

Your response

Question	Your response
<p>Question 1: Do you have any comments on our proposed approach to 'content and activity' which 'disproportionately affects women and girls'?</p>	<p>Confidential? – No</p> <p>1. Although intersectionality is mentioned in the guidance, we do not believe that it has been consistently integrated across the proposed actions. According to Glitch and the End Violence against Women Coalition, women and girls from racialised communities, transwomen and women with disabilities experience different forms or intensities of harm. The harms they face are tightly intertwined with systemic discrimination, both online and offline. By not embedding this nuance at the heart of the harm framework, the guidance risks offering a one-size-fits-all solution to a complex set of intersecting oppressions. Platforms should be required to conduct subgroup-specific risk assessments and engage directly with marginalised communities and civil society groups working with marginalised groups and on intersectional identity issues so as to inform safety-by-design. Platforms should also be encouraged to collect and report data on online gender-based harms disaggregated by intersecting identities, where possible, to improve knowledge around this area and use this information to design appropriate interventions that meet the needs of those sub-groups.</p> <p>2. Discussions have already been had on how the treatment of legal-but-harmful content in the Online Safety Act fails to address the cumulative nature and impact of misogynistic, degrading, or dehumanising content, especially when algorithmically promoted, and undermines the promise of a safe online environment. The Guidance acknowledges that women and girls do not need to experience explicit threats to be harmed. The drip-feed of violent ideologies, sexist commentary, and normalised humiliation creates a digital culture where abuse becomes an ambient and ever-present background noise that shapes how women behave, engage, and self-censor online.</p> <p>However, failing to categorise these harms distinctly leads to several risks like misdiagnosis of the problem where platforms may target the symptoms while ignoring the root causes of online gender-based harms. For instance, platforms may address abusive content without dealing with their search and recommending systems and engines that surface the content. Or that algorithmically surfaced content is more likely to be externalised as user behaviour rather than internalised as</p>

Question	Your response
	<p>platform responsibility. Further, solutions like block tools or user controls treat only the individual layer of harm, leaving systemic incentives unchallenged.</p> <p>We recommend some areas for improvement:</p> <ol style="list-style-type: none"> 1. Strengthening the typology of harms in the Guidance by creating clear distinctions between individual, systemic, and indirect harms. This would also include having a dedicated section on matrix mapping examples of each type of harm and their interaction. For example, this could include mapping how the use of algorithmic amplification of misogynistic content links to misogynistic behaviours and the targeting and harming of women and girls online. 2. Requiring platforms to conduct ecosystem-level audits, particularly on moderation model bias, user onboarding, default settings, and content ranking and recommendation systems. 3. The Guidance should further encourage independent auditing of recommender systems, similar to the approaches in the EU Digital Services Act, to assess how they might reinforce gendered harm. Addressing the distinction would help ensure platforms address not just what users do but what tier systems enable, amplify, or ignore. <p>This will meaningfully reduce technology-facilitated gender-based violence in the long term, ensuring that the UK is complying with its obligations under the Equality Act and the CEDAW. It will also mean that platforms are more accountable for not just content moderation but also for how their systems contribute to online gender-based harms. This will contribute to a systemic approach to preventing and addressing online gender-based harms .</p>
<p>Question 2: Do you have any comments on the nine proposed actions? Please provide evidence to support your answer.</p>	<p>Confidential? – No</p> <ol style="list-style-type: none"> 1. This guidance treats women and girls as a uniform category. It gestures towards intersectionality, but it does not fully operationalise it. In reality, Black women, women with disabilities, and women from economically marginalised communities face distinct and compounded forms of online harm. To omit this from the core of the risk framework will replicate the exclusions this Guidance seeks to address. 2. Most solutions place the burden of safety on users, yet the user controls are challenging to use and not easily visible to users. In 2023, Internet Matters found that many users,

