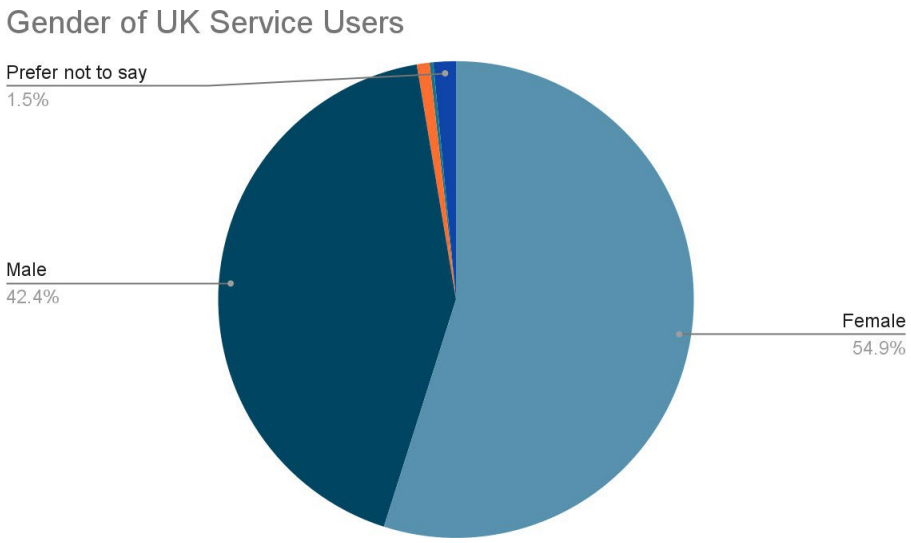
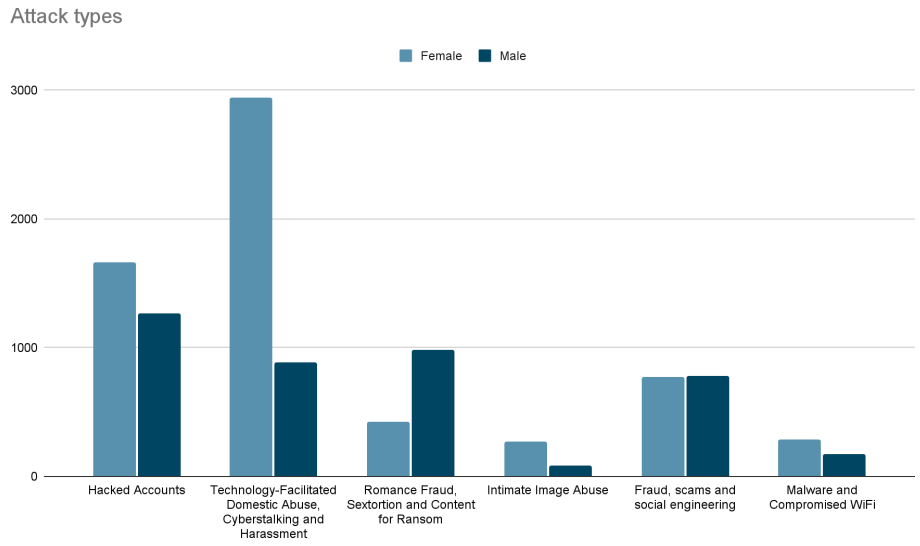
WARNING: This consultation response contains language and/or material that may be distressing

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'?	We commend the excellent overview of evidence in Chapter 2 showing that the harms in the draft guidance pose unique and disproportionate risks to women and girls. The approach aligns with The Cyber Helpline's frontline experience that certain forms of cybercrime and online harms disproportionately impact and silence women and girls' voices. We encourage continued clarification that addressing these harms is not "special treatment" but rather essential to equalise online safety and free expression for half of the population. This could be more explicitly framed and reinforce that protecting women and girls from cybercrime and online harms enables their own Article 10 rights. The Cyber Helpline supports victim-survivors of cybercrime and online harm, categorising these attacks across a number of different categories. We began collecting demographic data on service users in the middle of March 2023 and since that date, has opened 11,154 cases in the UK. 54.9% of these service users identified as female.  We recognise that non-gender-conforming people are less likely to seek support and feel it is an injustice to provide the data we hold for the crimes and harms these individuals experience. However, we know that individuals falling under the non-binary umbrella are also disproportionately likely to experience some of the same harms as women and girls. The guidance provided by Ofcom is likely to benefit them too, and it feels important to us that they are recognised and their voices heard within this guidance. **We strongly encourage further reference to transgender and non-binary people and transphobia alongside misogyny.** The chart below compares the attacks we categorise, collated into more broad categories and the victimisation rates of men and boys and women and girls. As the guidance acknowledges, there are often overlaps between the harms, and so the most prevalent harm is tagged at the time of categorisation.



We find similar trends to Ofcom's content and activity, which disproportionately affects women and girls. However, we propose some changes in how pile-ons and online harassment, and particularly 'online domestic abuse', are defined.

