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? – N The Guidance sets out many welcome steps and makes a good foundation overall. There are many positive actions included in the Guidance, such as the focus on safety-by-design, importance of listening to users, use of case studies, and clear action areas. **However**, **two areas require further reflection and refinement: terminology and the conceptual framing of harms**. - **Terminology: 'Online Domestic Abuse' vs. 'Technology-Facilitated Abuse':** 'Online domestic abuse' is not a commonly used phrase. We have recently concluded a global Delphi study exploring definition and conceptualisation around technology-facilitated gender-based violence, which concluded that **the most commonly recognised and understood terminology is 'technology-facilitated abuse'.**[1] Not only is this terminology more widely-recognised, it is also used in key policy documents such as the Domestic Abuse Act 2021 Statutory Guidance.[2] Using terminology which is consistent with policy documentation could ensure the Guidance is more complementary to future policy documents (including the VAWG Strategy expected to be published this summer.) **In addition, the term 'online domestic abuse' may prevent some instances from being identified or reported** – our recent study[3] reinforces the fact that not all victims-survivors of domestic abuse immediately recognise the harms or abuse being directed at them, in that way. One reason for this may be the increasing normalisation of certain behaviours of digital spaces that make this form of violence harder to recognise as abusive.[4] - **Incomplete Typology of Technology-Facilitated Harms:** The current categorisation of harms in the Guidance — namely, online misogyny,

[1] https://journals.sagepub.com/doi/10.1177/08862605241310465
[2] https://assets.publishing.service.gov.uk/media/62c6df068fa8f54e855dfe31/Domes-
2021_Statutory_Guidance.pdf
[3] .org/doi/10.1145/3706599.3719986
[4] city.ac.uk/news/tech-facilitated-abuse-and-the-new-normal/

Question	Your response
	online domestic abuse, pile-ons and harassment, and image-based sexual abuse — **fails to fully account for 1:1 forms of abuse that occur outside of intimate partner relationships**. Our evidence[5] shows that technology-facilitated abuse often occurs in a wide range of interpersonal contexts, including: Parental abuse or intergenerational control; Former acquaintances, colleagues, or casual contacts; Strangers who target individuals through digital platforms, especially in marginalised or public-facing communities. While group-based or relational abuse is important, exclusive focus on these categories overlooks a significant proportion of the experiences of women and girls online. For example, abuse from a controlling parent may involve stalking via apps[6], surveillance through devices[7], or coercion via messaging[8] — none of which comfortably fits into the current Guidance categories. To better reflect the diversity of victim-survivor experiences, we recommend: **Expanding the typology of harms to include 1:1 abuse that falls outside of intimate relationships; Including more granular examples or case studies that illustrate non-partner-based tech abuse; Ensuring the framing of harms does not assume relational proximity as a prerequisite for abuse to be recognised or addressed**.
Question 2: Do you have any comments on the nine proposed actions? Please provide evidence to support your answer.	Confidential? – N We welcome the nine proposed action areas, which cover important facets of platform responsibility, user protection, and accountability. However, to maximise their effectiveness, the Guidance must do more to **distinguish between aspirational recommendations** and **actionable, enforceable expectations**. Greater **clarity** around how these actions will be **monitored** and **evaluated** — particularly **how 'safer' outcomes will be defined and measured** — is essential. **Below, we offer detailed comments on each relevant area, drawing on our research and practice experience.** Within the areas of '**Taking Responsibility'** - - **Subject Matter Experts**: It is welcome to see encouragement of consulting with subject matter experts within this action area. That said, the sector is not well resourced or supported. Many services are significantly under-funded, and their rightful priority is supporting victims-survivors, and **we know that many requests for expertise are made without remuneration, placing pressure on already limited capacity.** Given the scale and profitability of the tech sector, there

[5] https://dl.acm.org/doi/10.1145/3706599.3719986
[6] https://petsymposium.org/popets/2025/popets-2025-0052.pdf
[7] https://dl.acm.org/doi/10.1145/3368860.3368861
[8] https://link.springer.com/article/10.1007/s00127-021-02113-w

