WARNING: This consultation response contains language and/or material that may be distressing

Your response

Question	Your response
Question 1: Do you have any comments on our proposed approach to 'content and activity' which 'disproportionately affects women and girls'?	Confidential? – N The four priority areas that are the cornerstone of the proposed guidance seem to capture the behaviours that align most closely with the research and experiences of women and girls in online environments. They are broadly reflective of the most prevalent and / or most harmful content for women and girls. The acknowledgment of the specific forms of violence and online harms that affect women and girls in particular is overwhelmingly welcome, especially given the omission of illegal content duties in respect of online gender based harms within the Online Safety Act (OSA) 2023. That said, I have some doubts as to the choice of "online gender-based harms" as the phrasing of choice. While that *is* reflective of the types of content and / or activity that the guidance is ostensibly designed to address – at least in part – it is something quite distinct to the wider, and more legally grounded recognition given to rights-based approaches under human rights instruments. The preferred proposed terminology—"online gender-based harms"—may benefit from refinement. While the phrase captures the types of conduct the guidance targets, it lacks the definitional clarity and normative anchoring found under legal frameworks such as the Council of Europe's Istanbul Convention and the UN Convention on the Elimination of All Forms of Discrimination against Women (CEDAW)**.** The term "technology-facilitated gender-based violence" (TFGBV) is used to describe abuse that is both gendered in motive and digital in form (Council of Europe, 2021; UN CEDAW Committee, 2017; Barker 2024). GREVIO, the Istanbul Convention's monitoring body, has repeatedly emphasised that technology-enabled violence falls within states' obligations to prevent, investigate, and sanction violence against women. Such an alternative form of phrasing could be reflective of a human rights based approach while capturing the content and activity as proposed. The proposed categorisation of harmful content and behaviours recognises both the individual-level impact on victims and the broader structural consequences of

Question	Your response
	online abuse targeting women and girls. When such abuse leads to the silencing or withdrawal of female voices from online spaces, it effectively undermines women's ability to participate fully in public discourse, democratic processes, and economic life. This dynamic has increasingly been acknowledged in international human rights frameworks, which highlight online gender-based abuse as a barrier to gender equality and the realisation of women's rights. The Council of Europe's Istanbul Convention (2011) — ratified by the UK — explicitly frames violence against women, including forms such as psychological abuse and harassment, as both a human rights violation and a manifestation of structural discrimination. Although it predates the ubiquity of digital platforms, its scope clearly extends to technology-facilitated violence. The Convention's monitoring body, GREVIO, has reinforced this interpretation, asserting that member states are required to address technology-facilitated abuse as part of their obligations under the treaty. Likewise, the UN Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) has reiterated through its General Recommendations (especially Recommendation No 1) that gender-based violence, including in its digital manifestations, constitutes a form of discrimination. States parties are thus under a clear duty to adopt legislative, policy, and regulatory measures to prevent and redress such harms. It is particularly important that Ofcom has been receptive to this, and these forms of digital manifestations are captured – in at least some form – in the proposed guidance. It is therefore a positive development to see specific forms of content *and* activity captured in the guidance to providers. Ofcom uses "content and activity" to indicate that the guidance covers not just harmful content but also behaviour patterns and platform features usage that can encourage, create, or cause harm. This is crucial because many online abuses of women involve persistent conduct, such as relentless monitoring or coordinated harassment, rather than isolated incidents. By including activity, Ofcom seeks to address these complex harms. The guidance defines relevant content and activity broadly: any online behaviours that "threaten, silence, abuse, monitor, coerce, or otherwise harm" women and girls, impacting their ability to express themselves freely.