Firstly, pile-ons and online harassment fail to include **doxxing**, the act of revealing personal information about someone online without their consent, within its definition. This is something we see occurring in pile-ons against female gamers, advocates, politicians and celebrities. We feel it is important that this terminology be included.

There are a further two forms of harassment that our data shows disproportionately impact women, girls and non-binary people. These are **'outing'** - threatening to, or actually, posting information that the victim-survivor wishes to keep private - such as their medical history, sexuality, religious beliefs or gender identity. These could be things that the victim-survivor has confided in the perpetrator of abuse about, or could be things that the perpetrator of abuse has found for other means such as finding private information through unauthorised access to accounts.

The second form that isn't mentioned is **content for ransom**, whilst 'sextortion' or webcam blackmail, disproportionately impacts men, in domestic and grooming cases we see that women and girls are held to ransom for information or intimate images. This ransom can take the form of money, sharing further information or images or withholding needs.

Furthermore, **'online domestic abuse'** as a phrase, fails to acknowledge the comorbidity of online and offline harms. We alternatively recommend the term **'technology-facilitated (domestic) abuse.'** We make note of the use of the term 'intimate relationship' within the consultation's definition of 'online domestic abuse.' In our frontline experience, the intimacy of a relationship has not been found to impact the tools and technologies used to perpetrate domestic abuse. Rather, we hold concern that the use of the term 'intimate' may detract from domestic abuse enacted by family members or short-term relationships. We therefore encourage review of the terminologies chosen within the consultation's definition.

Finally, in regards to 'online domestic abuse', the definition fails to include **financial abuse**, which is often perpetrated utilising technology. In domestic abuse and stalking cases, we see that technology is utilised to monitor, control and restrict finances as well as fraudulent activity taking place.

Confidential? – N

Question 2: Do you have any comments on the nine proposed actions? Please provide evidence to support your answer.	The nine action areas cover a holistic life cycle of steps for providers. Below we address each action. **1. Ensuring governance and accountability processes address online gender-based harms** Research shows that companies have been slow to tackle complex harms. Learning from homicide reviews indicate that numerous services spanning criminal justice, social services, health agencies and advocacy teams are well placed to provide insight of the risks posed to women and girls (Bracewell, Jones & Haines-Delmont, 2022). We strongly support measures like executive responsibility for women's safety and external advisory councils to drive cultural change. We particularly support the idea of accountable individuals. We note that guidance could further emphasise training for content moderators and trust and safety teams on gender-based abuse. Leadership buy-in is crucial, but day-to-day moderation teams also need expertise in this area to effectively recognise misogyny and intersectional abuse. Throughout our frontline services, our cyber specialists often work with online moderation teams to ensure their appreciation of the patterns and indicators of gender-based violence. Not all victim-survivors will connect with support teams who can advocate alongside them, as such, understanding the full context of the landscape is vital. The idea of a subject matter expert within this area needs to be more clearly defined. There are a number of specialised areas in this space, from policy to frontline support. Subject matter experts should be trauma-informed and victim-survivor led. Perhaps a database of subject matter experts should be held by Ofcom. By holding a database of this nature, Ofcom may seek the guidance and expertise from numerous individuals. This, in turn, ensures that collaboration is varied across subject matter experts, and refrains from a fixed panel approach, which may restrict diversity of contribution. Additional training could take place in partnership with specialist NGOs who can impart their expertise but also provide the victim-survivor's voice. We also recommend Ofcom encourage industry-wide knowledge sharing such as a voluntary multi-company advisory panel - to extend the benefits of expert consultation to providers who may have limited means and less resources. **2. Conduct risk assessments that focus on harms to women and girls** We endorse the call for gender-sensitive risk assessments and see this as a positive step. We agree that engaging survivors and frontline organisations in this process leads to more realistic risk identification. However, we encourage exploration of how these risk assessments can be achieved in a manner that provides robust support to the services that will utilise them. Established gender-based violence risk assessments have increasingly been critiqued on their validity. With research indicating that the successful indication of harm is substantially reliant upon the professional recognition of the services involved (Messing & Thaller, 2013; Turner, Medina & Brown, 2019; Graham et al., 2021). In consequence, we encourage that the guidance clarify the frequency of these gender-focused assessments, including both time scales and product changes that constitute revisitation. We would like to see these risk assessments summarised and shared as part of transparency reporting to both reinforce action 3 and to encourage best practices and contribution towards multi-agency knowledge sharing. **3. Be transparent about women and girls' online safety** Our service users echo the frustration at the "black box" of moderation and it is only through transparency that services can be held accountable to progress.