Question	Your response
	<p>particularly adolescent girls, found existing tools confusing and inaccessible. Blocking, filtering, and curating user experiences online is a temporary relief, but they are not a substitute for meaningful platform accountability. It is not enough to hand survivors better tools to manage violence after it has already occurred.</p> <p>Platforms should be required to prevent it by default, that is, ensure that a human-rights-based approach, equality-by-design, safety-by-design, and governance-by-design approaches are used. Platforms should set safer default settings, for example, requiring users to opt-in rather than opt-out. Tools like PhotoDNA and hash-matching tech have proven to be effective against CSAM, with the Revenge Porn Helpline 2023 Report noting a 100% increase in such reports in a single year. Initiatives like StopNCII should continue to be promoted and developed further to analyse images and text for toxicity, bias, and misogynistic language using Natural Language Processing (NLP) and deep learning. Additionally, cross-platform data sharing on abusers should be required because, as found in the Silence, Women Report (Demos, 2021), repeat violators often act across multiple platforms and evade bans through sock-puppet accounts.</p> <p>3. The reliance on ‘good practice’ rather than enforceable obligations is concerning. Without a clear pathway from recommendation to regulation, there is a risk that companies will cherry-pick the easiest interventions to maintain a good public persona while sidelining the more systemic changes that would actually reduce harm.</p> <p>4. There needs to be more frequent reporting and disaggregation, more than the 18 months provided for in the Guidance. Waiting 18 months for the first comprehensive public review is too slow given the rapid evolution and urgency of technology-facilitated gender based violence. Features, algorithms, and abuse vectors are routinely updated in response to business incentives or user trends. For example, TikTok, X (formerly Twitter), and Instagram have frequent updates to their platforms and services that can introduce new risks. There are also emerging threats like generative AI deepfakes. Additionally a long review window allows platforms to delay meaningful reform under the guise of ‘in progress’ safety measures. This risks undermining the urgency conveyed by the Guidance and can lead to harm scaling unchecked. Survivors, researchers and civil society organisations need timely and regular data to track harm trends and monitor company claims and advocate effectively.</p>

Question	Your response
	<p>OfCom's own Transparency Reporting Consultation in 2024 recognised that transparency reports must be timely, unbiased and comparative.</p> <p>We propose that Ofcom should require interim reports to be submitted every 6 months in the first 2 years following the publication of the Guidance. This could include updates on implementation of the nine actions, changes to platform policies affecting gendered safety, and new features or abuse vectors with potential impacts.</p> <p>Platforms should also be required to collect and report anonymised demographic data disaggregated by gender, race, age, disability, and other relevant characteristics, with attention to intersectional harm profiles, to show whether safety tools are protecting users equitably and effectively. This should include an analysis of differential access to, use of, and outcomes from safety tools. Where collecting such data is not possible, proxy indicators or user experience surveys should be used. Ofcom should provide a standardised disaggregation template to ensure comparability across platforms.</p> <p>Ofcom should also require platforms to adopt real-time transparency mechanisms, such as live dashboards or regularly update public metrics, particularly for high-risk content categories like image-based abuse and harassment. In addition, reporting cycles should include stakeholder engagement structures, such as public hearings or expert roundtables, to ensure that survivor experiences and civil society input actively inform the evaluation of platform safety.</p>
<p>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.</p>	<p>Confidential? – No</p> <p>Ofcom's 'good practice' steps offer a welcome shift toward embedding safety-by-design principles into platform governance, product design, and user support. The emphasis on risk assessments, survivor-informed governance, and trauma-aware reporting reflects a growing recognition that online gender-based violence is systemic, not incidental. However, these practices must be implemented with platform accountability to be genuinely effective. Risk assessments, for example, must be intersectional, transparent, and independently reviewed, rather than vague internal exercises. Similarly, survivor engagement should be formalised and resourced, not tokenistic.</p>