Question	Your response
	It includes both direct abuse (like threats or degrading comments) and indirect harms (such as spyware or impersonation). It spans illegal harms (e.g., credible threats, non-consensual pornography, stalking) and legal-but-harmful actions (e.g., misogynistic hate, cyberflashing). This broad scope acknowledges that women's online safety is threatened by a range of behaviours, beyond what existing law covers. That said, some of these behaviours are not behaviours that are specifically illegal or even recognised as legally harmful in legal jurisprudence or judicial consideration. This is particularly significant to note here – both in terms of the expectations being placed on providers, but also in terms of the need for monitoring of the effectiveness and implementation of the guidance. It is also important to note the gap between the legal categories of behaviours, and the guidance categories – something of substantive importance in the face of future potential OSA amendments. The guidance adopts a deliberately wide-ranging interpretation of harmful online content and behaviours, encompassing any actions that intimidate, suppress, harass, surveil, control, or otherwise negatively impact women and girls, including those that inhibit their freedom of expression (Ofcom, 2025). This inclusive framing captures both overt forms of abuse—such as explicit threats or degrading language—and more covert forms of harm, such as digital surveillance, impersonation, or manipulation via technological tools. This is a substantive and positive symbolic development even if the guidance itself does not have legal force. Importantly, the definition spans both criminal conduct (e.g. stalking, threats of violence, distribution of non-consensual sexual material) and legally permissible yet harmful behaviour, such as pervasive misogynistic commentary or cyberflashing—some of which have only recently begun to be regulated. By recognising this continuum of harm, the guidance reflects the complex and evolving nature of online abuse, acknowledging that the law does not yet fully encompass the wide range of risks women and girls encounter in digital spaces. Considering the four harm categories outlined, Ofcom's conceptual framework appears to encompass the major forms of digital abuse experienced by women and girls. While additional online threats exist—such as gendered disinformation campaigns, which aim to undermine

Question	Your response
	women's credibility through the dissemination of misogynistic or false narratives, or context-specific abuse, like that seen in gaming platforms—these examples largely fall within the broader categories already identified. For instance, targeted disinformation, or online posts with sexist undertones can be understood as a distinct form of online misogyny (Barker and Jurasz, 2019) and harassment, while abuse directed at women in gaming environments constitutes harassment within a specific digital context. The proposed categories are expansive enough to capture a spectrum of content and activity. A notable strength of the guidance is its conceptual flexibility. Rather than relying on a closed list of behaviours or contexts, Ofcom focuses on the effects of harmful conduct, such as silencing, intimidation, or coercion. This outcome-based framing provides adaptability as new digital spaces and technologies evolve. For instance, should new forms of abuse arise—such as gender-targeted harm within immersive virtual or augmented reality platforms—they would still likely fall within the scope of the guidance, provided they exhibit the harmful characteristics already described. It will be important for this conceptual flexibility to be maintained so that the guidance is technology neutral **and** gender sensitive. It is notable also, that the proposed categories is reflective of *both* content *and* conduct – so as to capture the so-called "lived reality" of online abuse, and gendered online harms affecting women and girls. That said, there are some questions that remain over the proposed approach and categories here. Specifically, there are some inevitable overlaps / interplays between the Illegal Content Register and the behaviours ostensibly captured within the categories proposed. Similarly, while there is overlap for some groups of users e.g., young girls (and therefore children), the proposed categories and approach here groups together *all* women and girls, and does not seem to differentiate between these different age groups. While the content and activity differential split is useful, there also needs to be some further thought given to the different experiences of young girls, teenagers, and older women. The experiences of online content are different for each of these sub-groups within this. The approach would do well to be cognisant and reflective of this – and this includes the approach through the four categories of prevalent harms. To be clear, the experiences of different groups of women and girls to

Question	Your response
	each of these forms of harmful content will be *very* different and distinct. The four priority categories outlined in Ofcom's draft guidance provide a strong foundation for addressing the forms of harm that most acutely impact women and girls in digital spaces. These categories are aligned with research on the gendered dynamics of online abuse, which show that women—especially those with intersecting identities such as race, disability, or LGBTQ+ status—experience disproportionately high levels of harassment, surveillance, and reputational harm (Amnesty International, 2018; Glitch, 2022). The guidance rightly includes both the most prevalent harms (such as sexualised trolling or doxxing) and the most impactful, such as technology-facilitated coercion and cumulative harassment. Ofcom's decision to explicitly recognise the differentiated impacts on women and girls marks a significant shift away from previous gender-neutral regulatory approaches that often obscured the structural dimensions of online harm (Dragiewicz et al., 2021; Henry & Powell, 2018). Furthermore, the guidance's emphasis on both **"**content" and "activity" is particularly appropriate and legally significant. Online harms rarely occur through a single message or piece of content; instead, they are often sustained, patterned behaviours—such as persistent harassment, coordinated pile-ons, or long-term surveillance—that inflict psychological, reputational, and civic harm (Citron, 2014; Stark, 2007). By encompassing "activity," Ofcom's guidance captures a broader spectrum of abuse, including behaviours not easily addressed through content moderation alone. For victims, bystanders, targets this is a pragmatic step. Ofcom's proposed definition—covering actions that "threaten, silence, abuse, monitor, coerce, or otherwise harm"—reflects a recognition of the continuum of harm**,** spanning both clearly criminal conduct (e.g., image-based sexual abuse, credible threats) and legal-but-harmful behaviours such as misogynistic speech, impersonation, and exposure to non-consensual sexual content. Recent scholarship and regulatory commentary highlight that while some of these harms may not meet criminal thresholds, they still result in exclusionary and chilling effects on women's speech and participation online. Importantly, while UK criminal law is gradually expanding to include offences like cyberflashing (see the Online Safety Act 2023), the law remains under-inclusive. A rights-based regulatory approach that accounts for non-

