls.

2.2 This section also explains how we have sought to take these objectives into account in developing the draft Guidance.

Understanding harms to women and girls online

2.3 Our first objective for the draft Guidance is to help ensure providers understand the risks and harms that women and girls currently face on online services.

2.4 The Act specifies that the draft Guidance should focus on "content and activity" which "disproportionately affects women and girls."[16] This could be very broad. There is evidence that many online harms have some disproportionate or distinctive effect on women and girls. Our Online Nation 2024 report found that women and girls interact with services differently than men and boys, including how much time they spend online, which services they use, the harms they encounter, and the impacts those harms have.[17]

2.5 We considered it important to narrow the focus of the draft Guidance to areas where women and girls experience a disproportionate and distinct harm, as well as areas where the primary impact of the content or activity is to reinforce, enact or enable misogyny, sexism or other forms of gender-based violence or abuse.[18]

Identifying harms to focus on

2.6 To identify which harms would best satisfy our objectives, we reviewed existing evidence including our Illegal Harms Register of Risks, and our draft Children's Register of Risks. We also considered additional evidence available that looks at women and girls' online safety in the round, including conducting an in-depth literature review and assessing responses to our consultations on Illegal Harms and Protection of Children.

[16] And in relation to which user-to-user and search services have duties under Part 3 and Part 4 of the Act.
[17] There are also differences between groups of women and girls due to their protected characteristics, for example increased risks of harm for women and girls from an ethnic minority background. This is further discussed in paragraph 2.13.
[18] Sexism and misogyny are closely linked to describe the hatred of women. We use the dictionary definitions, where misogyny refers to the feelings of, or beliefs in, the hatred of women, and sexism refers to discriminatory actions or behaviours taken on behalf of such beliefs or feelings. [accessed 11 February 2025].

2.7 We also tested our thinking with stakeholders from civil society, experts and industry, and integrated their feedback into the development of our focus areas.[19]

2.8 Based on this process, we propose that the draft Guidance should focus on four harms:

- **Online misogyny** includes the circulation of content that actively encourages or reinforces misogynistic ideas or behaviours, including content that incites hatred, abuse or threats toward women and girls. It also includes sexual or explicit content that normalises or encourages harmful sexual behaviour.[20] This harm spans across illegal content such as illegal threats and extreme pornography, as well as content which is legal but harmful to children, such as content normalising gendered or sexual violence.
- **Pile-ons and online harassment** describes cases where groups of coordinated individuals target a specific woman or girl, or groups of women and girls. It usually includes misogynistic content, as well as threats, image-based sexual abuse (explained in the following paragraph) and other forms of harassing content. While pile-ons can happen to any user, they often target women in public life, such as journalists, politicians, and celebrities. They can also include gendered disinformation, which can be used in coordinated harassment campaigns against women and girls in public life.[21] This harm spans across illegal content (harassment, image-based sexual abuse), as well as legal content which is harmful to children (misogynistic abuse).
- **Online domestic abuse** describes using technology for coercive and controlling behaviour (CCB) in the context of an intimate relationship. It can include monitoring or takeover of online accounts, harassment, or demeaning languages in messages, as well as using location information for stalking.[22] Where these actions amount to a pattern of coercive control or harassment, they are illegal content.
- **Image-based sexual abuse** refers to intimate image abuse (the non-consensual sharing of intimate images) and cyberflashing (sending explicit images to someone without their consent). Perpetrators can leverage these harms in different ways, depending on the context,[23] but at its core image-based sexual abuse represents a breach of privacy and bodily autonomy of those targeted.[24] This is illegal content.[25]

---

[19] Ofcom Stakeholder Workshop 1 on Women and Girls' Online Safety, 16 September 2024.

[20] Regehr, K., Shaughnessy, C., Zhao, M. and Shaughnessy, N., 2024. Safer Scrolling: How algorithms popularise and gamify online hate and misogyny for young people. [accessed 12 February 2025]; Women's Aid, 2023. Influencers and Attitudes: How will the next generation understand domestic abuse?. [accessed 24 October 2024].

[21] Demos (Judson, E.), 2021, Silence, Woman: An investigation into gendered attacks online. [accessed 11 February 2025]; Demos (Judson, E., Atay, A., Krasodomski-Jones, A., Lasko-Skinner, R. and Smith, J.), 2020. Engendering Hate: The Contours of State-Aligned Gendered Disinformation Online. [accessed 25 October 2024].

[22] Refuge, 2021. Unsocial Spaces. [accessed 11 February 2025]. Many of these controlling behaviours, such as stalking and harassment, can also occur outside of an intimate relationship.

[23] See for example, Moore, A., 2022. 'I have moments of shame I can't control': the lives ruined by explicit 'collector culture', The Guardian, 6 January. [accessed 28 October 2024]; Ofcom, 2024. Deepfake Defences: Mitigating the Harms of Deceptive Deepfakes. [accessed 28 October 2024]; Refuge, 2020. The Naked Threat. [accessed 28 October 2024].

[24] McGlynn, C., Johnson, K., Rackley, E., Henry, N., Gavey, N., Flynn, A. and Powell, A., 2021. 'It's Torture for the Soul': The Harms of Image-Based Sexual Abuse', *Social and Legal Studies, 30 (4).* [accessed 22 December 2024].

[25] The current intimate image abuse offences set out under the Act cover the sharing, or threatening to share, of intimate images without consent. At the time of writing, the Data (Use and Access) Bill is under consideration in Parliament, and amendments have been introduced relating to offences for creating 'purported sexual images' (for example, creating sexual deepfakes) of an adult. The UK Government has also

2.9 In line with our objective to help providers understand the nature of these harms, we set out a detailed view of these harms in Chapter 2 of the draft Guidance.

Interpreting these harm areas

2.10 Sometimes in the draft Guidance, and throughout this document, we use the term **online gender-based harms** to refer to this kind of content and activity in the round. We use 'harm' in line with our wider work on online safety, and to reflect the wide spectrum of content and activity we focus on (which have severe and enduring impacts, including forms of violence and abuse).

2.11 We note that many experts use the term 'violence' to describe a wide range of harms (including the term 'Violence Against Women and Girls', often shortened to 'VAWG').[26] Where we have drawn on or quoted external sources of evidence that use the term 'violence' in this way, we have not changed or explained it, given its widespread use.

2.12 We use 'gender-based' to reflect the holistic and preventative approach we want providers to take in understanding how these harms manifest and influence wider gender dynamics. The majority of individuals perpetrating harassment, domestic abuse and other forms of online or tech-enabled violence against women and girls are men.[27] Notably, online misogyny often circulates amongst – and is promoted to – boys and men.[28] As discussed in Chapter 2 of the draft Guidance, this can normalise sexual aggression towards women and girls, misogynistic behaviours, and attitudes around consent.[29] In this way, these types of harmful content and activity can uphold or encourage harmful gender-based norms, including impacts on men and boys. Part of the solution therefore includes focusing on these wider dynamics to prevent and respond to harms.

2.13 All four kinds of online gender-based harms are both systemic and intersectional. They are driven by longstanding forms of misogyny, sexism and gender-based violence which also intersect with other factors including age, race, ethnicity, socio-economic status, sexual orientation, gender identity, disability and religion.[30] We also recognise these areas can co-

---

announced its intention to create new offences for the taking of intimate images without consent and the installation of equipment with intent to commit these offences via its forthcoming Crime and Policing Bill. We are monitoring these developments.

[26] See for example research that sets out these harms on a "continuum of violence against women" with the normalisation of misogyny and entitlement (such as in sexist 'jokes') and social sanctioned aggressive behaviour on one end, and severe cases of assault and homicide on the other. Source: Kelly, L., 1988. Surviving Sexual Violence. [accessed 23 October 2024}.

[27] National Police Chiefs' Council, 2024. VAWG Strategic Threat and Risk Assessment. [accessed 6 February 2025].

[28] Internet Matters, 2023. "It's really easy to go down that path": Young people's experiences of online misogyny and image-based abuse. [accessed 6 January 2025]; Griffin, J., 2021. Incels: Inside a dark world of online hate, BBC News, 13 August. [accessed 11 February 2025]

[29] Regehr, K., Shaughnessy, C., Zhao, M. and Shaughnessy, N., 2024. Safer Scrolling: how algorithms popularise and gamify online hate and misogyny for young people. [accessed 11 February 2025]; Women's Aid, 2023. Influencers and Attitudes: How will the next generation understand domestic abuse?. [accessed 24 October 2024].

[30] 'Intersectional' was originally used by Dr. Crenshaw to describe the distinct experiences of Black women that occurred at the intersection of both racism and sexism. It is now more widely used to describe the ways forms of discrimination overlap creating specific and increased risks and harms. Source: Crenshaw, K., 1989. Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics, *University of Chicago Legal Forum*, 1989(1). [accessed 24 October 2024]; The Global Partnership, 2023. Technology-Facilitated Gender-Based Violence: Preliminary Landscape Analysis. [accessed 12 February 2025].

occur and overlap, both online and offline, and connect to harmful dynamics such as victim-blaming.[31]

Other considerations

2.14 There are other types of harmful content that disproportionately impact women and girls' safety online but do not necessarily fall fully within the previously mentioned categories, such as child sexual exploitation and abuse,[32] modern slavery and human trafficking, sexual exploitation of adults, and eating disorder content. These harms are addressed in our Illegal Content statement, and proposals on Protection of Children.

2.15 While we do not cover these issues in depth in the draft Guidance, where possible we address them as they overlap with the focus areas set out previously. For example, we note the overlap between tactics used by perpetrators of human trafficking and domestic abuse, [33] and we also highlight how Codes measures designed to tackle child sexual abuse material (CSAM) are related to techniques that can be used to prevent intimate image abuse and cyberflashing.

2.16 As part of this consultation, we would welcome feedback from stakeholders on our proposed focus areas.

Question 1: Do you have any comments on our proposed approach to 'content and activity' which 'disproportionately affects women and girls'?

Setting out what service providers can do to improve women and girls' safety

2.17 Our second objective for the draft Guidance is setting out practical and achievable recommendations providers can implement to improve women and girls' safety. This section describes our approach to meeting this objective. First, we explain how we propose to structure the information. Second, we explain our rationale, and finally, we set out the evidence base we have drawn on.

[31] Vera-Gray, F. and Kelly, L., 2020. Contested gendered space: public sexual harassment and women's safety work, *International Journal of Comparative and Applied Criminal Justice*, 44 (4). [accessed 25 October 2024]; The Global Partnership, 2023. Technology-facilitated gender-based violence: Preliminary Landscape Analysis. [accessed 18 January 2025].

[32] We recognise that some forms of child sexual exploitation and abuse (CSEA) disproportionately impact girls. For instance, as we set out in the Illegal Harms Register of Risks, girls are at greater risk of experiencing grooming and being depicted in child sexual abuse material. We do not propose to focus in depth on CSEA in the draft Guidance as there are separate areas of the Act that deal specifically with CSEA, including the CSEA reporting duties. We also highlight CSEA measures set out in the Illegal Content Codes as they apply to girls. We recognise that some of the ways that CSEA manifests online, such as self-generated intimate images and harmful sexual behaviour, have overlaps with online gender-based harms and draw these out where appropriate.

[33] Office of Family Violence Prevention and Services (Dabby, C.), 2019. Domestic Violence and Human Trafficking: Advocacy at the Intersections. [accessed 5 February 2025].

Structure

2.18 We propose to bring together our existing Codes and guidance for providers under illegal harms, protection of children and (only as applicable to a smaller number of providers) transparency. We also set out additional steps providers can take to go further.

2.19 In line with this, our proposed structure sets out **9 high-level actions** to improve the safety of women and girls online. Under each action, we include **foundational steps** and **good practice steps** for providers to take**.** These are explained in **Table 1.**

	Foundational steps	Good practice steps
Summary	Includes final and draft Codes measures[34] and information from our risk assessment guidance[35] relevant to each action. We also briefly refer to the Transparency Reporting duties under the Act. [36]	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 or draft 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 – either in final or draft form – to help providers comply with the corresponding duties in the Act as set out in the Legal Annex (Annex A1).	We consider that taking these steps may assist providers to demonstrate their approach to user safety more broadly.[37] It is possible that certain good practice steps may ultimately become codes measures. [38]

[34] Our Illegal Content Codes of Practice and draft Protection of Children Codes of Practice describe measures recommended for the purpose of compliance with 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. Again, the Children's Codes have not yet been set out in final form.

[35] 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. The Children's Risk Assessment Guidance has not yet been set out in final form.

[36] See section 77 of the Act. Duties around transparency reporting only apply to categorised services. Ofcom's draft 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 A1) 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.

