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

Consultation response form

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? – Y / **N** **Key themes** Refuge welcomes Ofcom's VAWG guidance and the inclusion of online domestic abuse as a key harm. However, we believe it should be strengthened by the addition of stalking as a fifth harm, the inclusion of measures on co-operating with law enforcement agencies and survivors who want to pursue criminal cases, and by going further on safety by design and perpetrator disruption measures. However, the guidance will only have impact if tech companies follow it and Refuge remains of the view that the guidance must be upgraded to a Code of Practice to have impact. The need to tackle online VAWG could not be more pressing. Refuge's *Unsocial Spaces* report (2021) found that 1 in 3 UK women have experienced online abuse, and 1 in 6 of these were abused by a partner or ex-partner, equivalent to at least 2 million women a year. [1] As the UK's largest domestic abuse service provider, Refuge's experience of supporting tech abuse survivors shows the urgency of regulation. Between 2018–2022, demand for our tech abuse team rose by 258%. [2] The most common harms reported to the team in 2024 were online stalking and compromised devices—issues that require targeted and enforceable responses from tech providers. In order to respond to this consultation, we have held several workshops on the draft guidance with both our specialist technology-facilitated abuse team and our Survivor Panel. Our response is based on their contributions as we as the organisation's expertise and experience in supporting survivors of domestic abuse.

Question	Your response
	We have provided highly detailed response to the guidance against questions 2 and 3 – which assesses and makes recommendations against all the 9 proposed actions and relevant good practice measures. Due to the level of detail, this has been submitted in alongside this consultation form and is titled 'Refuge Ofcom VAWG guidance Q2and3 Actions and Case Studies' This table forms the bulk of our response and should be read in conjunction with this submission. **Refuge would like to highlight the following strengths of the guidance:** • **Recognition of coercive and controlling behaviour -** inclusion in the Act as a priority offence is a vital foundation for this guidance • **Use of the term 'misogyny' -** we welcome the use of this language and the recognition of the structural nature of online VAWG • **A strong focus on safety by design –** looking to prevent online VAWG rather than just respond **Key concerns and recommendations** **1. Lack of enforceability** **Concern:** Voluntary guidance will not sufficiently protect women and girls. Refuge remains of the view that a legally enforceable Code is developed in order to deliver the change needed. While we recognise this is not wholly within Ofcom's power, there are steps the regulator can take to develop the guidance as a blueprint for a future Code of Practice **Refuge recommends:** • That Ofcom commit to working with the Department for Science, Innovation and Technology on upgrading the guidance to a legally enforceable Code of Practice • Ofcom clearly sets out within the guidance what steps tech companies must take on VAWG to be compliant with Children's and Illegal Harms Codes. The draft guidance is too vague on what companies must do and requires too much cross referencing with the Codes of Practice

Question	Your response
	• Robustly enforce the VAWG measures in the Children's and Illegal Harms Codes of Practice, using monitoring activity and engagement with tech companies to both hold them to account for the measures they must adopt as well as promoting the best practice elements of the guidance at every stage ○ *For more specific measures, please see points 5.25(a), 5.25(i) in the accompanying table* **2. Include online stalking explicitly as a fifth harm** **Concern:** Online stalking, a key form of online VAWG and often part of domestic abuse, is not currently named as a distinct harm. This is despite stalking being a priority offence in the Online Safety Act. It is vital that the VAWG guidance clearly sets out the action tech companies are required to take on stalking under the Illegal Harms Code as well as set out further best practice measures on stalking **Refuge recommends:** • Add stalking as a standalone harm alongside the existing four harms. • Increasing focus in the guidance on how tech companies can disrupt perpetrators' abuse, including measures on stalking and creation of multiple accounts. ○ *See points 3.19 (z), 4.42, 4.33, 5.15(b), 5.25(d), 5.25(e), 5.25(i) in the accompanying table for further detail* **3. Set out how tech companies should co-operate with law enforcement agencies and survivors in providing evidence of online VAWG** **Concern:** Survivors and criminal justice agencies currently struggle to obtain platform data to support criminal investigations and prosecutions. Tech companies hold vital data which can evidence abuse perpetrated on their platforms and should provide it to survivors and criminal justice agencies fully and promptly.