Question	Your response
	criminal but harmful conduct is therefore essential. Ofcom's broad framing allows for such flexibility and aligns with international best practice in digital rights regulation (UN OHCHR, 2021). In sum, the proposed approach to content and activity is to be welcomed, subject to the caveats and concerns noted above. • Amnesty International. (2018). *Toxic Twitter: A toxic place for women*. https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women/ • Barker, K. (2024). Emerging Practices in The Investigation and Prosecution of Digital Violence Against Women *Council of Europe* (2024). • Barker, K., & Jurasz, O. (2019). *Online Misogyny: A Challenge for Legal Regulation. Routledge.* • Citron, D. K. (2014). *Hate crimes in cyberspace*. Harvard University Press. • Council of Europe. (2011). *Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence* (Istanbul Convention). https://www.coe.int/en/web/istanbul-convention • Council of Europe. (2021). *GREVIO General Recommendation No. 1 on the digital dimension of violence against women*. https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a491e6 • Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N., Woodlock, D., & Harris, B. (2021). Technology-facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*, 21(2), 310–328. https://doi.org/10.1080/14680777.2020.1864019 • Glitch. (2022). *The Ripple Effect: COVID-19 and the online abuse of Black women and non-binary people*. https://glitchcharity.co.uk/our-work/covid19-ripple-effect • Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence, & Abuse*, 19(2), 195–208. https://doi.org/10.1177/1524838016650189

Question	Your response
	• Ofcom. (2025). *A Safer Life Online for Women and Girls: Practical Guidance for Tech Companies (Annex A)*. • Stark, E. (2007). *Coercive control: How men entrap women in personal life*. Oxford University Press. • UN CEDAW Committee. (2017). *General Recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19*. https://www.ohchr.org/en/treaty-bodies/cedaw/general-recommendations • UN OHCHR. (2021). *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf
Question 2: Do you have any comments on the nine proposed actions? Please provide evidence to support your answer.	Confidential? – N The nine proposed actions in Ofcom's draft guidance represent a forward-thinking and balanced framework to reduce online harm disproportionately affecting women and girls. By organising the actions into three pillars—Taking Responsibility, Preventing Harm, and Supporting Users—the framework recognises that technological design, governance culture, and user experience all interact in the production and mitigation of gendered digital violence. Collectively, the actions provide a practicable roadmap to implement the safety-by-design ethos embedded within the Online Safety Act 2023, while extending its protective scope through non-binding but robust best practices. Governance, Accountability, and Risk Assessments (Actions 1 and 2) are especially critical. Research has shown that without institutional leadership on gendered harms, safety is often treated as a reactive concern rather than an embedded value (Henry & Powell, 2018). Requiring services to explicitly consider women and girls in governance structures and risk assessments—rather than assuming gender-neutral impact—advances the statutory purpose under Section 149 of the Communications Act 2003 to promote equality in regulation. Evidence from the corporate sector indicates that internal accountability

Question	Your response
	mechanisms, including safety officers and audit frameworks, are vital to systemic change (UK Centre for Data Ethics, 2023). Such change is essential for the guidance to be effectively implemented. Transparency (Action 3) is essential not only for regulatory oversight but also to empower civil society and users to hold companies accountable. Transparency reporting has already shown its value in areas such as hate speech moderation (European Commission, 2022). Ofcom's emphasis on transparency aligns with both the UN Guiding Principles on Business and Human Rights and Article 10 of the European Convention on Human Rights, ensuring that any moderation actions are subject to scrutiny and appeal. The 'Preventing Harm' cluster—Actions 4 through 6—are grounded in a credible safety-by-design approach. In particular, abusability testing (Action 4) draws on emerging best practice in responsible product development, as advocated by regulators like the UK's Digital Regulation Cooperation Forum and Australia's eSafety Commissioner. Studies on intimate partner violence have highlighted how digital tools—originally designed with neutral or benign purposes—can be weaponised for coercive control, especially via default settings that expose user data (Dragiewicz et al., 2021). Ofcom's recommendation for privacy-protective defaults and content circulation controls responds directly to these concerns and is grounded in empirical evidence of risk. Similar interventions (e.g. TikTok's default private account settings for minors, Apple's AirDrop update to prevent unsolicited images) have demonstrated efficacy and user acceptance. Again, this is a progressive development within the wider regulatory ecosystem. The final group of actions—Supporting Women and Girls (Actions 7–9)—is equally well-founded. Enhanced user control tools such as mass-block features or 'safe mode' configurations directly reflect requests from abuse survivors and frontline organisations (Glitch, 2022). These measures not only improve user autonomy but also limit exposure to secondary victimisation. The inclusion of trauma-informed reporting processes and effective moderation staffing (Action 9) is supported by work from the Ada Lovelace Institute and Amnesty International, both