[37] 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.

[38] 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

	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.[39]	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 draft Guidance

2.20 We do not expect all service providers to need to – or be able to – implement all of the foundational steps or good practice steps we have set out under each action. We recognise that some of these may only be relevant or applicable to certain services, for example because of their size, risk level or functionalities. Service providers can use their discretion to determine which solutions will be most relevant to meet their illegal harm and protection of children duties and be most impactful for their users. However, we strongly encourage providers to implement relevant good practice steps in addition to taking the action required to meet their enforceable duties.

2.21 For some of the foundational and good practice steps, we also include **case studies**. These are intended to be illustrative only, serving as practical demonstrations of how providers *could* take action. We selected the case studies based on where we assessed it would be most impactful and useful to set out additional information. For example, they draw out a complex or sensitive application to women and girls' safety. The case studies are not meant to be instructions or directives for in-scope services. Ultimately, it is up to service providers to determine how they can achieve the action set out.

2.22 We are looking for feedback from stakeholders on the nine high-level actions, as well as the good practice steps and associated case studies, the rationale for which is explained in the following section. We are not consulting on any of our foundational steps or the associated case studies as these cover Codes and risk assessment guidance which we have already consulted on through separate processes.[40]

---

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 draft 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.

[39] We also indicate where the foundational step appears in other Ofcom documents, such as our Illegal Content Codes of Practice and our Draft Protection of Children Codes of Practice. Where we refer in the 'Guidance at a Glance' document to a Code measure being at consultation or in draft, we recognise that they may be subject to change following the publication of this document and inclusion in this table does not -pre-judge Ofcom's final decision. Where we refer in that document to measures being 'final', that means that these measures are included in Ofcom's draft Illegal Content Codes of Practice as laid before Parliament on 16 December 2024. We expect to issue these and for them to come into force on 17 March 2025, unless either House of Parliament resolves not to approve them.

[40] We published our Illegal Harms consultation in November 2023 (and have since published our final statement in December 2024), our Protection of Children consultation in May 2024 (we expect to publish our statement in April 2025), and our Transparency Reporting consultation in July 2024 (we expect to publish our statement in early 2025).

Approach

2.23 To develop the actions and identify the relevant foundational and good practice steps, we have drawn on a **safety-by-design** approach. We heard from a number of stakeholders in their responses to previous consultations on online safety matters,[41] as well as from workshop participants, that this framework can be useful for embedding women and girls' safety into the design and operation of a service.

2.24 We are aware there are different models and interpretations of safety-by-design.[42] For the purposes of this draft Guidance, by safety-by-design we mean a proactive approach to integrating safety considerations into the design cycle of products, systems, or processes. This includes making iterative improvements to existing systems on longstanding services or features. It also can include retirement (replacing or removing a feature or functionality altogether), as well as ensuring new services or features can be designed with safety in mind from the outset.

2.25 Using this approach, we analysed points of intervention across three stages for how a service is run: governance and accountability, testing and service design, and operations and maintenance.[43]

2.26 For each stage, we looked at a broad range of evidence to assess what providers could do to meaningfully improve women and girls' safety.[44] We also considered the need for these actions to be broad enough to be achievable for all services in scope. We also aimed to ensure the actions demonstrated a vision of safety where providers take responsibility for ensuring a foundation of safety for women and girls. In this way, user controls and user tools can be used to create an added layer of personalised support.[45]

2.27 Based on this approach, we identified the **nine high-level actions**. These are split into **three chapters,** each representing one of the stages of how a service is run (**Table 2**).

	Description	Action
Chapter 3: Taking responsibility	How providers can make decisions and conduct assessments that account for women and girls' experiences.	**Action 1:** Ensure accountability processes address online women and girls' online safety
		Action 2: Conduct risk assessments that capture harms to women and girls
		Action 3: Be transparent about women and girls' online safety

[41] For example, we received a number of responses on this theme as part of our November 2023 Illegal Harms consultation: NSPCC response to the November 2023 Illegal Harms Consultation, p.14; OSAN response to the November 2023 Illegal Harms Consultation, p.1; EVAW response to the November 2023 Illegal Harms Consultation, p.3; CARE response to the November 2023 Illegal Harms Consultation, p.9; Domestic Abuse Commissioner response to the November 2023 Illegal Harms Consultation, p.2; Victims Commissioner response to the November 2023 Illegal Harms Consultation, p.2.

[42] See for example, Science Direct, Development Lifecycle - an overview. [accessed 20 December 2024].

[43] This model is an adapted version of a 'secure systems design lifecycle'. Source: Strohmayer, A., Slupska, J., Bellini, R., Neff, G., Coventry, L., Hairson, A. and Dodge, A., 2021. Trust and Abusability Toolkit: Centering Safety in Human-Data Interactions. [accessed 30 October 2024].

[44] This included reviewing current industry practice, engaging with stakeholders including service providers, civil society and other experts in online gender-based harms, reviewing academic literature, and considering responses received to our previous Online Safety consultations. Further detail is included in paragrphs 2.33-2.45.

[45] 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 22 October 2024].

	Description	Action
Chapter 4: Preventing harm	How providers can prevent harm through the design of their services.	**Action 4:** Conduct abusability evaluations and product testing
		Action 5: Set safer defaults
		Action 6: Reduce the circulation of online gender-based harms
Chapter 5: Supporting women and girls	What providers can do to support women and girls when harms happen on services.	**Action 7:** Give users better control over their experiences
		Action 8: Enable users who experience online gender-based harm to make reports
		Action 9: Take appropriate action when online gender-based harm occurs

Table *2*: Chapter structure of the draft Guidance

2.28 We considered alternative actions, such as setting out more prescriptive or specific actions. However, we considered that this approach would not cover the broad range of services in scope of the Guidance. For example, a specific action such as 'preventing upload of intimate image abuse' would not apply to search services, as they provide access to content on other services, rather than acting as a platform allowing users to upload it.

2.29 We also considered alternative structures for grouping the actions, such as splitting chapters by harm areas (for example, one chapter each on online misogyny, pile-ons, domestic abuse and image-based sexual abuse), or splitting chapters in line with the existing Codes of Practice structure (for example, one chapter each on Terms of Service, Enhanced User Controls, Reporting and Complaints, and so on). However, we determined that these structures introduced duplication (across chapters, as well as with our draft Illegal Harms Statement and consultation on Protection of Children) and additional complexity.

2.30 We therefore determined that setting higher-level 'safety-by-design' actions across various stages of service design and operation best meets our stated objective. In the round, we consider that the nine actions represent an achievable vision of safety for women and girls online.

2.31 This approach is also in line with the draft Statement of Strategic Priorities for Online Safety set out by the Government, which emphasises the importance of safety-by-design in tackling violence against women and girls. We have also had regard to the Department for Science, Innovation & Technology's 2025 report looking at the impact of platform design on online violence against women and girls.

Supporting evidence

2.32 The following section explains how we gathered and analysed the evidence for the draft Guidance and how this evidence supports the information we include under each action.

Establishing our evidence base

2.33 This section outlines our methodology for identifying foundational and good practice steps, including limitations and additional considerations.

Foundational steps and associated case studies

2.34 For the foundational steps, we conducted a review of our Statement on Illegal Harms and consultations on Protection of Children and Transparency. We analysed which aspects of our existing work would be most relevant to online gender-based harms. We then used relevant evidence to draw out illustrative 'case studies' associated with some of the foundational steps. We do not detail evidence in support of these foundational steps in this document as this is set out in our Illegal Harms Statement, and consultations on Protection of Children and Transparency guidance.

2.35 While we have not yet set out our final position on our Codes of Practice and risk assessment guidance on Protection of Children, for the purposes of this draft Guidance on online gender-based harms, we have indicated how we think our proposed measures outlined in our Protection of Children Consultation would be relevant to achieving the aims set out in the draft Guidance. However, any such references are made on a provisional basis and are subject to revision once Ofcom has finalised its position on these in our statement in April 2025.

Good practice steps and associated case studies

2.36 To identify the good practice steps, we reviewed safety measures currently deployed by industry and conducted a systematic literature review of academic, civil society, government, and other relevant research on online gender-based harms. This process primarily focused on UK-based research, but we also looked at international contexts to strengthen our understanding of how online gender-based harms manifest and global initiatives to address them, including from the eSafety Commissioner, the United Nations, and the Global Partnership (the latter of which Ofcom is a member).[46] We also considered stakeholder feedback on potential safety measures from past consultations (including on Illegal Harms and Protection of Children), as well as what we know of current industry practice by engaging with service providers who have published statements outlining their work on this issue. We also met with a group of survivors of domestic abuse to hear directly about what changes they want to see.[47]

2.37 In addition, we considered relevant aspect of our Media Literacy work.[48] Specifically, we drew on insights from our Best Practice Design Principles for Media Literacy.

2.38 We also held a stakeholder workshop in September 2024 to further gain evidence and insights about the kinds of harms women and girls experience online, and further examples about how the design and operation of services could be changed to reduce those risks. Participants included over 19 organisations from across civil society, academia, law enforcement and other experts from across the UK.

---

[46] See for example Australia's eSafety Commissioner's recent report on Technology, gendered violence and Safety by Design, the ongoing work of the Global Partnership for Action on Gender-Based Online Harassment and Abuse, and initiatives from the United Nations Global Population Fund. We engage regularly with international partners on this issue (including through our membership in the Global Partnership and the Global Online Safety Regulators Forum).

[47] Ofcom / Refuge meeting, 20 November 2024.

[48] Ofcom has statutory duties in relation to media literacy - some of which have been introduced by the Act as set out in the Legal Annex (Annex A1) and are particularly relevant to women and girls' online safety. Whilst there are close links between the policy areas of media literacy and online safety, they are distinct. Our media literacy work is broader in scope than online safety, in terms of both the content and services to which it applies, including through work looking at what service providers can do to support people to use, understand and create online media and communications in a variety of contexts.

2.39 Once we had compiled a list of examples of potential good practice steps, we evaluated each according to a set of criteria: alignment with existing policy positions (published in final or draft form), new risks/burdens for users (including to privacy or self-expression and any equality impacts), and applicability to one or more categories of online gender-based harm set out previously. We also considered the need to capture steps that spanned across the different stages of the design and operation of a service in line with the safety-by-design approach explained in paragraph 2.23.

2.40 We tested some of our analysis at a second stakeholder workshop in November 2024 with a wider group of stakeholders. 35 organisations attended this workshop including 7 services, as well as public bodies, civil society, academia, law enforcement. These workshops were a central part of our evidence gathering process and we are grateful to those who participated in them.

Limitations and additional considerations

2.41 We looked at current safety features that providers use as part of our evidence gathering. This informed both our good practice steps and the development of the case studies for this section.

2.42 Some of the evidence we use in the following sections comes from our analysis of safety features in use on specific services. This analysis has been an important part of our effort to ensure the safety tools we recommend are practical and technically feasible.

2.43 We have drawn on examples of good practice from a range of different services. We have looked at safety measures on dating services, including Hinge and Bumble; social media and video sharing services such as Facebook, Instagram, Reddit, YouTube, Snap, Twitch, Tumblr, TikTok, Discord and Imgur; search services, including Bing; and pornography services, such as those provided by Aylo and OnlyFans. At this stage, we are not in a position to offer any endorsement or comprehensive assessment of how effectively these services have implemented the features or their broader approach to women and girls' safety.

2.44 While we have engaged with a range of different service types, there are areas, for example gaming, file-sharing and search services, where we have less evidence of good practice. We also recognise that this is a fast-moving space, both in terms of how harms manifest and the kind of safety interventions available for providers. In consulting on the draft Guidance, we welcome further evidence from stakeholders on the benefits and risks of the good practice steps we have set out, as well as further examples of good practice. We also invite stakeholders to provide any additional information that may help strengthen our evidence base on good practice, as well as bad practice, including for different service types and services of different sizes.

2.45 Finally, we consider that some of the foundational and good practice steps proposed in the draft Guidance to improve women and girls' online safety are also likely to benefit other groups at heightened risk of experiencing the online harms this draft Guidance focuses on. This could include, for example, the heightened risks of pile-ons because of their race or ethnicity,[49] and those at a heightened risk of a range harms due to their gender identity or

[49] In a study by Amnesty International, Black, Asian and Minority Ethnic (BAME) women MPs received almost half (41%) of the abusive tweets, despite there being almost eight times as many white MPs in the study. Source: Amnesty International UK, 2017. Black and Asian Women MPs Abused More Online. [accessed 6 February 2025]; Ofcom, 2024. Experiences of using online services. [accessed 6 February 2025].

sexuality.[50] We have considered these potential positive impacts on other groups as part of our Equality Impact Assessment (see Annex A1).