Question	Your response
	Refuge recommends: • The guidance sets out that tech companies should set out clear processes for survivors to request and be provided with data on the abuse they have been subject to on a platform. This should be provided promptly with appropriate safeguards • The guidance sets out that tech companies should promptly co-operate with requests for information from law enforcement agencies and create clear processes for this data to be requested and provided **2. Make full use of Ofcom powers to categorise services** **Concern:** Platform categorisation currently depends too heavily on size or reach and does not reflect actual harm potential or emerging threats. Smaller platforms (e.g., deepfake sites) are commonly used to abuse survivors of VAWG and can cause enormous harm. **Refuge recommends:** • **Ofcom revisits its categorisation decisions to better incorporate** not just size but also the level of risk and harm, which the Online Safety Act (2023) gives them the power to do. **4. Centre perpetrator accountability** **Concern:** The guidance has a weak focus on stopping perpetrators and making them accountable for their actions and favours a focus on survivor action to keep themselves safe. Throughout the guidance passive and vague language is often used which masks the action and responsibility of the perpetrator. For example, the guidance often notes the 'experience of online abuse' as opposed to 'are subject to online abuse or targeted by abusers' **Refuge recommends:** • Throughout the guidance, use **assertive, survivor-centred language**, which reflects that individuals (and mostly men) are making a choice to abuse women

Question	Your response
	○ *For more specific measures, please see points Action1:1.12, 5.20(b), 5.20(f), 5.25(a), 5.25(g) in the accompanying table* *"It is really frustrating that it boils down the person who is being abused to take action or change. It has always been down to me. The focus should be on the perpetrator. There should be concrete consequences to their abusive actions, particularly their freedom to use tech."Refuge Survivor Panel Member* • Set **clear expectations** that tech companies should hold perpetrators, especially **repeat offenders**, to account and ensure that there are consequences for abusive behaviour on their platforms ○ *For more specific measures, please see points 5.25(a), 5.25(d) in the accompanying table* • Encourage tech companies to **proactively take down VAWG content** and to provide hybrid (automated and human combination) content moderation ○ *See Action 6 in the accompanying table* *"You need to make it as burden-light as possible for the survivor by taking reports of abuse from survivors seriously and responding quickly. When we do report, we want to be regularly updated with progress, understand who has seen the report and what the next steps are. We need human moderators and contacts." Refuge Survivor Panel member* **5. Strengthen corporate responsibility measures** **Concern:** If the guidance is to have impact, it is vital that preventing and responding to online VAWG is thoroughly embedded in companies' leadership and governance. The guidance could go further to set ambitious standards in embedding survivor safety at the highest levels in tech companies. **Refuge recommends:** • Ofcom recommends that tech companies set, monitor and report against VAWG Key Performance Indicators. These could include abusability testing for all existing and new products,

Question	Your response
	timeframes for responding to reports of online VAWG, accounts suspended following reports of online VAWG • Ofcom produce recommended governance metrics for tech companies to monitor and develop their approach to online VAWG ○ *See Action 1 in accompanying table for further detail* • State clearly in the guidance that successful strategies to tackle online VAWG need to be led from the highest levels in tech companies, be present in every aspect of the business and incorporated in corporate strategy and review cycles. ○ *See for example: 3.19(e) on HR and DP policies in the accompanying table for more detail* *"I question about how seriously Boards and Senior Management are taking the violence on their platforms. How much is being invested to ensure their platforms are **safe spaces.** My advice to tech company Boards and Senior Management is to be curious and well-informed about what is working for survivors' online safety." Refuge Survivor Panel Member* **6. Ensure competing rights are understood and balanced** **Concern:** The impact of online abuse on the freedom of speech of women and girls must be set out in the guidance. Online abuse acts to silence women and girls, impacting their freedom of expression and ability to participate in public conversation and debate **Refuge recommends:** • The guidance clearly sets out that freedom of expression does not justify violence or abuse and reassert that enabling safe participation online is a crucial part of upholding the right to free expression for women and girls. ○ *For further detail see Action 6, 5.15(f), 5.25(e), 5.25(g) in the accompanying table* **7. Embed independent VAWG expertise**