Question	Your response
	should be a clear expectation that **expert input must be appropriately compensated**. Otherwise, the knowledge needed to inform effective prevention and response efforts will remain inaccessible. We also suggest the Guidance makes explicit reference to **longer-term partnerships and capacity-building**, rather than short-term or transactional engagement. - **Victim-Survivor and User Engagement**: If the Guidance continues to encourage tech companies to engage with victims-survivors, then the Guidance must also be provided setting out **how they can do so sensitively and in a way which will not trigger or cause any further harm to the individuals involved**. Feedback from victims-survivors must also be representative, methodologically sound, and address the risk of piecemeal improvements which mask broader harms. - **User Surveys**: Tech companies should be mindful of perceptions when engaging users on this topic. From our research into technology-facilitated abuse, we know that **victim-survivors often do not recognise what they are experiencing as abuse**, due to both the **normalisation of digital surveillance** and control[9], and a **lack of awareness** around emerging forms of harm. Likewise, **perpetrators may rationalise or deny their abusive actions** (e.g., framing surveillance as 'keeping someone safe')[10]. These dynamics should be explicitly acknowledged in the Guidance. Surveys that fail to account for them risk producing misleading results and may be used to safety-wash company behaviour. **We therefore recommend that Ofcom include guidance on: Incorporating behavioural insights into survey design; Validating questions through collaboration with practitioners and researchers; Triangulating survey findings with other forms of data, such as complaint logs or helpline trends.** Within the areas of '**Preventing Harm'** - - **Abusability Assessments and Red Teaming**: It is highly welcome that the Guidance includes abusability assessments, threat modelling[11], and red teaming. These techniques are critical for uncovering how platforms and products can be exploited to cause harm. However, for maximum impact, the Guidance should encourage companies to: **Apply these assessments across all products and services, including those outside the formal scope of the Online Safety Act; Extend this practice to connected technologies and smart devices, which**

[9] https://dl.acm.org/doi/10.1145/3706599.3719986

[10] Evidence on the finding is not yet publicly available (see: https://www.genderandtech.net/study-on-tech-abuse-perpetration). We would be happy to share further with Ofcom ahead of the evidence being published.

[11] https://discovery.ucl.ac.uk/id/eprint/10129049/1/Tanczer_Threat%20Modeling%20Intimate%20Partner%20Violence_VoR.pdf

Question	Your response
	remain under-regulated[12] yet are increasingly used to facilitate abuse (e.g., via surveillance, coercion, and control); Make these practices routine and proactive, embedding them into product development cycles as a standard element of responsible innovation.[13]. Given this Guidance is meant to be ambitious and is different to a formal code, **there is an opportunity to push for this** – for companies to adopt these practices as standard and ensure safety becomes part of their corporate culture (not just things they need to do for in scope projects to tick a box). - **Safer Defaults**. This is welcome, but it will be just as key to ensure that **simplicity and usability**[14] is retained in changes to default settings. Companies must be encouraged to ensure that user design is taken into consideration, so that safer defaults (which are absolutely needed) do not become more complicated defaults or harder-to-use which will create a further issue. We would also recommend the Guidance including more **proactive use of** '**reminders**' – particularly reminders that users are logged into their accounts on 'other' devices, and **notifications to all users of a system** within a home network if new devices are added[15]. For example, if a new camera is added to a home network, that all users are notified instead of just the family member (typically male) who has set up the account. We would also welcome additional steps where there are enhanced concerns around privacy and security – such as apps which blur the line between privacy and security.[16] Within the areas of '**Supporting Women and Girls'** - **Intersectionality / Personas**: Understanding that women and girls are not a homogenous group is essential. Experiences of technology-facilitated abuse vary significantly across lines of race, age, disability, immigration status, sexual orientation, and socio-economic status. Guidance should urge companies to embed intersectional thinking across all actions, including in user research, support pathways, and design processes. We recently published a paper using personas based on Refuge case data to demonstrate how help-seeking behaviours differ across user profiles. These personas can support more inclusive and effective intervention.[17]

[12] https://assets.publishing.service.gov.uk/media/607d7fdcd3bf7f400b462d9e/The_UK_code_of_practice_for_consumer_IoT_security_-_PETRAS_UCL_research_report.pdf
[13] https://journals.sagepub.com/doi/10.1177/10778012231222486
[14] https://dl.acm.org/doi/pdf/10.1145/3688459.3688477
[15] https://journals.sagepub.com/doi/10.1177/10778012231222486
[16] https://petsymposium.org/popets/2025/popets-2025-0052.pdf
[17] https://dl.acm.org/doi/10.1145/3706599.3719986