Rationale and supporting evidence for the nine actions

2.46 In this section, we set out our rationale and the supporting evidence for each of the nine actions. For each action, we explain the overarching outcome we think the action could achieve for women and girls' safety, including why we consider it to be an important area for providers to go further than what we have set out in the foundational steps. We also discuss the evidence base in support of the good practice steps and associated case studies.

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

2.47 Governance and accountability processes, including how decisions are made and prioritised, form the foundation of how a service operates. Various sources suggest that service providers have been slow to address the complexities of online gender-based harms due to a lack of accountability, inconsistent enforcement, and a failure to prioritise user safety.[51] This is due a range of factors, including a lack of diverse perspectives in leadership, particularly from women and marginalised groups.[52] Actively embedding the concerns of women and girls within leadership and decision making is essential to ensuring online gender-based harms is accounted for thoroughly, and that new and emerging risks are swiftly identified and mitigated.[53]

2.48 In the draft Guidance, we include **foundational steps** and associated **case studies** which we consider relevant to providers fulfilling this action from across our draft and final Codes of Practice (in our Governance measures[54] and Terms of Service measures).[55]

2.49 In addition, we have analysed wider evidence suggesting **good practice steps** providers could take to further demonstrate, both internally and externally, a commitment and accountability for women and girls' safety. Good practice steps could include:

---

[50] Ofcom's Online Experiences Tracker data found that reports of stalking, cyberstalking or harassing behaviour are higher among transgender women and non-binary people (16%) compared to cisgender respondents (4%). Source: Ofcom, 2024. Experiences of using online services. [accessed 6 February 2025]; According to 2016 US research, 33% of the LGBTQ+ individuals sampled had been sexually harassed online, compared to 6% of heterosexual people. Source: Data & Society Research Institute/CiPHR (Lenhart, A., Ybarra, M., Zickuhr, K. and Price-Feeney, M.), 2016. Online Harassment, digital abuse and cyberstalking in America. [accessed 6 February 2025].

[51] Akiwowo, S., 2022. How to Stay Safe Online. [accessed 22 October 2024]; Taylor, L., 2021. Public Actors Without Public Values: Legitimacy, Domination and the Regulation of the Technology Sector, *Philosophy & Technology,* 34. [accessed 16 December 2024]; Investor Alliance for Human Rights, 2024. Investors Say Tech Companies are Failing to Address Systemic Human Rights Risks Inherent in Business Models and Exacerbated by AI. [accessed 16 December 2024].

[52] Akiwowo, S., 2022. How to Stay Safe Online. [accessed 22 October 2024]; Diversity in Tech, 2024. The Lack of Diversity in Tech. [accessed 16 December 2024]; White, S., 2024. Women in tech statistics: The hard truths of an uphill battle, *CIO,* 8 March. [accessed 16 December 2024]; Department for Science, Innovation & Technology and PUBLIC, 2025. Platform Design and the Risk of Online Violence Against Women and Girls. [accessed 12 January 2025].

[53] 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 22 October 2024].

[54] Illegal Content (ICU A1, ICU A2, ICU A3, ICU A4, ICU A5, ICU A6, ICU A7, ICS A1, ICS A2, ICS A3, ICS A4, ICS A5, ICS A6, ICS A7), draft Protection of Children (PCU A1, PCU A2, PCU A3, PCU A4, PCU A5, PCU A6, PCU A7, PCS A1, PCS A2, PCS A3, PCS A4, PCS A5, PCS A6, PCS A7).

[55] Illegal Content (ICU G3, ICS G3), draft Protection of Children (PCU D3, PCS D3).

- **Setting policies** designed to tackle forms of online gender-based harm.[56] [57]We considered evidence and examples highlighting how terms of service can clearly describe harms to women and girls, such as 'misogynoir' (hate directed at Black women and girls),[58] and set sexual harassment policies, which we explored in a case study.

  > While the Act requires providers to take down illegal content, and to protect children from harmful content, it is up to providers to determine where they want to set their thresholds about what kind of legal content adults can encounter on their service. Some choose to do so in a way which covers different subsets of content and activity that disproportionately affects women and girls, such as dedicated policies on sexual harassment.

  > Policies on gender-based harms can be particularly effective where they are designed to capture the specific ways that content or activity manifests on the service because of its functionalities or features. They can also help users understand what kind of content a provider has chosen to allow on a service.

- **Ensuring that governance and decision-making consider intersectionality** of online harms. During our workshop, we heard this can help ensure harms are effectively addressed.[59] This step is also supported by multiple sources from both academics and civil society, noting it can help ensure harms are addressed holistically.[60]
- **Consulting with subject matter experts**, particularly those with experience of supporting survivors of gender-based harms when setting policies and Terms and Conditions. Existing published evidence,[61] feedback from workshop participants,[62] and desk-based research into industry practice, indicate that consultations can be done to support the development of Terms that capture the sensitivities of online gender-based harms.
- **Training staff** involved in setting policies or governance and decision making on online gender-based harms and safety-by-design. This was suggested during our workshops as a means to improve the safety of women and girls.[63]

---

[56]Department for Science, Innovation & Technology and PUBLIC, 2025. Platform Design and the Risk of Online Violence Against Women and Girls. [accessed 12 January 2025].

[57] Ultimately, it is up to services to decide which policies will be most appropriate for their service.

[58] Bailey, M., 2021. Misogynoir Transformed: Black Women's Digital Resistance. [accessed 28 October 2024]; Glitch, 2023. The Digital Misogynoir Report: Online abuse against Black women allowed and enabled to thrive. [accessed 22 October 2024]; 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 22 October 2024].

[59] Ofcom Stakeholder Workshop 1 on Women and Girls Online Safety, 16 September 2024.

[60] Bailey, M., 2021. Misogynoir Transformed: Black Women's Digital Resistance. [accessed 28 October 2024]; Glitch, 2023. The Digital Misogynoir Report: Online abuse against Black women allowed and enabled to thrive. [accessed 22 October 2024]; Noble, S. 2018. Algorithms of Oppression: How Search Engines Reinforce Racism. [accessed 19 December 2024].

[61] 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 22 October 2024]; Strohmayer, A., Slupska, J., Bellini, R., Neff, G., Coventry, L., Hairson, A. and Dodge, A., 2021. Trust and Abusability Toolkit: Centering Safety in Human-Data Interactions. [accessed 30 October 2024].

[62] Ofcom Stakeholder Workshop 1 on Women and Girls Online Safety, 16 September 2024; Ofcom Stakeholder Workshop 2 on Women and Girls Online Safety, 19 November 2024.

[63] Ofcom Stakeholder Workshop 1 on Women and Girls Online Safety, 16 September 2024. 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 22 October 2024]; Centre for

- **Creating a media literacy-by-design policy** to promote critical and informed use of its service, as set out in Best Practice Design Principles for Media Literacy.
- **Establishing an oversight mechanism**[64] for Trust and Safety decisions, which we explore in an illustrative case study.

> There could be flexibility in terms of what this external oversight mechanism could look like. Broadly, it could be used to conduct an independent quality assurance of trust and safety decisions, such as content moderation. This could involve engaging with external experts or setting up an external appeals ombudsman. Some evidence suggests this can help tackle certain forms of online gender-based abuse. [65]

> We recognise this step may be most appropriate for high-risk and high-reach services given the resource demands. Nevertheless, we consider that it can be an effective route for accountability on decision making related to women and girls' safety.

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

2.50 Risk assessments are a core element of ensuring a service is safe for users. Effectively capturing the experiences of women and girls is part of this. Existing evidence suggests that women and girls' experiences and gendered harms get broadly overlooked and culturally diminished in organisations.[66] This is why there is a need for gender-sensitive risk assessments[67] which capture the particular nuances and dynamics of gender-based harms.

2.51 We include **foundational steps** related to service providers risk assessment duties, as recommended in our Illegal Content Risk Assessment Guidance and draft Children's Risk Assessment Guidance. We also highlight our Codes of Practice on setting moderation policies that have regard to the findings of the risk assessment and evidence of emerging harms.[68]

2.52 Beyond these steps, we have identified additional **good practice** for service providers to further capture gender dynamics in their risk assessments[69] and strengthen their understanding of user behaviour and women and girls' experiences. The additional good practice steps could include:

International Governance Innovation (Dunn, S., Vaillancourt, T., and Brittain, H.), 2023. Supporting Safer Digital Spaces. [accessed 30 January 2025].

[64] It is worth noting that we do not have powers to include alternative dispute resolutions (ADR) recommendations in the Codes as currently laid out in the Act. It would be for the Secretary of State to amend the Act by regulations to include ADR following consultation with Ofcom (and others).

[65] LEAF (Khoo, C.), 2021. Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence. [accessed 30 January 2025].

[66] Criado-Perez, C. 2019. Invisible Women. [accessed 12 February 2025].

[67] This can be done by making sure that existing risk assessment processes take into consideration gender-specific issues, or by conducting an additional assessment specifically and exclusively focused on gender and other intersecting characteristics.

[68] Illegal Content (ICU C3, ICS C2), Draft Protection of Children (PCU B2, PCS B3).

[69] These good practice steps are also examples of 'enhanced inputs' for providers' risk assessments, as set out in our Illegal Content Risk Assessment Guidance and draft Children's Risk Assessment Guidance. [accessed 12 February 2025].

- **Using external assessors** to monitor emerging threats was recommended by participants in our workshops.[70] Further evidence suggests it can be particularly relevant for localised or highly contextual risk areas.[71]
- **Engaging with survivors and victims** to better understand their experiences. We heard from participants at our workshop[72] the importance of ensuring the voices of survivors and victims are meaningfully taken into account when assessing risks of harm. However, we also heard that many of the organisations that are able to safely and responsibly facilitate these engagements face significant resourcing pressure. Providers should be aware of this when seeking out engagement with these kinds of organisations.
- **Conducting user surveys** to better understand users' preferences and experiences of risk. We illustrate how this sort of model could work through a case study.

> Chayn, an organisation that supports survivors and victims of domestic abuse, has worked with service providers to develop a survey using trauma-informed design. This survey aims understand users' experiences of sexual abuse, assault and harassment.[73] We have identified that this case study could impact data protection and privacy rights. Therefore, we have clarified that when considering the use of personal information, providers must also consider privacy rights and comply with duties under the UK General Data Protection Regulation ('UK GDPR'). We also encourage providers to consult the Information Commissioner's Office's (ICO) guidance on UK GDPR requirements[74] and the Age-Appropriate Design Code,[75] when processing the personal information of children.

- **Conducting additional impact assessments** on issues such as self-expression and freedom from discrimination. Evidence suggests this can support organisations to understand how different groups of users, including women and girls, may be impacted by their services.[76]

---

[70] Ofcom Stakeholder Workshop 1 on Women and Girls Online Safety, 16 September 2024; Ofcom Stakeholder Workshop 2 on Women and Girls Online Safety, 19 November 2024.

[71] 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 22 October 2024]; Glitch, 2023. The Digital Misogynoir Report: Online abuse against Black women allowed and enabled to thrive. [accessed 22 October 2024]; LEAF (Khoo, C.), 2021. Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence. [accessed 30 January 2025]; Centre for International Governance Innovation (Dunn, S., Vaillancourt, T., and Brittain, H.), 2023. Supporting Safer Digital Spaces. [accessed 30 January 2025]; eSafety Commissioner, 2024. Technology, gendered violence and Safety by Design. [accessed 3 January 2025]; National Democratic Institute, 2021. Addressing Online Misogyny and Gender Disinformation: A How-To Guide. [accessed 30 December 2024]; Ofcom Stakeholder Workshop 1 on Women and Girls Online Safety, 16 September 2024; Ofcom Stakeholder Workshop 2 on Women and Girls Online Safety, 19 November 2024.

[72] Ofcom Stakeholder Workshop 2 on Women and Girls Online Safety, 19 November 2024

[73] Chayn (Hussain, H.), 2021. Trauma-informed design: understanding trauma and healing.[accessed 6 February 2025].

[74] ICO, UK GDPR guidance and resources. [accessed 12 February 2025].

[75] ICO, Age appropriate design: a code of practice for online services. [accessed 12 February 2025].

[76] Equality and Human Rights Commission, 2019. Human Rights and Business. [accessed 16 December 2024].; United Nations Human Rights Office of the High Commissioner, 2011. UN Guiding Principles on Business and Human Rights. [accessed 16 December 2024]; 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 22 October 2024]; LEAF (Khoo, C.), 2021. Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence. [accessed 30 January 2025].