Question	Your response
	Concern: Despite the knowledge and skill of the VAWG sector and of survivors, the guidance does not provide sufficient emphasis or detail about engagement with VAWG organisations and appropriate reimbursement *"Once I realised that I was a victim of tech abuse the only thing that helped me to survive was the support of Refuge, which led me on to the Refuge tech support team. The tech support team went through a thorough process, in order to pinpoint where the threat was coming from. Once this had been established, safety precautions were implemented to eliminate the threat and to stop/avoid any further potential tech threats. Tech hygiene advice was also given." Refuge Survivor Panel Member* **Refuge recommends:** • Define **'independent VAWG expertise'** clearly and require it be embedded in policy review and design. ○ *See for further detail: 3.13(c), 3.13(e), 3.19(b), 3.26(c) Action 4, 4.20(b) 5.25(e), 5.25(h), 5.20(d), Case Study 3 in the accompanying table* • **Recommend that tech companies co-design monitoring and feedback** systems with survivors and VAWG experts • Ofcom itself continue to work with survivors and VAWG experts of the development of the guidance as well as monitoring its impact • Strengthen guidance on **user privacy, control, and transparency** so it better considers the needs of VAWG survivors ○ *See for example*: *Action 1 in the accompanying table* • Stipulate that tech companies should provide **fair compensation** for independent VAWG expertise • Establish an **Ofcom VAWG Advisory Group** including VAWG sector experts and tech company representatives to come together to discuss guidance implementation, emerging forms of abuse and best practice developments

Question	Your response
Question 2: Do you have any comments on the nine proposed actions? Please provide evidence to support your answer.	Confidential? – Y / **N** Refuge has reviewed each of the nine proposed actions, related good practice steps and case studies and made a series of recommendations as to where these can be developed and strengthened. This has been submitted as a Microsoft Word Document titled 'Refuge Ofcom VAWG guidance Q2and3 Actions and Case Studies' and should be read in conjunction with this consultation response.
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? – Y / **N** Refuge has reviewed each of the nine proposed actions, related good practice steps and case studies and made a series of recommendations as to where these can be developed and strengthened. This has been submitted as a Microsoft Word Document titled 'Refuge Ofcom VAWG guidance Q2and3 Actions and Case Studies' and should be read in conjunction with this consultation 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? – Y / **N** Refuge welcomes Ofcom's focus on encouraging tech providers to take ambitious, meaningful action to tackle online gender-based harms. The publication of assessments on how providers are addressing women and girls' safety is a vital step towards transparency and accountability. However, more robust, and proactive measures are needed to ensure real-world impact for survivors. **1. Enforce priority offences and embed VAWG guidance across all engagements** Refuge strongly recommends that Ofcom enforces VAWG-related priority offences consistently and assertively. In all regulatory interactions with tech companies, Ofcom should explicitly highlight the VAWG guidance, its purpose, and the ways in which guidance compliance helps companies meet their legal obligations regarding illegal content. This is especially crucial in addressing the evolving landscape of online harm. For example, Refuge's Survivor Panel highlighted links between incel ideology, and

Question	Your response
	wider misogynistic behaviour online. These complex, intersecting threats require joined-up thinking. Tech companies need to have these threats consistently flagged by Ofcom and for them to pay for VAWG sector expertise about how to tackle abuse. See also our Advisory Group recommendation below. **2. Create co-produced training for tech companies** Ofcom should commission and support the development of specialist training for tech companies on how to implement the VAWG guidance effectively. This training must be co-produced and delivered by expert organisations within the VAWG sector to ensure it reflects the lived realities of survivors and current patterns of abuse. We also recommend that VAWG training and awareness becomes a standard part of tech company practice so that everyone, from Board-level to senior management, to design teams and content moderators are trained. **3. Establish a VAWG advisory group** We strongly recommend the establishment of an Advisory Group made up of tech company representatives and VAWG specialists including survivors. This group should serve as a forum to share insights, track emerging threats, and guide responsive action on online VAWG. Crucially, VAWG representatives should be compensated for their expertise and time, in recognition of the specialist knowledge they bring. **4. Require VAWG data collection and sharing** To understand and respond effectively to VAWG online and emerging threats, Ofcom should require tech companies to collect and share disaggregated data with them on the perpetration of online VAWG on their platforms. Better data collection will not only support enforcement and mitigation strategies but also increase awareness across the tech sector about how their platforms are being used to perpetrate harm. **5. Promote and require accessible safety guidance** Tech companies should be required to provide and prominently promote accessible safety information for users, including specific resources for survivors of online VAWG. Refuge's Tech Safety pages[1] offer a strong model for this, providing clear, survivor-centred guidance and