Question	Your response
	of which have highlighted the inadequacy of current reporting mechanisms, particularly for racialised and marginalised women. In sum, the nine actions are coherent, evidence-informed, and feasible. Ofcom's framing is sufficiently flexible to allow differentiated implementation by service size and type, while setting high normative expectations for proactive design, governance, and support. We strongly endorse their adoption in the final guidance and recommend that Ofcom supplement them with clear implementation indicators and timelines to support consistency and accountability across the sector.
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.	Confidential? – N Chapters 3 to 5 of Ofcom's draft guidance present a comprehensive and flexible framework aimed at improving online safety for women and girls. The recommendations are designed to be scalable and proportionate, allowing services to implement safety measures based on their size, risk profile, and functionality. The guidance avoids a one-size-fits-all approach and instead encourages targeted interventions and a diverse toolkit, aligned with broader regulatory standards and legal obligations. Importantly, the framework is attentive to human rights considerations, especially freedom of expression, privacy, and due process. Rather than calling for blanket censorship, it seems to promote procedural safeguards such as transparency in content moderation, clear appeals mechanisms, and user empowerment features. These align with the UK's statutory duties, including under Section 149 of the Communications Act 2003, which requires Ofcom to have regard to the principles of transparency, accountability, proportionality, and consistency in regulation. Further, the guidance resonates with the UN Guiding Principles on Business and Human Rights, which call on both states and companies to identify, prevent, and address adverse human rights impacts linked to their operations, including those related to digital platforms (OHCHR, UN Guiding Principles). Ofcom may wish to explicitly reference these frameworks in the finalised guidance to reinforce the normative grounding of its recommendations.

Question	Your response
	The regulatory model also reflects a balance between voluntary uptake and statutory enforcement. On the incentive side, the guidance anticipates that transparency reporting and reputational dynamics will encourage services to adopt best practices. At the same time, Ofcom retains significant enforcement powers under the Online Safety Act 2023, including the ability to impose substantial fines or service access restrictions if platforms breach their obligations regarding illegal content or child safety (Online Safety Act 2023, s.122-130). If the voluntary uptake of the guidance's non-binding measures—such as trauma-informed reporting processes, automated tools to reduce the circulation of abusive material, and proactive safety-by-design features—proves insufficient, there is likely to be growing political and public pressure to legislate further. This was evidenced during the development of the Online Safety Act itself, where provisions were strengthened in response to public concern about harms facing women and girls. It is nevertheless pertinent that this aspect is captured here, especially if the proposed guidance is the beginning of tangible and responsible responses outside of purely legislative frameworks to address the pernicious impacts of online forms of violence against women and girls. This is likely to be particularly important should further legal reform be forthcoming. Moreover, the guidance is well supported by real-world case studies demonstrating the achievability of the proposed measures. For instance, social media platforms like Instagram and TikTok have piloted AI-driven content moderation tools and user safety nudges, while gaming companies have implemented customisable blocking and muting features in response to gender-based harassment (Ofcom Draft Guidance, Annex A, 2025). The presence of these working models undercuts arguments that the good practice steps are impractical or speculative. Adopting a proactive safety-by-design mindset is also strategically beneficial for industry. Preventative features reduce the long-term costs of reactive content moderation and enhance user engagement, particularly among demographics historically underserved or unsafe in digital spaces. Platforms that foster inclusive environments—where women and girls can participate without fear of