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

2.53 Evidence suggests transparency is an important mechanism for increasing responsibility of providers. This can help drive positive outcomes and support users to make informed and empowered decisions about their online experiences.[77] For women and girls, it could shine a light on how service providers are addressing online gender-based harms.

2.54 As referred to in the Legal Annex (Annex A1) to this consultation, under the Act, categorised services are required to publish annual transparency reports, some of which may be relevant to issues covering women and girls' safety. We have referred to this transparency duty in the draft Guidance, although we recognise that this applies to a smaller number of providers than the other duties.

2.55 We primarily focus this section on the **good practice steps** all service providers (and not just those categorised services who will have a specific duty in this area) can take to increase transparency. Specifically, we highlight:

- **Sharing information** about prevalence of different forms of online gender-based harms, gender- and race- disaggregated data on reports and outcomes, and more detail about which posts are flagged by automated content moderation.[78] We also heard from workshops participants that they would like this information shared.[79]
- Research suggests that **providing more detail about which posts are flagged** by automated content moderation, active bystanders, and the targeted users themselves can shine a light on women and girls' experiences.[80]
- **Exercising caution** in sharing personal information. We are aware that certain kinds of information could enable perpetrators to exploit a specific feature, or identify particular groups or individuals in ways that put them at risk. [81]

2.56 We have identified this good practice step as potentially impacting data protection and privacy rights. Therefore, we have signposted in the draft Guidance to relevant guidance from the ICO and made clear that providers will need to comply with the requirements of data protection law when sharing personal data. We note that the ICO is due to publish updated guidance on anonymisation in Spring 2025.[82]

2.57 We do not currently include a case study for this good practice step as we did not identify suitable industry practice to draw from. Therefore, we would welcome stakeholder responses with case studies of how transparency can be implemented in practice.

---

[77] As explored in our Consultation on Transparency Reporting, transparency requirements can lead providers of services to take measures to reduce harms stemming from their activities. We have seen some evidence of this in other sectors, but we are yet to see how these findings will translate to the online safety space.
[78] Glitch, 2023. The Digital Misogynoir Report: Online abuse against Black women allowed and enabled to thrive. [accessed 22 October 2024]; International Center for Journalists (Posetti, J. and Shabbir, N), 2022. The Chilling: A global study of online violence against women journalists. [accessed 22 October 2024]; Department for Science, Innovation & Technology and PUBLIC, 2025. Platform Design and the Risk of Online Violence Against Women and Girls. [accessed 12 January 2025].
[79] Ofcom Stakeholder Workshop 1 on Women and Girls Online Safety, 16 September 2024.
[80] Glitch, 2023. The Digital Misogynoir Report: Online abuse against Black women allowed and enabled to thrive. [accessed 22 October 2024];
[81] eSafety Commissioner, 2024. Technology, gendered violence and Safety by Design. [accessed 3 January 2025]; Appelman, N., 2023. Disparate Content Moderation Mapping Social Justice Organisations Perspectives on Unequal Content Moderation Harms and the EU Platform Policy Debate. [accessed 22 October 2024].
[82] See ICO, Our plans for new and updated guidance. [accessed 12 February 2025].

Action 4: Conduct abusability evaluations and product testing

2.58 Abusability evaluations and product testing emerged within our workshops and review of wider evidence base as an important mechanism for harm prevention. They encourage those involved in the design and deployment of products to pre-empt how something could be misused.[83] We have heard that this is particularly relevant to domestic abuse[84] and pile-on harassment, where perpetrators may use a range of innovative tactics to bypass safety features and exploit services.[85]

2.59 There are several **foundational steps** relevant to online gender-based harms which we highlight from our Illegal Content Risk Assessment Guidance and draft Children's Risk Assessment Guidance related to product testing and significant change risk assessment. In addition, we include steps drawn from our Illegal Codes of Practice measures on testing recommender systems.[86]

2.60 We have identified evidence indicating that additional **good practice steps** would be beneficial. These steps could help service providers go further, enabling a broader and deeper understanding of how users could exploit products in the context of online gender-based harms. They also limit the likelihood of users easily and widely exploiting a service, which can lead to resource and reputational consequences.[87]

- **Using red teaming for abusability testing** to help identify how malicious actors could exploit a service, feature of functionality. Our illustrative case study covers:

> Ofcom's research on how 'red teaming' can be used to prevent misuse of GenAI systems that may enable users to share and generate deepfake intimate images.[88]

> The kind of changes a provider of such services could make following this testing, drawing on evidence from various companies' red teaming approaches to GenAI systems. This can include improving input and output filters (such as content filters), updating blocklists for specific public figures, and removing nudity content from its training datasets.[89]

> These techniques may generally not be as valuable for smaller, low risk platforms, but would be valuable for services with known risks, such as a service that has a known issue with motivated perpetrators' using a particular functionality.

---

[83] Beers, A., Nguyên, S., Sioson, M., Mayanja, M., Ionescu, M., Spiro, E. S. and Starbird, K., 2021. The Firestarting Troll, and Designing for Abusability. [accessed 31 October 2024]; Ofcom stakeholder engagement workshop, 16 September 2024.

[84] Freed, D., Palmer, J., Minchala, D. E., Levy, K. E. C., Ristenpart, T. and Dell, N. L., 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology, *CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*.[accessed 28 October 2024]. Ofcom Stakeholder Workshop 1 on Women and Girls Online Safety, 16 September 2024.

[85] Jankowicz, N., Hunchak, J., Pavliuc, A., Davies, C., Pierson, S. and Kaufmann, Z., 2021. Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online. [accessed 31 October 2024].

[86] Illegal Content Codes of Practice (ICU E1)

[87] Strohmayer, A., Slupska, J., Bellini, R., Neff, G., Coventry, L., Hairson, A. and Dodge, A., 2021. Trust and Abusability Toolkit: Centering Safety in Human-Data Interactions. [accessed 24 October 2024].

[88] Ofcom, 2024. Red Teaming for GenAI Harms - Revealing the Risks and Rewards for Online Safety. [accessed 30 October 2024].

[89] For more information on what red teaming is and best practices when deploying the methodology see our discussion paper: Ofcom, 2024. Red Teaming for GenAI Harms - Revealing the Risks and Rewards for Online Safety. [accessed 30 October 2024].

- **Working with experts** with direct or relevant experience engaging with and understanding perpetrator behaviours. During our workshops, participants emphasised how this can help providers understand longstanding and emerging threats.[90]
- **Using 'personas'** to help design safer experiences based on how different women and girls' may use a service.[91]
- **Adhering to principles on monitoring and evaluating** features as evidenced in Ofcom's Best Practice Design Principles for Media Literacy.

Action 5: Set safer defaults

2.61 Our research shows that default settings can be a powerful tool to encourage safer behaviour online.[92] In the context of online gender-based harms, making a service less susceptible to abuse by default makes it easier for women and girls to keep themselves safe.

2.62 Safer defaults to address online gender-based harms include foundational steps from our Illegal Content Codes of Practice focusing on settings, functionalities and user support in relation to child safety and support.[93] We also highlight relevant measures from our Draft Protection of Children Codes of Practice related to user controls[94] and search moderation.[95]

2.63 We also include additional **good practice steps** including:

- **Setting stronger and customisable defaults** around interactions, privacy and geolocation. Evidence suggests these defaults could increase safety of women and girls experiencing unwanted contact.[96] They could also enable users to have better control over their own data use[97] and location information. We also heard from workshop participants that these defaults can support women and girls' safety.[98] We include an illustrative case study to provide further detail on how location information can be made safer by default.

  > Many users are not aware when they share photos and videos that include location metadata on social media and messaging services. This can inadvertently reveal users' locations.[99]

  > Likewise, many providers will collect and share users' locations to enhance social networking, which can lead to unintended consequences.[100]

---

[90] Ofcom Stakeholder Workshop 1 on Women and Girls Online Safety, 16 September 2024; Ofcom Stakeholder Workshop 2 on Women and Girls Online Safety, 19 November 2024.
[91] World Wide Web Foundation, 2021. Tech Policy Design Lab: Online Gender-Based Violence and Abuse. [accessed 30 October 2024]; Department for Science, Innovation & Technology and PUBLIC, 2025. Platform Design and the Risk of Online Violence Against Women and Girls. [accessed 12 January 2025].
[92] Ofcom, 2024. Behavioural insights to empower social media users. [accessed 12 February 2025].
[93] Illegal Content (ICU F1, ICU F2).
[94] Draft Protection of Children (PCU G4).
[95] Draft Protection of Children (PCS B2).
[96] eSafety Commissioner, 2024. Technology, gendered violence and Safety by Design. [accessed 3 January 2025].
[97] GLAAD, 2024. GLAAD Social Media Safety Index Platform Scorecard. [accessed 29 October 2024].
[98] Ofcom Stakeholder Workshop 1 on Women and Girls Online Safety, 16 September 2024
[99] Baddam, B., 2018. Technology and its Danger to Domestic Violence Victims: How Did He Find Me?. *Albany Law Journal of Science & Technology*, 28 (1). [accessed 29 October 2024].
[100] Dhondt, K., Le Pochat, V., Voulimeneas, A., Joosen, W. and Volckaert, S., 2022. A Run a Day Won't Keep the Hacker Away: Inference Attacks on Endpoint Privacy Zones in Fitness Tracking Social Networks, *Proceedings of*

> Our desk research indicates that some services are already deploying defaults to reduce unintentional sharing of location, for example by removing metadata from images on upload. Other services use badges, symbols or banners to notify users when they are sharing their location, or provide the option to share location for a specified time.
> We have taken steps to ensure that we signpost relevant guidance from the ICO on these issues.

- **Bundling defaults together.** Research shows this can be particularly valuable for users who want to implement the most security and privacy default options (for example, those at risk of controlling or coercive behaviour and stalking). [101] We heard from workshop participants,[102] as well as survivors and victims of domestic abuse and frontline experts, that this could be a valuable and reassuring tool.[103]
- Strengthening **account security,** for example through two-factor or multi-factor authentication. Following our discussions with stakeholders[104] and analysis of research supporting this good practice, we note it is particularly relevant for increasing safety for women and girls experiencing coercive control or stalking, as it can make it harder for perpetrators to monitor accounts non-consensually.[105]
- **Providing information about account access.** This has been shown to help users understand who has access to their accounts and on what devices. As with account security, this can be a valuable tool for those who are being monitored as part of a pattern of domestic abuse, or are otherwise at risk of having their account targeted or hacked.[106]
- **Identifying when to remind users about their default settings.** This can help users understand how their account is set up and what they may want to change.[107]

Action 6: Reduce the circulation of online gender-based harms

2.64 This action aims to capture the importance of preventing and reducing the spread of online gender-based harms. We consider steps to reduce the circulation of this content and

---

the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22). [accessed 29 October 2024].

[101] Behavioural Insights Team, 2021. Active Online Choices: Designing to Empower Users. [accessed 29 October 2024].

[102] Ofcom Stakeholder Workshop 1 on Women and Girls Online Safety, 16 September 2024.

[103] Ofcom / Refuge meeting, 20 November 2024

[104] Ofcom stakeholder engagement workshop, 16 September 2024; World Wide Web Foundation, 2021. Tech Policy Design Lab: Online Gender-Based Violence and Abuse. [accessed 30 October 2024]; eSafety Commissioner, 2024. Technology, gendered violence and Safety by Design. [accessed 3 January 2025].

[105] 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 22 October 2024]; End Cyber Abuse, 2022. Orbits: A global field guide to advance intersectional, survivor-centred, and trauma-informed interventions to technology-facilitated gender-based violence. [accessed 5 February 2025]; Chayn, 2022. Trauma-informed design: the whitepaper. [accessed 17 December 2024]; 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 3 January 2025];

[106] Ofcom stakeholder engagement workshop, 16 September 2024; 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 3 January 2025];

[107] Wohllebe, A., Hübner, D., Radtke, U., Podruzsik, S., 2021. Mobile apps in retail: Effect of push notification frequency on app user behavior. *Innovative Marketing.* [accessed 30 January 2025].

activity are important in creating a safer life online for women and girls – as discussed in Chapter 2, misogynistic and abusive content often goes **'viral'**. This not only has a silencing impact on the women and girls targeted, but the sheer volume and reach of this content can normalise harmful gender dynamics, and in acute cases, radicalise boys and men.[108]

2.65 This action can be achieved in a variety of ways: from deterrence and friction ('persuasion') which ask users to reconsider what they are posting, to preventing uploads or taking down content ('removal'), or the downranking or deprioritisation ('reduction') of certain kinds of content. It is up to services to decide which methods will be most appropriate in each case. However, we expect that in most cases, a mix of approaches will be most effective.