Question	Your response
	tools. Ofcom should encourage providers to adopt similar best practices and ensure they are highly visible across platforms.
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? – Y / **N** **Summary of Key Recommendations:** 1. Require tech companies to set up a structured **intersectional risk assessment framework** and collect and analyse **disaggregated data** on Online VAWG. 2. Encourage **accessible design** across all safety features, taking into account protected characteristics 3. Strengthen the guidance on **understandable and inclusive safety defaults**. Refuge welcomes Ofcom's commitment to embedding human rights and equalities within the VAWG guidance. However, we believe the current assessments require strengthening to fully reflect the complex and intersectional nature of the harms women and girls face online, particularly those from marginalised groups. We are concerned about the ability of tech companies to respond to online VAWG because the profile of their workforce does not reflect demographics of women and girls in the UK. As the World Economic Forum's 2024 Global Gender Gap Report states, "women make up only 25% of the workforce in the technology sector, with a mere 10% occupying senior positions." **Recommendation:** To include in the Guidance an explanation about the importance of tech companies hiring a diverse workforce. **Workforce diversity** will support tech companies to tackle online gender-based harms. See also Action 1 in the accompanying table, where we make a recommendation for a new good practice step 3.19(e) on Human Resources practices. ` **1. Intersectional risk assessment must be central, not peripheral** Refuge strongly recommends that the **risk assessment framework** includes a **specific and structured equalities**

Question	Your response
	analysis of the risks facing women and girls with **overlapping protected characteristics**, in line with best practice guidance from the VAWG sector[2]. The draft guidance needs to be bolstered so that tech companies understand how to respond to **intersectional inequalities,** in particular • Race and ethnicity • Disability and neurodivergence • Sexual orientation and gender identity • Immigration status and English as an additional language **Recommendation**: Ofcom to revise the impact assessment to require platforms to integrate **intersectionality into the design, implementation, and evaluation** of safety systems. This includes platform architecture, automated moderation, human review, complaints handling, and risk assessments. Our research underscores how **some groups of women are disproportionately targeted online**. According to Refuge's *Unsocial Spaces* report: • **75% of LBTQ+ women** surveyed had experienced online abuse • **62% of young women** and **45% of women from ethnic minority backgrounds** also reported abuse. These figures underline the need for tailored responses to harm, informed by the experiences of specific groups **Recommendation:** All platform-level risk assessments and transparency reporting should be required to capture **demographic data on victims and perpetrators**, ensuring that interventions are responsive to the most at-risk groups. This should include the collection and analysis of **disaggregated data** to measure harm and effectiveness of safety interventions across different groups **2. Equitable – Not Just Equal – access to platform safety tools** Online platforms must ensure that women and girls are offered options which are **accessible and usable** across differing abilities, languages, and levels of digital literacy.

Question	Your response
	A 'one-size-fits-all' approach will disproportionately disadvantage groups such as survivors with disabilities, older survivors, or those with English as an additional language. Refuge's experience supporting survivors reveals how complex and poorly communicated safety settings can lead to women being unaware of how to protect themselves online or inadvertently exposing themselves to further harm. We strongly encourage the avoidance of a creating a **two-tier system of safety**, where marginalised users are left with inadequate protection due to inaccessibility. **Recommendation**: Ofcom should encourage platforms to: • Implement **assistive technologies**, including screen reader compatibility and simplified navigation. • Explicitly design safety features with **survivors with disabilities and neurodivergence in mind**. **3. Preventing harm through safer defaults and informed use** Refuge welcomes Ofcom's emphasis on **safer default settings** (Action 5) but encourages stronger guidance around the **accessibility and understandability of user options** (para. 4.22–4.25). Survivors may not understand what they are consenting to in complex terms and conditions, particularly during or after traumatic experiences when they are most in need. **Recommendation**: We urge Ofcom to: • Strengthen guidance on making safety options **clear, plain, and accessible**, especially for survivors with cognitive overload or limited technical skills. • Consider mandating a **universal safety check-up or onboarding guide** that walks users through important privacy and safety settings, available in multiple languages and formats. **4. Signposting to specialist support**

Question	Your response
	We welcome the requirement (5.15(f)) for platforms to signpost users to relevant support for harms such as domestic abuse or image-based sexual abuse. However, many survivors Refuge supports are unable to access appropriate online help because the services signposted are **generic and not inclusive** of those with specific needs. We reiterate here and throughout the need for tech companies to make best use of the VAWG expertise available in the UK. For tech companies to demonstrate accountability, for the harms generated on their service, they should pay for the knowledge and skills of the specialist services throughout, including a contribution to the running of VAWG services to which they are signposting. See this detailed in Refuge response to Question 1. **Recommendation**: Ofcom should require that signposting includes: • **Specialist VAWG services**, including those for **Black and minoritised women, LBTQ+ survivors, disabled survivors**, and those with **English as an additional language**. • **Multilingual resources** and **easy-read formats**. • Clearly visible support information that appears at relevant touchpoints, such as platform sign-up, updates to software or reporting.
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.	Confidential? – Y / N This question falls outside of our expertise.

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