Question	Your response
	abuse—are more likely to attract sustained interaction and community building. The proposals seem – at least conceptually – to strike a balance and establish benchmarks for tangible, testable mechanisms to address online violence against women and girls. **References:** • Amnesty International. (2018). *Toxic Twitter: Women's experiences of abuse on Twitter*. https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-3-2/. • Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N., Woodlock, D., & Harris, B. (2021). Technology-facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*, 21(2), 310–328. • European Commission. (2022). *Code of conduct on countering illegal hate speech online – evaluation 2022*. • Glitch. (2022). *The Ripple Effect: Covid-19 and the online abuse of Black women and non-binary people*. https://glitchcharity.co.uk/our-work/covid19-ripple-effect. • Henry, N., & Powell, A. (2018). *Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research*. *Trauma, Violence, & Abuse*, 19(2), 195–208. • Ofcom. (2025). *Draft Guidance: A Safer Life Online for Women and Girls*. • UK Centre for Data Ethics and Innovation. (2023). *Responsible Innovation in Online Services*. https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation • UN OHCHR. (2011). *Guiding Principles on Business and Human Rights*. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

Question	Your response
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?	Confidential? – N Ofcom's proposed strategy to promote adoption of its guidance on content and activity disproportionately affecting women and girls is well-calibrated in principle, but could benefit from additional incentivisation mechanisms, regulatory clarity, and sectoral collaboration. The dual emphasis on transparency and reputational accountability—through publication of provider-level assessments—represents an effective, rights-respecting tool for promoting uptake without imposing legal compulsion. However, greater detail is needed regarding the indicators, metrics, and frequency of these assessments to ensure consistency, comparability, and impact. Similarly, what will substantive encouragement (and / or remedial0 action look like? Encouragement is only one aspect of tangible change – alongside encouragement there needs to be some form of remedial element so as to ensure widespread uptake. As it stands, the lack of mandated requirements seems to be a substantive blocking mechanism to the uptake of best practices. The logic of "regulation through transparency" is now well-established in areas such as environmental and financial disclosure (Black, Hopper, & Band, 2007), and is increasingly applied to digital governance. Publicising how individual services respond to gender-based online harms can exert reputational pressure and encourage competition on safety outcomes. The success of the European Commission's Code of Conduct on Hate Speech (European Commission, 2022) and Australia's eSafety transparency reporting scheme (eSafety Commissioner, 2023) demonstrates that soft regulatory tools—when well-structured—can significantly influence corporate behaviour. These approaches are particularly effective when paired with clear benchmarking, public league tables, or annual scorecards. Ofcom could adopt a similar model through an Online Safety Index, evaluating platforms on abuse response rates, safety tool availability, and design accountability. To maximise uptake, Ofcom should also consider positive incentives beyond reputational pressure. One promising approach is a voluntary certification scheme, analogous to "Trustmark" models used in digital privacy (e.g., the Age Appropriate Design Code). Services meeting Ofcom's

Question	Your response
	thresholds for good practice—such as trauma-informed reporting, mass-blocking tools, or proactive harm detection—could receive a public-facing badge or endorsement. Such schemes have been shown to influence consumer behaviour and encourage competitive safety differentiation (ICO, 2021). In addition, Ofcom should consider establishing a cross-sector co-regulatory forum, bringing together platforms, civil society groups, academics, and survivors' organisations. This would promote collaborative standard-setting and knowledge-sharing, akin to initiatives such as the Global Internet Forum to Counter Terrorism (GIFCT). Lessons from that model show that shared protocols and tooling can enhance response to distributed harms, while reducing resource duplication (GIFCT, 2021). A further avenue is for public sector institutions—particularly in education, youth services, and civic engagement—to integrate adherence to Ofcom's safety guidance into procurement policies. Providers that can evidence compliance with good practice could be favoured in contract awards, effectively incentivising uptake via market mechanisms aligned with public interest. Finally, Ofcom's proposed assessments must incorporate intersectional dimensions. Research shows that racialised women, disabled women, LGBTQ+ users, and young women often experience heightened levels of digital abuse (Glitch, 2022; Amnesty International, 2018). Evaluating platform safety through a disaggregated lens—supported by engagement with equality bodies and researchers—will ensure that good practices are not only adopted, but meaningfully effective for all user groups. In summary, Ofcom's encouragement strategy is a promising base. Its impact will be enhanced by: (1) transparent benchmarking; (2) incentives through certification and procurement; and (3) inclusive co-regulatory structures. It is a promising start but much future work will be required for the best practice proposals to take effect across a sufficient proportion of providers. The best practice proposals must remain flexible and cannot be static.