2.66 User-to-user service providers should implement proportionate systems to prevent uploads of illegal content, as well as remove it swiftly when they become aware of it.[109] Likewise, search providers should put in place search moderation systems that allow them to moderate illegal content.[110] For legal content, in some cases, providers may also seek to limit the circulation of such content through persuasion, removal and reduction. This could be because it is harmful to children, and therefore providers need to take steps to protect children on their service from encountering it.[111] It could also be because such content violates a provider's terms of service.[112]

2.67 While prevention of upload through persuasion or removal is an effective way to reduce exposure to online gender-based harm, it may not always be possible or appropriate. This could be, for example, because the content is deemed by a service provider to be misleading, offensive, or otherwise risky, but not illegal, or otherwise not clearly violative of the terms of service.[113] In these cases, service providers may strive to reduce the harm. Reduction refers to limiting the circulation and visibility of content rather than removing it entirely.[114]

2.68 We include **foundational steps** across persuasion, removal and reduction related to content and search moderation drawn from the Illegal Content Codes,[115] as well as relating to recommender systems, age assurance, and user support from our draft Protection of Children Codes.[116]

---

[108] Vodafone, 2024. AI 'Aggro-rithms': young boys are served harmful content within 60 seconds of being online. [accessed 13 February 2025]; Institute of Strategic Dialogue (Bundtzen, S.), 2023. Misogynistic Pathways to Radicalisation: Recommended Measures for Platforms to Assess and Mitigate Online Gender-Based Violence. [accessed 29 October 2024].

[109] See section 10 of the Act which sets out 'safety duties about illegal content' which apply in relation to regulated user-to-user services.

[110] Section 27 of the Act sets out 'safety duties about illegal content' which apply in relation to regulated search services.

[111] Duties relating to the protection of children are set out in sections 11-13 and 20-21 of the Act for regulated user-to-user services and sections 28-30 and 31-32 for regulated search services.

[112] In Chapter 4 of the draft Guidance, we do not specify what service provider's terms of service should regulate, but rather review how they can enforce the policies they set out in their terms of service.

[113] For example, because it is harmful to children (e.g. pornography) or because content is highly contextual and therefore difficult to detect at the point of upload (e.g. some misogynistic content).

[114] Gillespie, T., 2022. Do Not Recommend? Reduction as a Form of Content Moderation, *Social Media + Society.* [accessed 12 February 2025].

[115] Illegal Content (ICU C9, ICS C1, ICS C7, ICS F2, ICS F3).

[116] Draft Protection of Children (PCU F1, PCU F2, PCS B1, PCU H2, PCU H3, PCU H4, PCU H5, PCU H6, PCU H7, PCU E3, PCS E3).

2.69 We have also identified a range of **good practice steps** providers can implement to further address the circulation of illegal and harmful content on their platforms. These fall into three categories:

- Persuasion. We include implementing **'frictions'**[117] **through nudges** (design measures within an online environment to promote some behaviours and/or discourage others). We also note some good practice that reflects stronger processes, such as introducing identity verification, which may reduce the 'disinhibition effect' that causes people to post more harmful content.[118] However, we note that identity verification can also introduce important privacy considerations.[119] [120] We include an illustrative case study about how 'nudges' could be implemented.

  > Our case study illustrates how a provider could use a nudge to prompt someone to edit a message that is likely to be harmful. Participants at our workshops identified this to be a beneficial feature.[121]
  > We are aware some providers of dating services currently deploy similar sorts of nudges, both to deter harmful uploads and to prompt users to deploy safety features such as blocking.
  > We are also aware that some services use forms of deterrence messaging for specific search terms.

- Removal. We highlight **hash matching for intimate image abuse**, drawing on evidence from providers already doing this voluntarily through their own systems or through partnerships with StopNCII.org.[122] We include this within a case study that explores how intimate image abuse could be addressed by pornographic services.

  > The adult content industry is at high risk of intimate image abuse. Recent cases highlight instances in which non-consensual intimate images and child sexual abuse material has been uploaded to adult services, and in some cases, the material was available for some time after being reported, resulting in significant public and financial pressure, as well as legal action.[123]
  > In this case study, we illustrate how providers can 'layer' different preventative techniques to address intimate image abuse. This includes techniques identified

---

[117] Cox, A. L., Gould, S. J., Cecchinato, M. E., Iacovides, I. and Renfree, I., 2016. Design frictions for mindful interactions: The case for microboundaries, *CHI EA '16: Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems.* [accessed 28 January 2025]; Department for Science, Innovation & Technology and PUBLIC, 2025. Platform Design and the Risk of Online Violence Against Women and Girls. [accessed 12 January 2025].

[118] Ofcom Stakeholder Workshop 2 on Women and Girls Online Safety, 19 November 2024; Cheung, C.M., Wong, R.Y.M. and Chan, T.K., 2021 Online disinhibition: conceptualization, measurement, and implications for online deviant behavior, *Industrial Management & Data Systems*, 121 (1). [accessed 17 December 2024].

[119] Identity verification was discussed as a potential safety tool at both our September and November stakeholder workshops. Participants outlined both benefits and risks of such features.

[120] Ofcom will be consulting on draft guidance for Category 1 services specifically on identity verification in the future which we expect to include further details on how to implement verification appropriately.

[121] Ofcom Stakeholder Workshop 2 on Women and Girls Online Safety, 19 November 2024.

[122] Following feedback to our November 2023 Illegal Harms Consultation (Domestic Abuse Commissioner, Refuge, The Cyber Helpline, and Victims Commissioner), we will set out proposals for some additional measures in our Spring 2025 Consultation. This will feature a range of potential measures, including but not limited to measures to ban those that share CSAM, Intimate Image Abuse Hash Matching to prevent the sharing of non-consensual imagery, and a broader automated content moderation measure.

[123] BBC, 2021. GirlsDoPorn victims win rights to their videos, 17 December. [accessed 06 January 2025].

through our desk research and workshops[124] aimed at addressing intimate image abuse, such as hash matching, consent 'nudging', uploader verification, deterrence messaging, and consent verification. We are aware that several pornography services currently deploy similar techniques.

> If implemented effectively, these methods for preventing intimate image abuse can stop harm from occurring on a service. They can not only reduce the risk of harm from the initial upload but also interrupt any future circulation of that content. This is particularly relevant for intimate image abuse content which can easily go 'viral'. [125]

- Reduction. As set out in Chapter 2, online gender-based harms can not only have a silencing impact on the women and girls targeted but also normalise harmful gender dynamics due the sheer volume and reach of this content. In acute cases, it can even radicalise boys and men. We draw on a range of evidence and recommendations made by participants in our workshops to showcase other ways providers can reduce circulation and exposure of harmful content, including **deprioritising,**[126] **blurring**[127] and **demonetising**[128] harmful content, as well **as removing links**[129] and **scanning for duplicates**[130] of violative content.

2.70 Many of the methods in this section (persuasion, removal, and reduction) often rely on automated processes. Importantly, many of them may use 'proactive technology' within the meaning of the Act.[131]

2.71 We outline additional good practice steps as well as an illustrative case study exploring how these automated systems can be continually improved to be accurate, effective, contextually nuanced and unbiased in the context of online gender-based harms.[132]

---

[124] Ofcom Stakeholder Workshop 1 on Women and Girls Online Safety, 16 September 2024; Ofcom Stakeholder Workshop 2 on Women and Girls Online Safety, 19 November 2024.
[125] Law Commission, 2022. Intimate image abuse: A final report. [accessed 30 January 2025].
[126] Appelman, N., 2023. Disparate Content Moderation Mapping Social Justice Organisations Perspectives on Unequal Content Moderation Harms and the EU Platform Policy Debate. [accessed 22 October 2024]; 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 22 October 2024]; Ofcom Stakeholder Workshop 1 on Women and Girls Online Safety, 16 September 2024.
[127] For example, the use of automatically blurring nude images to prevent cyberflashing. Source: 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 22 October 2024]; Ofcom Stakeholder Workshop 1 on Women and Girls Online Safety, 16 September 2024. We are also aware from our desk research that some services use these tools.
[128] Jankowicz, N., Gomez-O'Keefe, I., Hoffman, L., and Vidal Becker A. 2024. It's Everyone's Problem: Mainstreaming Responses to Technology-Facilitated Gender-Based Violence. [accessed 13 February 2025.]
[129] For example, links to intimate image abuse content. Source: MyImageMyChoice, 2024. Deepfake Abuse: Landscape Analysis: The Exponential Rise of Deepfake Abuse in 2023-2024. [accessed 20 January 2025].
[130] SWGfL (Revenge Porn Helpline) response to the November 2023 Illegal Harms Consultation, p.14.
[131] Section 231 of the Act. Please see footnote 38 which explains potential restrictions on our ability to demonstrate certain good practice should be Codes measures.
[132] Ofcom Stakeholder Workshop 1 on Women and Girls Online Safety, 16 September 2024; Ofcom Stakeholder Workshop 2 on Women and Girls Online Safety, 19 November 2024; Kwarteng, J., 2022. Misogynoir: Challenges in Detecting Intersectional Hate, *Social Network Analysis and Mining,* 12 (1). [accessed 31 October 2024]; Glitch, 2023. The Digital Misogynoir Report: Online abuse against Black women allowed and enabled to thrive. [accessed 22 October 2024];

2.72 We intend to consult on further measures related to this action later this year – including automated content moderation and hash matching for intimate image abuse. For now, we have included these within our good practice steps.

Action 7: Give users better control of their own experiences

2.73 Core to women and girls' safety online is empowering them to curate their own experiences and have greater control over who contacts them, what they see, and what information about them is visible or searchable to others. In following this action, we are asking service providers to consider that 'safety' may look different to those at risk of online gender-based harm, including how it can change over time.

2.74 In the draft Guidance, we include foundational steps and associated case studies which we consider relevant to providers fulfilling this action based on measures from across our Illegal Content Codes and draft Protection of Children Codes on User Support, User Controls, and Recommender Systems.[133]

2.75 In addition, we have identified several **good practice steps** providers could take to further improve the experiences of women and girls, especially those experiencing significant risks of harm who may be considering leaving a service:[134]

- Allowing users to delete or change the **visibility settings** of the content they upload. Multiple sources from civil society note the importance of allowing users to personalise their privacy settings.[135] We heard from survivors of domestic abuse that they wanted more options to increase their privacy, and for that privacy to stay in place when services or functionalities update.[136]
- Providing users with tools to **block and mute** multiple accounts simultaneously was suggested in our workshop,[137] as well as in various reports, [138] as a means to provide women and girls with greater control over who can contact them. We explore how this could be implemented in an illustrative case study.

> We heard from participants during our workshop that providers may offer users a variety of mass blocking tools which allow them to control more easily who interacts with their accounts and content online.[139]

[133] Illegal Content (ICU J1, ICU J2, ICU F2), draft Protection of Children (PCU G1, PCU G2, PCU F3, PCU G4, PCU E1, PCU E2, PCU E3, PCS E1).
[134] A study from UNESCO on the experiences of women journalists found that 1 in 5 women surveyed described how they withdrew from all online interaction following their experience. Source: UNESCO (Posetti, J., Aboulez, N., Bontcheva, K., Harrison, J. and Waisbord, S.), 2020. Online Violence Against Women Journalists. [accessed 6 January 2025].
[135] World Wide Web Foundation, 2021. Tech Policy Design Lab: Online Gender-Based Violence and Abuse. [accessed 30 December 2024]; End Cyber Abuse, 2022. Orbits: A global field guide to advance intersectional, survivor-centred, and trauma-informed interventions to technology-facilitated gender-based violence. [accessed 5 February 2025].
[136] Ofcom / Refuge meeting, 20 November 2024.
[137] Ofcom Stakeholder Workshop 2 on Women and Girls Online Safety, 19 November 2024.
[138] 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 22 October 2024]; Institute for Strategic Dialogue (ISD) response to the November 2023 Illegal Harms Consultation, p.11; Department for Science, Innovation & Technology and PUBLIC, 2025. Platform Design and the Risk of Online Violence Against Women and Girls. [accessed 12 January 2025]. .
[139] Ofcom Stakeholder Workshop 2 on Women and Girls Online Safety, 19 November 2024.

> This could include, for example, giving users the options for automated blocking processes, or to not only to block a post's author but all users who have re-shared it or follow that account.