Question	Your response
	<p>The proposed usability testing and safer defaults seem promising, but should go further. Platforms should not only test features for potential misuse but also be willing to redesign or remove those that consistently enable harm. Default protections should also be dynamic, responding to real-time indicators like sudden spikes in harassment. Reporting tools must allow for cumulative, context-aware reports, particularly in cases of coercive control or stalking, paired with anonymised support channels to reduce barriers for victims.</p> <p>While the case studies and recommendations are helpful, their discretionary nature poses a serious risk. Without enforceability, platforms may adopt surface-level changes without addressing deeper structural issues. Ofcom should consider making the most effective good practices binding in future Codes and supporting industry-wide tools, like shared hash databases or predictive moderation, that address coordinated abuse across platforms, in a human rights respecting manner. Safety cannot be left to platform goodwill; it must be a regulatory priority grounded in the lived experiences of those most at risk.</p>
<p>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?</p>	<p>Confidential? – No</p> <p>Ofcom's proposal to publish an assessment of how providers address women and girls' safety is a strong accountability measure, particularly if it includes service-specific evaluations. Public transparency can pressure platforms to improve, especially regarding user trust and brand reputation. However, this assessment needs to be regular, data-driven, and disaggregated by service type, size, and harm area to be effective.</p> <p>Notwithstanding, transparency alone may not drive meaningful change across the board, particularly for smaller or less visible providers. Ofcom should consider introducing an accreditation scheme for providers that adopt and implement the most impactful good practices. This could offer a reputational incentive while helping users identify safer platforms.</p> <p>Lastly, Ofcom could establish an independent advisory panel of experts, including survivors and civil society, to monitor implementation and advise on future iterations of the Guidance. Making the implementation process more participatory would strengthen legitimacy and ensure providers remain responsive to real-world harms.</p>

Question	Your response
<p>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.</p>	<p>Confidential? – No</p> <p>Ofcom’s inclusion of an equality and rights-based impact assessment is essential in acknowledging this Guidance's broader legal and social implications. However, the assessments would benefit from deeper analysis of how intersecting forms of discrimination, such as racism, ableism, homophobia, and transphobia, shape the experience of online harm for different groups of women and girls. Without this, the assessments risk overlooking how structural inequality magnifies vulnerability to digital abuse.</p> <p>The rights assessment appropriately considers freedom of expression and the right to privacy. Notwithstanding, more could be done to balance these rights with the right to safety and participation in public life, particularly for women who are often silenced and forced offline by abuse. International human rights standards, including those articulated in CEDAW (General Recommendation 35) and the Istanbul Convention (Article 17), support proactive regulation where online environments restrict the ability of women and girls to speak freely without fear. Ofcom should articulate more clearly how this Guidance upholds these protections.</p> <p>Finally, a more detailed analysis of potential unintended consequences would strengthen the impact assessment. For example, while automated moderation tools aim to reduce harm, they may inadvertently silence marginalised voices if not trained on sufficiently diverse data. Ofcom should encourage regular auditing of safety tools and recommend safeguards to ensure interventions do not inadvertently reinforce the inequalities they seek to address.</p>
<p>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</p>	<p>Confidential? – No</p> <p>The Guidance has the potential to positively support the principle of treating Welsh no less favourably than English, particularly through its stated commitment to bilingual publication and inclusive consultation processes. Ensuring that all official guidance, summaries, and consultation materials are available in Welsh and English is a necessary baseline for compliance and inclusion.</p> <p>However, to fully realise this commitment, Ofcom should consider going beyond translation to ensure that Welsh-speaking users can meaningfully engage with and benefit from the safety</p>

Question	Your response
effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.	<p>features recommended. This includes encouraging platforms to provide safety tools, reporting mechanisms, and automated moderation in Welsh and ensuring that risk assessments consider language-based accessibility and safety barriers for Welsh speakers.</p> <p>To strengthen the positive impact, Ofcom could also work with Welsh-language civil society organisations and digital rights advocates to ensure that the implementation of the Guidance reflects the lived experiences of Welsh-speaking communities. In doing so, Ofcom would meet its legal obligations and reinforce the value of linguistic equity in digital safety policy.</p>

Please complete this form in full and return to OS-Section54@ofcom.org.uk.