Question	Your response
	References • Amnesty International. (2018). *Toxic Twitter: A toxic place for women*. https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/ • Black, J., Hopper, M., & Band, C. (2007). *Making a success of principles-based regulation*. Law and Financial Markets Review, 1(3), 191–206. • eSafety Commissioner. (2023). *Transparency report 2022–23*. • European Commission. (2022). *Code of Conduct on countering illegal hate speech online – Results of the 2022 evaluation*. • Glitch. (2022). *The Ripple Effect: COVID-19 and the online abuse of Black women and non-binary people*. https://glitchcharity.co.uk/our-work/covid19-ripple-effect. • Global Internet Forum to Counter Terrorism (GIFCT). (2021). *Annual Transparency Report 2021*. https://gifct.org/transparency/ • Information Commissioner's Office (ICO). (2021). *Age appropriate design code: A code of practice for online services*.
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.	Confidential? – N Ofcom's supporting impact assessments for its draft guidance on online harm to women and girls represent a thoughtful and generally well-grounded approach. The assessments acknowledge that tackling technology-facilitated gender-based violence (TFGBV) raises significant questions about freedom of expression, equality of access, and non-discrimination, particularly in the context of diverse user experiences. However, there is scope to strengthen both the legal reasoning and empirical foundations underpinning these assessments, particularly by drawing more explicitly on international human rights jurisprudence and intersectional data. The Rights Impact Assessment (RIA) is consistent with Ofcom's statutory duties under the Human Rights Act 1998 and Articles 8 and 10 of the European Convention on Human Rights (ECHR). It correctly identifies that freedom of expression is a qualified right that must be balanced against the rights of others, including the rights to

Question	Your response
	dignity, privacy, and freedom from discrimination. This reflects established principles in ECHR case law, such as in *Delfi AS v. Estonia* (2015), where the European Court of Human Rights confirmed that online platforms may bear responsibility for preventing serious harm caused by third-party speech, particularly when victims belong to protected groups. That said, the RIA could be enhanced by more explicitly referencing the growing body of international jurisprudence framing online abuse of women as a structural rights violation. The CEDAW Committee's General Recommendation No. 35 on gender-based violence and the Council of Europe's Istanbul Convention both affirm that digital forms of violence, including harassment and surveillance, fall within the scope of human rights violations. GREVIO, the Istanbul Convention's monitoring body, has also emphasised that state parties must adopt regulatory frameworks addressing technology-enabled abuse (Council of Europe, 2021). Incorporating these references would strengthen the legal coherence of the assessment and reinforce Ofcom's normative position. The Equality Impact Assessment (EqIA) is also commendable in identifying that women and girls face disproportionately high levels of online harm. Research provides compelling evidence that intersectional identities—including race, sexuality, disability, and trans status—significantly shape digital safety outcomes. Yet while the EqIA acknowledges differential impact, it stops short of identifying specific mitigations for these intersectional groups. Ofcom should consider disaggregating its impact analysis further, for example by evaluating how the proposed guidance supports women with intersecting protected characteristics under the Equality Act 2010 (e.g., Black women, disabled women, LGBTQ+ youth), who often experience compounded and unique forms of harm online (Amnesty International, 2020). The Impact Assessment (IA) itself appropriately anticipates that implementation costs may vary by provider size and function. However, it could benefit from a more robust evidence base regarding cost-benefit estimates. For example, safety-by-design interventions have been shown to reduce long-term moderation and reputational costs, particularly in high-risk content areas (CDEI, 2023). Ofcom might draw on comparative models, such as Australia's eSafety regime, where proactive design and transparent complaint systems have reduced abuse-related platform burdens over time.

Question	Your response
	Overall, the assessments reflect a serious engagement with regulatory obligations but would benefit from stronger articulation of intersectionality, international law, and long-term social and economic benefits. I encourage Ofcom to refine the RIA and EqIA with greater specificity, supported by disaggregated data and cross-jurisdictional insights. **References** • Amnesty International. (2020). *Toxic Twitter: Women's experiences of abuse on Twitter*. https://www.amnesty.org • Centre for Data Ethics and Innovation (CDEI). (2023). *Responsible innovation in online safety: A cost-benefit perspective*. https://www.gov.uk • Council of Europe. (2021). *GREVIO General Recommendation No. 1 on the digital dimension of violence against women*. https://www.coe.int • Delfi AS v. Estonia, no. 64569/09, ECHR 2015. • Glitch. (2022). *The Ripple Effect: COVID-19 and online abuse of Black women and non-binary people*. https://fixtheglitch.org • UN CEDAW Committee. (2017). *General Recommendation No. 35 on gender-based violence against women*. https://www.ohchr.org
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.	Not answered.

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