- **Allowing users to filter out content** from users without identity verification.[140]
- **Providing users with greater control over what content is recommended** to them.[141]
- **Allowing users to signal what kind of content they do and do not want to see.** We had regard to evidence from civil society and the Department for Science, Innovation & Technology that this level of personalisation provides women and girls with the ability to curate their online experiences.[142] We explore this in an illustrative case study that details how services can let users set custom filters to hide content containing terms or themes they do not want to engage with.[143]
- Signposting users to **supportive information**. In addition to existing published evidence,[144] we heard from stakeholders at our workshop about the importance of signposting users to specialist support for gender-based harms.[145]

Action 8: Enable users who experience online gender-based harms to make reports

2.76 One of the main themes we have identified from research reports,[146] engagement with civil society organisations,[147] and consultation responses[148] was the need for reporting and complaints systems to work for women and girls. Developing accessible, navigable, and trauma-informed reporting and complaints systems is essential to enabling women and girls who experience online gender-based harms to make reports.

2.77 We include **foundational steps** and associated case studies in the draft Guidance based on our Illegal Content Codes and draft Protection of Children Codes on Reporting and Complaints, as well as User Support.[149]

2.78 We also include additional **good practice steps** providers can take to further improve the experiences of women and girls reporting online gender-based harms on their services. This

[140] 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 22 October 2024].
[141] 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 22 October 2024].
[142] World Wide Web Foundation, 2021. Tech Policy Design Lab: Online Gender-Based Violence and Abuse. [accessed 30 December 2024]; eSafety Commissioner, 2024. Technology, gendered violence and Safety by Design. [accessed 30 January 2025].
[143] Department for Science, Innovation & Technology and PUBLIC, 2025. Platform Design and the Risk of Online Violence Against Women and Girls. [accessed 12 January 2025].
[144] 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 22 October 2024]; LEAF (Khoo, C.), 2021. Deplatforming Misogyny. [accessed 30 January 2025]; Department for Science, Innovation & Technology and PUBLIC, 2025. Platform Design and the Risk of Online Violence Against Women and Girls. [accessed 12 January 2025].
[145] Ofcom Stakeholder Workshop 1 on Women and Girls Online Safety, 16 September 2024; Ofcom Stakeholder Workshop 2 on Women and Girls Online Safety, 19 November 2024
[146] Refuge, 2022. Marked as Unsafe. [accessed 30 January 2025].
[147] Ofcom Stakeholder Workshop 1 on Women and Girls Online Safety, 16 September 2024; Ofcom Stakeholder Workshop 2 on Women and Girls Online Safety, 19 November 2024.
[148] Refuge response to the November 2023 Illegal Harms Consultation, p.4; Victims' Commissioner for England and Wales response to the November 2023 Illegal Harms Consultation, p,8; Domestic Abuse Commissioner's Office response to the November 2023 Illegal Harms Consultation, p.7.
[149] Illegal Content (ICU D1, ICU D2, ICS D1, ICS D2, ICS D3, ICS D4, ICS D5, ICU D4, ICU D5, ICU D6, ICS F1), draft Protection of Children (PCU C1, PCU C2, PCS C1, PCS C2, PCU C4, PCS C4, PCS E2).

could improve safety while also giving providers access to data on users experience as users may be more able and willing to complete accurate reports.[150] The good practice steps include:

- Trauma informed processes, such as providing a 'quick **exit button**' throughout the reporting process to help ensure users' safety.[151]
- Allowing users to **track and manage their reports**. Multiple sources note that enabling users to track and manage their reports can provide increased agency and transparency,[152] which we explore in detail in a case study.
  - We draw on evidence from a design prototype from the Web Foundation that demonstrates how providers could enable users to track and manage their reports.[153]
  - We envisage this is most relevant to services that receive a high volume of reports as it could be technically complex to implement, especially someone makes multiple reports.
- A report from the eSafety Commissioner suggests that allowing **users to give feedback** on a service's reporting process can build constructive feedback loops.[154]
- Establishing **trusted flagger** programmes in partnership with organisations that have relevant expertise. We explore this in detail in a case study:
  - We considered feedback from workshop participants[155] about trusted flagger programmes emphasising they can allow experts to escalate sensitive and contextual issues such as domestic abuse and stalking.
  - We have explored in our case study how trusted flagger programmes can address women and girls' safety. However, we heard that there are also significant operational challenges for both service providers and the organisations designated as trusted flaggers to be mindful of.[156]
- In addition to evidence,[157] we heard from workshop participants[158] that allowing users to **report incidents of abuse**, including those that occurred off-service**,** can be beneficial to women and girls' safety. We also provide a case study to illustrate how this could be implemented.

---

[150] Refuge, 2022. How online platforms are failing domestic abuse survivors. [accessed 17 December 2024]. The report said, 'This is likely due to the myriad barriers survivors faced when reporting, such as the distress caused from lengthy waiting times.'
[151] Chayn, 2022. Trauma-informed design: the whitepaper. [accessed 17 December 2024]; eSafety Commissioner, 2024. Technology, gendered violence and Safety by Design. [accessed 30 January 2025].
[152] End Cyber Abuse, 2022. Orbits: A global field guide to advance intersectional, survivor-centred, and trauma-informed interventions to technology-facilitated gender-based violence. [accessed 5 February 2025]; PEN America (Vilk, V. and Lo, K.), 2023. Shouting into the Void. [accessed 30 December 2024]; Refuge response to the November 2023 Illegal Harms Consultation, p.12.
[153] World Wide Web Foundation, 2021. Tech Policy Design Lab: Online Gender-Based Violence and Abuse. [accessed 30 December 2024].
[154] eSafety Commissioner, 2024. Technology, gendered violence and Safety by Design. [accessed 30 January 2025].
[155] Ofcom Stakeholder Workshop 2 on Women and Girls Online Safety, 19 November 2024.
[156] Ofcom Stakeholder Workshop 2 on Women and Girls Online Safety, 19 November 2024.
[157] Wilson Center (Jankowicz, N., Hunchak, J., Pavliuc, A., Davies, C., Pierson, S. and Kaufmann, Z.), 2021. Malign Creativity: How gender, sex, and lies are weaponized against women online. [accessed 30 January 2025].
[158] Ofcom Stakeholder Workshop 2 on Women and Girls Online Safety, 19 November 2024.

> The ability to report off-service abuse could enable providers to recognise and address how online gender-based harms are often part of wider patterns of behaviour.[159]
> We are aware that some providers already implement similar reporting systems that allow them to investigate and take action when presented with evidence of certain types of off-service conduct, including doxing and carrying out non-consensual sexual activities.
> We believe this kind of offering would be especially relevant for services which enable offline encounters, such as dating and other meet-up services.

- Adopting principles on **user-centric design** as set out in Ofcom's Best Practice Principles for Media Literacy By Design.

Action 9: Take appropriate action when online gender-based harms occur

2.79 This action covers the ways providers react to online gender-based harms once they have happened. This includes content and activity identified through user reports, as well as content and activity which a provider has become aware of through other means, for example through automated content moderation.

2.80 The foundational steps and associated case studies we highlight in the draft Guidance under this action relate to measures in our Illegal Content Codes and draft Protection of Children Codes on content moderation and reporting and complaints.[160]

2.81 Providers could further build on these measures to ensure their response supports survivors and victims through a range of **good practice steps,** including:

- Taking **enforcement action** against users who continually violate a service's Terms of Service. During our stakeholder engagement workshop, we heard that this is an important means for providers to support women and girls.[161] Additional evidence indicates the importance of appropriate responses to those violating terms repeatedly.[162] We also include an illustrative case study on how this could be implemented.

> Evidence shows a small number of users are responsible for a high proportion of harm. These users engage in repetitive and abusive behaviour which targets women, such as repeatedly posting the same sexually explicit content.[163] The case study sets out that providers could reduce the impact of serial perpetrators through strike-based enforcement policies.

[159] Domestic Abuse Commissioner's Office response to the November 2023 Illegal Harms Consultation, p.3.
[160] Illegal Content (ICU C2, ICU C4, ICU C5, ICU C6, ICU C7, ICU D7, ICU D8, , ICU D10, ICS C3, ICS C4, ICS 5, ICS C6, ICS D6, ICS D7, ICS D9), draft Protection of Children (PCU B1, PCU B3, PCU B4, PCU B5, PCU B6, PCU C5, PCU C6, PCU C8, PCS B4, PCS B5, PCS B6, PCS B7, PCS C5, PCS C6, PCS C8).
[161] Ofcom Stakeholder Workshop 2 on Women and Girls Online Safety, 19 November 2024.
[162] Wilson Center (Jankowicz, N., Hunchak, J., Pavliuc, A., Davies, C., Pierson, S. and Kaufmann, Z.), 2021. Malign Creativity: How gender, sex, and lies are weaponized against women online. [accessed 30 December 2024]; 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 22 October 2024]; International Center for Journalists (Posetti, J. and Shabbir, N), 2022. The Chilling: A global study of online violence against women journalists. [accessed 22 October 2024];
[163] Wilson Center (Jankowicz, N., Hunchak, J., Pavliuc, A., Davies, C., Pierson, S. and Kaufmann, Z.), 2021. Malign Creativity: How gender, sex, and lies are weaponized against women online. [accessed 30 December 2024];

- We are aware some service providers already deploy similar kinds of strike-based policies. Users are often informed when they receive a strike and about the consequences of this.
- These techniques for addressing serial perpetrators are likely to be most useful and appropriate on services with a known issue of motivated perpetrators or the misuse of a particular functionality. Providers should be mindful of the implications for users' privacy, self-expression, and ability to associate with others.
- We have identified this case study as potentially impacting on data protection and privacy rights. Content moderation and tools that assess users' behaviours are likely to involve processing of personal data. This includes where moderation actions are applied to a user's account (such as a strike, service restriction or ban). We have therefore signposted to relevant ICO guidance on these issues.[164]

- Adding **fact-checking and labelling.** Our evidence suggests this can be leveraged during a pile-on to help respond to gendered misinformation.[165]
- **Adding watermarks and metadata.** Watermarks in particular have been shown to be a potential response to the circulation of non-consensual intimate image abuse, including for sex workers.[166]
- We heard from workshop participants that identifying and preventing the creation of new accounts by banned users is important in making services safer for survivors and victims of online gender-based harms.[167]
- **Sending high risk reports (e.g. domestic abuse)** to specialist teams can help to ensure the report is handled accurately and with necessary context.[168] Relatedly, we explain that providers could use **dedicated reporting channels** for online gender-based harms.[169] During the development of the draft Guidance, we spoke with a group of survivors and front line domestic abuse organisations who emphasised how difficult it can be to receive an appropriate response on content that is threatening or coercive, but could look benign.[170]
- A report on safety-by-design from eSafety Commissioner suggests **hiding content likely to be harmful** while it is being assessed.

2.82 We welcome feedback from stakeholders on these good practice steps and case studies, including examples of other services currently deploying the same or similar practices.

---

[164] This includes the ICO's guidance on Content moderation and data protection and its forthcoming guidance on Profiling and Behaviour ID Tools for Online Safety (due to be published in Spring 2025). Source: ICO, Our plans for new and updated guidance. [accessed 12 February 2025].
[165] Internet Governance Forum, 2021. Best Practice Forum on Gender and Digital Rights: Exploring the concept of gendered disinformation. [accessed 30 December 2024]; National Democratic Institute, 2021. Addressing Online Misogyny and Gender Disinformation: A How-To Guide. [accessed 30 December 2024].
[166] Sanders, T., Trueman, G., Worthington, K. and Keighley, R., 2023. Non-consensual sharing of images: Commercial content creators, sexual content creation platforms and the lack of protection, *New Media & Society*, 27 (1). [accessed 12 February 2025].
[167] Ofcom Stakeholder Workshop 1 on Women and Girls Online Safety, 16 September 2024; Ofcom Stakeholder Workshop 2 on Women and Girls Online Safety, 19 November 2024.
[168] 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 22 October 2024]; Women's Aid, 2023. Influencers and Attitudes: How will the next generation understand domestic abuse?. [accessed 24 October 2024].
[169] Centre for International Governance Innovation (Dunn, S., Vaillancourt, T., and Brittain, H.), 2023. Supporting Safer Digital Spaces. [accessed 30 January 2025].
[170] Ofcom / Refuge meeting, 20 November 2024.

Question 2: Do you have any comments on the nine proposed actions? Please provide evidence to support your answer.

Question 3: Do you have any comments about the effectiveness, applicability or risks of the good practice steps or associated case studies we have highlighted in these nine action areas? Are there any additional recommendations of good practice we should consider, or any service providers who are currently implementing similar practices that we have not included? Please provide evidence to support your comment.

Note: we are not consulting on the foundational steps and associated case studies as the measures and guidance which underpin the foundational steps have gone through separate consultation processes.

Encouraging providers to take ambitious action

2.83 Our third objective with this draft Guidance is to encourage providers to take action to secure our vision for a safer life online for women and girls. As the online safety regulator, we have a range of tools available to us to encourage providers to take action.