Question	Your response
	- **Access to Information**. It will be a welcome step for women and girls to have more control over their experiences, and better reporting systems. However, it will also be critical for women and girls to be able to access information from platforms, including after it has been delete. Giving women and girls control over their digital safety includes not only better reporting tools but also meaningful access to information, including historical or deleted data. **Abusers often exploit features that erase traces of contact, surveillance, or manipulation. Platforms must make it easier for victim-survivors to retrieve relevant data for evidentiary purposes** and to understand how they have been targeted. This could include: **Clear records of device logins, location access, and deleted messages; Options to download interaction histories and metadata; Transparent audit logs of administrative changes in group settings or shared devices**.[18]
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 The good practice steps and case studies highlighted demonstrate important progress, **but several critical issues remain regarding their effectiveness, applicability, and potential risks**, which must be addressed to ensure meaningful impact. - **Enforcement**: Give the non-binding nature of this Guidance compared to formal Codes, **there is a significant risk that companies may not take necessary actions without the credible threat of enforcement**. Evidence from prior regulatory frameworks shows that voluntary compliance alone is insufficient in driving systemic change across the tech sector. It is imperative that the **Guidance articulates how Ofcom will identify and challenge poor-performing services—whether through penalties, mandatory audits, or other sanctions**. Tackling VAWG must be treated as a **non-negotiable obligation**, not an optional 'nice-to-have' feature. - **Legal Risk**: To incentivise compliance, public **transparency measures such as performance rankings, best practice awards, or 'naming and shaming' initiatives could prove highly effective**. However, these strategies must be underpinned by a robust legal risk mitigation framework to protect Ofcom from defamation or slander claims. Clear guidelines should be established to ensure that public statements are fact-based, proportional, and legally sound, enabling Ofcom to voice concerns openly while safeguarding all parties.

[18] https://link.springer.com/article/10.1007/s10896-023-00619-2

Question	Your response
	- **Named Accountability vs. Corporate Responsibility**: While appointing a named individual responsible for compliance is a positive step, **we fear that companies might insulate themselves by shifting liability onto individuals, potentially limiting broader corporate accountability**. Ofcom should conduct a risk assessment to evaluate the **likelihood of insurance claims or other corporate strategies that undermine accountability**. Consideration should be given to reinforcing corporate-level responsibility in parallel, ensuring that accountability is not siloed at the individual level alone. - **Compliance Training:** It is positive that staff involved in the design and operational management of a service will be 'sufficiently trained in the service's approach to compliance with online safety duties.' However, further detail on what 'sufficient training' is – would be welcome. There is a risk that what is deemed 'sufficient' by a service, is not. **We would welcome clarity on how 'sufficient' will be measured to ensure it is effective, and also clarification around how this training will take account of emerging technology areas in relation to tech abuse**. This is a rapidly evolving field and there is a risk that training becomes outdated very quickly. It would also be welcome that Ofcom clarify that **'staff involved' may include relevant non-permanent staff, such as contractors who are bought in design and set-up a service** before it is handed over to the permanent operational teams who manage business as usual services. - **Unintended Consequences**: There is a **risk that services cherry-pick improvements set out in the Guidance**, and that other areas (e.g. not-in-scope services that we know still pose a significant threat to women and girls such as connected devices[19]) will naturally worsen as attention shifts. **We would very much welcome Ofcom conducting a baselining survey (immediately, not in 18 months) to assess the current practices in place, so that unintended consequences (such as other areas worsening) can be monitored properly as part of implementation** – and potentially contribute to future iterations of the Guidance. - **Increased Deletion / Visibility Changes**: Ensuring victim-survivors have **access to content, including messages or media deleted by perpetrators, is critical for both their safety and for legal redress**. Restricted access to deleted content severely hampers victims' ability to build cases for prosecution or protection orders. The Guidance should explicitly mandate that **platforms retain and provide secure access to such records for victim-survivors and law enforcement where appropriate.**

[19] https://bristoluniversitypressdigital.com/view/journals/jgbv/5/3/article-p431.xml

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 Publishing an assessment of how providers are addressing the safety of women and girls is a positive and necessary step to drive accountability and transparency. **To maximise its impact, we suggest the following enhancements.** - **Clear, Accessible Reporting:** Given the assessments could create public pressure on services to do more, **they must be digestible for the general public and easy to understand.** This could include using **one-word descriptors (such as with schools) such as 'good' or 'underperforming**' to make clear where the service is considered to be in comparison to their peers. These concise indicators should be **complemented by detailed reports** accessible to stakeholders who want deeper insight. - **Multi-Source Evidence for Assessments**: Robust assessments should integrate a variety of evidence streams, including **independent audits to verify compliance, direct user feedback to capture lived experience, and provider self-reporting** to identify internal awareness and commitment. This **triangulated approach** increases the credibility and comprehensiveness of assessments, ensuring they reflect both organisational processes and real-world impact. - **Recognition and Incentives for Excellence:** Consider introducing public awards or certifications for best-performing providers. **Highlighting 'best in class' performers not only reward positive behaviour but creates aspirational benchmarks within the industry**. Additionally, establishing **public trust indicators—visible badges or ratings that inform user choice—can empower consumers** to select safer services, thereby creating market-driven incentives for compliance.. - **Driving a Cultural Shift Beyond Compliance**: Encouragement should go beyond compliance with in-scope services. Providers should be **incentivised to embed the principles of this Guidance across their entire corporate culture, including out-of-scope products and services where they have influence and where harms to women and girls have been documented**. Genuine safety improvements require organisational commitment at all levels and across all relevant products, not just regulatory minimums.

Question	Your response
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
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? – N

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