2.84 The foundational steps set out in the draft Guidance are ones we have recommended in our Codes of Practice (either in final or draft form) or risk assessment guidance for securing compliance with legal duties.[171] Providers now have a duty to assess the risk of illegal harms on their services, with a deadline of 16 March 2025. Subject to the Codes completing the Parliamentary process, from 17 March 2025, providers will need to take the safety measures set out in the Codes or use other effective measures to protect users from illegal content and activity. We are ready to take enforcement action if providers do not act promptly to address the risks on their services.

2.85 We urge providers to go further and implement the good practice we have set out, in order to make their services, functionalities and features safer for women and girls. While not substitutes for the foundational steps, should providers choose to take up the good practice we outline, this could supplement how they show us they are meeting their duties in the round.

2.86 We will also consider other ways we can encourage service providers to take the nine actions and implement the good practice examples. We would welcome views on effective approaches to engage services with the final Guidance and set an ambitions vision for women and girls' online safety.

2.87 As part of our effort to encourage providers to take action, we also plan to publish an assessment of how providers are keeping women and girls safe on their services. We will do this in the first half of 2027, around 18 months after we finalise the Guidance. The assessment will draw together insights gained through our broader regulatory work on online safety. It will also 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.

[171] Providers who take or use the measures described in a Code of Practice which are recommended for the purpose of complying with a relevant duty will be treated as having complied with that relevant duty although providers may take alternative steps to comply.

2.88 By publishing this report, we also hope to empower the public to make informed choices about the services they use.

2.89 We would welcome feedback from stakeholders on the approach to encouraging take up of the Guidance.

Question 4: Do you have any feedback on our approach to encouraging providers to follow the Guidance, including our proposal to publishing an assessment of how providers are addressing women and girls' safety? Do you have any examples or suggestions of other ways we could encourage providers to take up the 'good practice' recommendations?

Next steps

2.90 We are inviting stakeholders' views on our draft Guidance. The deadline for responses is 23 May 2025.

2.91 Once we have considered all responses, we will publish a statement explaining our final decisions on the Guidance, alongside the final Guidance itself. We expect this to be by the end of 2025.

Updating the Guidance

2.92 Once we have published the final Guidance, we will update it periodically to give service providers relevant information on how they can address content and activity that disproportionately affects women and girls. For example, we will update it as relevant:

- To reflect updated or finalised aspects of the online safety regime;[172]
- To reflect changes to relevant legislation, such as in relation to criminal offences;
- As and when there are other shifts in our understanding of how online gender-based harms manifest, or how it can be addressed, which we consider important to reflect.

2.93 As noted in paragraph 1.9, we must consult on any changes we make in the future.

[172] For example, we intend to consult on additional measures in spring 2025. This will include work we announced earlier this year, to consult on how automated tools can be used to proactively detect illegal content and the content most harmful to children, going beyond the automated detection measures we have currently recommended.

A1. Legal Annex

Ofcom's general duties

2.94 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.

2.95 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.

2.96 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 as amended by section 82 of the Act).

2.97 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.

2.98 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. They include 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.

Media literacy

2.99 As we explain in paragraph 2.37, we also propose to draw upon Ofcom's media literacy duties under section 11 of the CA 2003 (as amended by the Act) in our proposals for the draft Guidance. Ofcom's media literacy duties are set out under section 11 of the CA 2003.

2.100 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.

2.101 Ofcom must perform this new 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.

2.102 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 regulated services to protect themselves and others in relation to the matters set out in this section.[173]

Summary of relevant duties of providers under the Act

2.103 In the following sections, we summarise the provisions of the Act which are relevant to service providers for the purposes of this draft Guidance.

[173] 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.

Safety duties relating to illegal content

2.104 The Act imposes duties of care on providers of regulated user-to-user services and providers of regulated search services[174] in relation to, among other things, "illegal content".[175]

2.105 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.[176] 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.

2.106 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

2.107 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'[177]).[178]

2.108 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.[179] The duties on search services include using 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 Section 2, Volume 1 of Ofcom's Consultation on Protecting children from harms online.

[174] Part 2 of the Act provides definitions related to these services.
[175] Under section 59 of the Act, 'illegal content' is defined as "content that amounts to a relevant offence".
[176] Section 10 and 27 of the Act.
[177] As defined in section 60 of the Act.
[178] 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.
[179] 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).

Duties about content reporting and complaints

2.109 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 draft Guidance: content reporting[180] and complaints procedures.[181]

2.110 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

2.111 Providers of regulated user-to-user and search services have a duty to carry out a suitable and sufficient illegal content risk assessment[182] 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.

2.112 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[183] 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

2.113 The Act also sets out that where Ofcom has designated a relevant service as either category 1 or 2B (user-to-user services) or category 2A (search services or combined services), the service will appear on Ofcom's register of categorised services.[184] Once a year, Ofcom must issue every such provider with a transparency notice requiring them to produce a transparency report about that service.[185]

Human rights

2.114 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 European Convention of Human Rights ('ECHR').

[180] Section 20 and section 31 of the Act.
[181] Section 21 and section 32 of the Act.
[182] Section 9 and 26 of the Act.
[183] Section 11 and 28 of the Act.
[184] Section 95(2) of the Act.
[185] Section 77 of the Act.

2.115 Of particular relevance to Ofcom's functions under the Act are the right to freedom of expression (Article 10 ECHR)[186] and the right to privacy (Article 8 ECHR).[187] We have had particular regard to these rights when developing the draft Guidance, to ensure that the actions and good practice 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.[188] 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.

2.116 In formulating our proposals, we have carefully analysed where we have identified the potential for interference with ECHR rights, to make sure any such interference is proportionate. This analysis is set out in Annex A2.

Impact assessment

2.117 Impact assessments provide a valuable way of evaluating 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 a large majority of our policy decisions. Our impact assessment guidance sets out our general approach to how we assess and present the impact of our proposed decisions. We set out our impact assessment in relation to these proposals in Annex A2.

Equality and Welsh language impact assessments

2.118 See Annex A2 for more information about how Ofcom has applied its duties under the Equality Act 2010 and the Northern Ireland Act 1998, as well as our duties relating to the Welsh language, in producing the draft Guidance.

[186] The right to freedom of expression includes the freedom to hold opinions and to receive and impart information and ideas without interference by public authority. Article 10(2) of the ECHR states that this right may be restricted in certain circumstances.

[187] Article 8(1) of the ECHR states that everyone has the right to respect for his private and family life, his home and his correspondence. Article 8(2) sets out limited qualifications stating that public authorities must not interfere with the exercise of this right unless necessary in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[188] Other ECHR rights which may also be relevant to Ofcom's functions under the Act are the right to freedom of thought, conscience and religion (Article 9 ECHR) and the right to freedom of assembly and association (Article 11 ECHR).

A2. Impact assessments

Impact assessments

A2.1 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. 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 proposed decisions.[189]

A2.2 Our draft 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 they could take to tackle online gender-based harms.

A2.3 We assess the impact of our draft 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 impact of these measures have already been assessed in previous Ofcom publications related to online safety codes and risk assessment and transparency guidance. Here we therefore focus on the potential impact on service providers if they engage with the draft Guidance and implement the good practice steps.

Impacts on service providers

A2.4 Overall, we do not think the draft Guidance will impose any significant burdens on service providers. This is because the draft Guidance does not mandate any new requirements. Rather, it is framed as a call to action and sets out good practice that we strongly encourage service providers to implement.

Costs and risks

A2.5 Service providers who choose to engage with the final Guidance will incur some small costs in 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. We expect that service providers who choose to engage with the guidance would do so by taking the actions it sets out and implementing the good practice recommendations.

A2.6 Service providers that implement the good practice recommendations may incur additional costs. These costs could be more substantial and may be in the form of one-off and ongoing costs. In Table 3, we provide some consideration for what these costs could involve based on the draft Guidance and the examples of good practices highlighted across the actions. 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. We expect a service provider would only implement the good practice steps if it

[189] Ofcom, Impact assessment guidance, 2023.

considered the potential costs to be proportionate to the expected online safety benefits to users, given they are not required to adopt the good practices steps.

Actions	Example of good practice steps	Potential costs for service providers
Ensure governance and accountability processes address online gender-based harms	This could include having policies that are designed to tackle forms of online gender-based harms.	Staff costs associated with developing new polices, or updating existing policies, and implementing these policies to clearly tackle online gender-based violence.
Conduct risk assessments that focus on harms to women and girls	This could include conducting user surveys to better understand the experiences of different groups.	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 forms of online gender-based harms.	Staff costs associated with determining the information that can be shared on the prevalence of online gender-based violence, and on the effectiveness of measures in place.
Conduct abusability evaluations and product testing	This could include using red teaming for abusability testing.	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 defaults	This could include setting strong and customisable defaults around user interaction and privacy.	Staff and systems infrastructure costs associated with developing and implementing user defaults that are strong and customisable.
Reduce the circulation of content depicting, promoting or encouraging online gender-based harms	This could include continuously improving automated content moderation.	Staff and systems infrastructure costs associated with reviewing and improving 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.	Staff and systems infrastructure costs associated with developing and implementing tools that can provide users with greater control over the content they see.

Actions	Example of good practice steps	Potential costs for service providers
Enable users who experience online gender-based harms to make reports	This could include allowing users to track and manage their reports.	Staff and systems infrastructure costs associated with developing and implementing a system where users can track and manage reports.
Take appropriate action when online gender-based harms occurs	This could include taking action against users who continuously violate a service's Terms of Service.	Staff costs associated with determining what an appropriate form of action may be and when it may come into effect, and systems infrastructure costs associated with its implementation.

Table 3: Potential costs for service providers implementing the good practice steps

Rights assessment

A2.7 In Annex A1 of this consultation, we have set out Ofcom's duties under the European Convention of Human Rights ('ECHR'). In carrying out our rights assessment of our proposals, we have addressed the relevant rights impacts on users, services and other persons and have considered the extent to which our proposals may interfere with certain rights in the ECHR as set out in Schedule 1 of the Human Rights Act 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.

A2.8 We note 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.[190] The draft Guidance draws 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, and we do not separately consider any relevant impacts here.

Freedom of expression

A2.9 Any interference with this right 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 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.

A2.10 Overall, we consider that the actions and good practice steps we propose to include in the draft Guidance represent a fair balance between securing adequate protections for women

[190] Paragraph 10(1) of Schedule 4 to the Act states that *'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 (b)the importance of protecting the privacy of users.

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 consider that any interference with the right to freedom of expression is proportionate to the legitimate aims pursued and place weight on all the specific evidence of harm set out in our consultation. We have 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.

A2.11 We recognise 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. Existing evidence shows many women and girls limit their online speech due to concerns over abuse, harassment and other forms of harm. This can 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.

A2.12 We consider that in tackling gender-based harms service providers can have a significant impact on the online experience of women and girls, including positively impacting their ability to express themselves freely. Therefore, we consider it proportionate to the aim of creating a safer life online for women and girls that the good practice recommendations we have made may result 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, can do online.

Privacy

A2.13 Article 8 of the ECHR sets out the right to respect an individual's private and family life. Some of our good practice proposals will involve the collection and processing of personal data. The ICO is responsible for the regulation of information rights and data privacy. The ICO has a range of data protection compliance guidance which we encourage service providers to consult.

A2.14 In our good practice proposals, we make 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 have incorporated references to applicable ICO guidance on data protection legislation in the draft Guidance. For example, under Action 2, in relation to the case study on gender sensitive risk assessments, we have specified that when considering the use of personal information, providers must also consider privacy rights and comply with duties under the UK GDPR.

A2.15 We also encourage service providers to consult the ICO's guidance on UK GDPR requirements and the Age-Appropriate Design Code, when processing the personal information of children. Under Action 3: Be transparent about women and girls' online safety, one of the good practice steps is about exercising caution in sharing information about user reports and their outcomes and we remind services that they will need to comply the requirements of data protection law when sharing involves personal data. We have also noted in this consultation the forthcoming updated ICO guidance on anonymisation and pseudonymisation (due for publication in Spring 2025). In case study 9 on removing geolocation information by default, we reference standard 10 of the ICO's Age Appropriate Design Code. In case study 25 on taking action on serial perpetrators, we reference the ICO guidance Content moderation and data protection and planned forthcoming ICO guidance Behaviour ID Tools for Online Safety.

A2.16 We believe that our approach will assist service providers to limit the extent of any interference with a user's right to privacy while enabling them to follow the good practice steps set out in the draft Guidance. These steps are 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.

Equality impact assessment

Legal Context

A2.17 Section 149 of the Equality Act 2010 ('the 2010 Act') 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 2010 Act 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.

A2.18 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.[191]

A2.19 To help us comply with our duties under the 2010 Act 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.

A2.20 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[192]).

A2.21 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.

A2.22 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.

[191] Ofcom, 2014. Revised Northern Ireland Equality Scheme for Ofcom
[192] Ofcom, 2023. Impact assessment guidance

Equality impact assessment

A2.23 We have carefully considered the impacts of our proposals 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.

A2.24 The 'foundational steps' outlined in the draft Guidance reflect Codes measures and information from our risk assessment guidance we have already set for service providers (in statement or consultation) elsewhere. These steps have undergone previous Equality Impact Assessments, which concluded (either on a final or initial basis) 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.

A2.25 We have assessed the 'good practice steps' outlined in the draft Guidance and do not envisage they would have a detrimental impact on any particular group of people. Taken together, 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, in line with the broader aims of the Act.

A2.26 Our proposals aim to empower users, improve equality of opportunity and foster positive interactions between users. We consider this will benefit other groups of people beyond women and girls (who are the primary focus). For example, our proposals for good practice to address online gender-based harm in transparency reporting can improve users' understanding of how service providers address these types of harms. Our proposal for good practice in relation to safer defaults, such as bundling settings for services with many features or frequent updates, are valuable for those at risk of coercive and controlling behaviour and stalking, as they ensure users always have the most secure and private options. They can 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. Other proposals relating to abusability evaluations and product testing encourage providers to understand diverse user experiences and create an inclusive online environment. Red teaming may take into account abuse such as threats and harassment toward individuals with protected characteristics and help prevent it. Overall, we expect a wide range of users to benefit from implementing our good practice proposals.

A2.27 We note that no single method is completely free of bias and our draft 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, detailed in the following paragraphs, which could occur as an unintended consequence of our proposals, or if they are implemented without consideration of users with protected characteristics. We have considered these risks in setting out our proposals for good practice steps and believe that they can be generally mitigated as set out in the following paragraphs.

A2.28 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. There is also a risk of excluding certain groups if features are not well-designed. To mitigate these risks, we emphasise the importance of service providers implementing

these practices in a way that is inclusive, user-friendly and considerate of users' emotional and cognitive states. As mentioned in the draft Guidance, this can be achieved through gender-inclusive, accessible and regularly reviewed Terms of Service and community guidelines which respond to trends in online gender-based harms. 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.

A2.29 We also understand 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 suggest service providers implement robust verification processes and providing a clear appeal mechanism, as suggested in the draft Guidance.

A2.30 Overall, we believe 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 draft Guidance is designed to engage, inform and reduce online gender-based harms. We therefore consider that our proposals will have a generally positive impact on individuals with protected characteristics. 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 our good practice proposals.

Question 5: Do you have any comments on the impact assessment, rights assessment, or equality impact assessments? Please provide any information or evidence in support of your views.

Welsh language impact assessment

Legal context

A2.31 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).[193]

A2.32 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 so 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.

[193] 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.

Welsh language impact assessment

A2.33 The Welsh language has official status in Wales. To give effect to this, certain public bodies, including Ofcom, are required to comply with Welsh language standards.[194] Accordingly, we have considered:

- the potential impact of our policy decisions on opportunities for persons to use the Welsh language;
- the potential impact of our policy decisions on treating the Welsh language no less favourably than the English language; and
- how our recommendations have been formulated to have, or increase, a positive impact; or not to have adverse effects or to decrease any adverse effects.

A2.34 Ofcom's powers and duties in relation to online safety regulation are set out in the Act and must be exercised in accordance with our general duties under section 3 of the CA 2003. In formulating our proposals in this draft Guidance, where relevant and to the extent we have discretion to do so in the exercise of our functions, we have considered the potential impacts on opportunities to use Welsh and treating Welsh no less favourably than English.

A2.35 The 'foundational steps' outlined in the draft Guidance reflect Codes measures and information from our risk assessment guidance we have already set for service providers (in statement or consultation) elsewhere. As noted in this consultation document, these are wide-ranging and are also at different stages of implementation. These foundational steps have undergone previous Welsh Impact Assessments, as part of previous consultations and statements on implementing those aspects of the regime, which have concluded either on a final or initial basis 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.

A2.36 We have assessed the 'good practice steps' in the draft Guidance. We are recommending 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), user surveys (Action 2), information about account access (see Action 5), and when designing their reporting processes (see Action 8). To this extent, we consider 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. We do not consider that any adverse effects are likely to arise as a result of our proposals.

Question 6: Do you agree that the draft Guidance is likely to have positive effects on opportunities to use Welsh and treating Welsh no less favourably than English? If you disagree, please explain why, including how you consider the draft Guidance could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.

[194] The Welsh language standards with which Ofcom is required to comply are available on our website here.

A3. Where we are seeking input

We are seeking comments from all interested parties on the draft Guidance. In particular, we would welcome comments on the following:

Question 1: Do you have any comments on our proposed approach to 'content and activity' which 'disproportionately affects women and girls'?

Question 2: Do you have any comments on the nine proposed actions? Please provide evidence to support your answer.

Question 3: Do you have any comments about the effectiveness, applicability or risks of the good practice steps or associated case studies we have highlighted in Chapter 3, 4 and 5? Are there any additional examples of good practices we should consider? Please provide evidence to support your comment.

Question 4: Do you have any feedback on our approach to encouraging providers to follow this guidance, including our proposal to publishing an assessment of how providers are addressing women and girls' safety? Do you have any examples or suggestions of other ways we could encourage providers to take up the 'good practice' recommendations?

Question 5: Do you have any comments on our impact assessment, rights assessment, or equality impact assessment? Please provide any information or evidence in support of your views.

Question 6: Do you agree that our draft Guidance is likely to have positive effects on opportunities to use Welsh and treating Welsh no less favourably than English? If you disagree, please explain why, including how you consider the draft Guidance could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.

A4. Responding to this consultation

How to respond

A4.1 Ofcom would like to receive views and comments on the issues raised in this document, by 17:00 on Friday 23 May.

A4.2 You can download a response form here. You can return this by email or post to the address provided in the response form.

A4.3 If your response is a large file, or has supporting charts, tables or other data, please email it to OS-Section54@ofcom.org.uk, as an attachment in Microsoft Word format, together with the cover sheet. The email address is for this consultation only and will not be valid after 23 May 2025.

A4.4 Responses may alternatively be posted to the address below, marked with the title of the consultation:

Ofcom Online Safety Group.
Ofcom
Riverside House
2A Southwark Bridge Road
London SE1 9HA

A4.5 We welcome responses in formats other than print, for example an audio recording or a British Sign Language video. To respond in BSL:

- send us a recording of you signing your response. This should be no longer than 5 minutes. Suitable file formats are DVDs, wmv or QuickTime files; or
- upload a video of you signing your response directly to YouTube (or another hosting site) and send us the link.

A4.6 We will publish a transcript of any audio or video responses we receive (unless your response is confidential)

A4.7 We do not need a paper copy of your response as well as an electronic version. We will acknowledge receipt of a response submitted to us by email.

A4.8 You do not have to answer all the questions in the consultation if you do not have a view; a short response on just one point is fine. We also welcome joint responses.

A4.9 It would be helpful if your response could include direct answers to the questions asked in the consultation document. The questions are listed at Annex X. It would also help if you could explain why you hold your views, and what you think the effect of Ofcom's proposals would be.

A4.10 If you want to discuss the issues and questions raised in this consultation, please send an email to OS-Section54@ofcom.org.uk.

Confidentiality

A4.11 Consultations are more effective if we publish the responses before the consultation period closes. This can help people and organisations with limited resources or familiarity with the issues to respond in a more informed way. So, in the interests of transparency and good regulatory practice, and because we believe it is important that everyone who is interested in an issue can see other respondents' views, we usually publish responses on the Ofcom website at regular intervals during and after the consultation period.

A4.12 If you think your response should be kept confidential, please specify which part(s) this applies to and explain why. Please send any confidential sections as a separate annex. If you want your name, address, other contact details or job title to remain confidential, please provide them only in the cover sheet, so that we don't have to edit your response.

A4.13 If someone asks us to keep part or all of a response confidential, we will treat this request seriously and try to respect it, either by not publishing the response at all, or by only publishing the bits that are not confidential. Sometimes we might think it is important to disclose parts of a response that have been marked as confidential for reasons of transparency, but we will consult you before we do. Occasionally we might have a legal obligation to publish information or disclose it in court, but again, as far as possible, we will let you know.

A4.14 Even if your response is not marked as confidential, we might still decide not to publish all or part of it in certain circumstances. For example, if we have concerns about the impact on your privacy or the privacy of others, that the content of the response might facilitate the commission of crime, or about the sensitive nature of the content more generally. If we decide not to publish all or part of your response, we will still take it into account in our consideration of the matter.

A4.15 To fulfil our pre-disclosure duty, we may share a copy of your response with the relevant government department before we publish it on our website.

A4.16 Please also note that copyright and all other intellectual property in responses will be assumed to be licensed to Ofcom to use. Ofcom's intellectual property rights are explained further in our Terms of Use.

Next steps

A4.17 Following this consultation period, Ofcom plans to publish a statement by the end of 2025.

A4.18 If you wish, you can register to receive mail updates alerting you to new Ofcom publications.

Ofcom's consultation processes

A4.19 Ofcom aims to make responding to a consultation as easy as possible. For more information, please see our consultation principles in Annex x.

A4.20 If you have any comments or suggestions on how we manage our consultations, please email us at consult@ofcom.org.uk. We particularly welcome ideas on how Ofcom could more effectively seek the views of groups or individuals, such as small businesses and

residential consumers, who are less likely to give their opinions through a formal consultation.

A4.21 If you would like to discuss these issues, or Ofcom's consultation processes more generally, please contact the corporation secretary:

Corporation Secretary
Ofcom
Riverside House
2a Southwark Bridge Road
London SE1 9HA
Email: corporationsecretary@ofcom.org.uk

A5. Ofcom's consultation principles

Ofcom has seven principles that it follows for every public written consultation:

Before the consultation

1. Wherever possible, we will hold informal talks with people and organisations before announcing a big consultation, to find out whether we are thinking along the right lines. If we do not have enough time to do this, we will hold an open meeting to explain our proposals, shortly after announcing the consultation.

During the consultation

2. We will be clear about whom we are consulting, why, on what questions and for how long.
3. We will make the consultation document as short and simple as possible, with an overview of no more than two pages. We will try to make it as easy as possible for people to give us a written response.
4. When setting the length of the consultation period, we will consider the nature of our proposals and their potential impact. We will always make clear the closing date for responses.
5. A person within Ofcom will be in charge of making sure we follow our own guidelines and aim to reach the largest possible number of people and organisations who may be interested in the outcome of our decisions. Ofcom's Consultation Champion is the main person to contact if you have views on the way we run our consultations.
6. If we are not able to follow any of these principles, we will explain why.

After the consultation

7. We think it is important that everyone who is interested in an issue can see other people's views, so we usually publish the responses on our website at regular intervals during and after the consultation period. After the consultation we will make our decisions and publish a statement explaining what we are going to do, and why, showing how respondents' views helped to shape these decisions.

A6. Consultation coversheet

Basic details

Consultation title:

To (Ofcom contact):

Name of respondent:

Representing (self or organisation/s):

Address (if not received by email):

Confidentiality

Please tick below what part of your response you consider is confidential, giving your reasons why

- Nothing ☐
- Name/contact details/job title ☐
- Whole response ☐
- Organisation ☐
- Part of the response ☐

If you selected 'Part of the response', please specify which parts:

If you want part of your response, your name or your organisation not to be published, can Ofcom still publish a reference to the contents of your response (including, for any confidential parts, a general summary that does not disclose the specific information or enable you to be identified)?

Yes ☐ No ☐

Declaration

I confirm that the correspondence supplied with this cover sheet is a formal consultation response that Ofcom can publish. However, in supplying this response, I understand that Ofcom may need to publish all responses, including those which are marked as confidential, in order to meet legal obligations. If I have sent my response by email, Ofcom can disregard any standard e-mail text about not disclosing email contents and attachments.

Ofcom aims to publish responses at regular intervals during and after the consultation period. If your response is non-confidential (in whole or in part), and you would prefer us to publish your response only once the consultation has ended, please tick here.

Name Signed (if hard copy)

A7. Consultation survey

Please tell us how you came across about this consultation.

- ☐ Email from Ofcom
- ☐ Saw it on social media
- ☐ Found it on Ofcom's website
- ☐ Found it on another website
- ☐ Heard about it on TV or radio
- ☐ Read about it in a newspaper or magazine
- ☐ Heard about it at an event
- ☐ Somebody told me or shared it with me
- ☐ Other (please specify)