	However, how accountability will be coupled with this transparency is unclear. We suggest that final guidance encourages providers to take action in response to their findings, potentially, encouraging record keeping of the approaches and responses undertaken by services and transparency of their goals. . **4. Conduct abusability evaluations and product testing** Safety-by-design is a priority for us, feeding into action 2 as well, we believe that (as much as possible) a **standardised approach should be taken to safety**, in the same way that vehicles require mandatory safety features, are crash tested, and rated by Euro NCAP for safety - we believe that technology should be required to meet a minimum standard for online safety before going to market. This inclusion of foundational steps for abusability evaluations and red-teaming exercises is sensible. We would encourage collaboration and consultation with victim-survivor support services in this space who will have a unique insight into threats. We caution that smaller providers may lack the expertise and resource for robust abusability evaluations and product testing and suggest that common toolkits be available and continue to be adapted to these smaller companies. We echo back to our prior response, which states that the successful identification of harm and risk is substantially reliant upon the professional recognition of the services involved (Messing & Thaller, 2013; Turner, Medina & Brown, 2019; Graham et al., 2021). Although much of our frontline cyber-concerns present using widely accessible technologies. We also suggest expanding abusability testing to clearly cover emerging technologies including the metaverse, AR/VR and smart home technologies. **5. Set Safer Defaults** We fully agree that the baseline configuration of a service should be the safest. The onus should be on providers to set these wisely and users should then have the flexibility to customize these.We appreciate that larger companies and services may draw upon their own subject-matter experts and consultants to shape how this is delivered. For those that do not seek this guidance, a baseline configuration in collaboration with subject-matter expert testimonies as to *why* certain features are vital may provide valuable context to implore and product development to situate the victim-survivor first. We have a minor recommendation here, if certain features are off or on by default for safety, a user should be briefly informed why - aligning with media literacy goals and a user-centric approach. Delivery should be inclusive of additional needs and disabilities that may require alternative manners of information dissemination. **However, we also note that 'common sense' security and privacy education is not always best practice, particularly in cases of stalking and domestic abuse**. We know that stalking is fixated, obsessive, unwanted and repetitive. Taking the first two criteria into account, by removing a stalker's access, such as by blocking them or removing their access to an account, incidents have occurred where stalking has escalated, leading to physical harm or more overt behaviours. Media literacy should also encourage this thinking, making users aware of potential risks whilst avoiding fueling hypervigilance and trauma. We know that this is not relevant to all users so this requires more thought but when common sense and education tells us to block someone who is abusive online, social media companies have a responsibility to ensure that this education takes place. For example, generalised advice on how/when to block people does not consider risk assessment. **6. Reduce the circulation of online gender-based harms** This action is crucial. We support the approach of persuasion, removal and reduction and believe that hash databases should become standard. In particular, we were glad to see the mention of 'nudge' systems, knowing this was trialed by various companies a number of years ago and never taken forward by them, despite the technology having existed for some time and trials showing a reduction in harmful content being posted by young people, it has not seemed to be rolled out.

	A caveat here is the need for clear policies and safeguards around reduction with platforms providing full transparency on what triggers downranking to avoid perceptions of bias or censorship. **Furthermore, we emphasise the risk of driving gender-based harms and misogynistic content more underground to platforms that create a stronger echo-chamber and more extremist communities.** We recommend that providers document their rationale for any reductions of content. This draws back to our prior comment; *We suggest that final guidance encourages providers to take action in response to their findings, potentially, encouraging record keeping of the approaches and responses undertaken by services and transparency of their goals.* We agree there is a risk of overreach of this automation and that discussions may be erroneously flagged. However, due to the prevalence and consequential impact of gender-based harms, overreach would be preferable to inaction. **A question to consider is whether the data for 'recommender systems' or algorithms could be used to identify users at-risk of being susceptible to misogynistic content or actively looking for it to implement preventative measures and onward signposting and/or referrals to preventative programs and Channel Panels.** **7. Give users better control of their own experiences** Empowering users is at the heart of our ethos, and we are pleased to see this included in the guidance. We hear frequently that the ability to block multiple accounts at once reduces trauma and is more practical. The ability to set custom filters is also invaluable, not only for immediate impact but to reduce trauma reminders in the future. We are delighted to see mention of signposting to supportive information - connecting users to specialist resources directly from the platform is vital. Our recommendation in this area is **user-controlled rate limiting** as a tool. For example, being able to pause all incoming messages for a specific period of time. This can support with managing overwhelm during abuse and pile-on incidents. We also encourage that effective user controls must be easy to find and use. Last year, X removed SMS two-factor authentication for free users, forcing many to go without two-factor authentication due to not having the knowledge to use authenticator apps or due to authenticator apps not being accessible. **Any feature that provides security and safety to individuals should not be locked behind a paywall,** and this should be emphasised in the guidance. Referring back to the risks associated with taking privacy and security actions during a stalking or domestic abuse case, users need to be armed with information regarding risks to make clear and informed choices, considering potential escalations due to implementing security and privacy features. Users are not entirely in control until they are aware of this risk. Greater control of the content recommended to users is an exciting suggestion and offers an opportunity to educate users on algorithms and how content is recommended. We see that cybertrauma can be fueled by content recommended by algorithms, and feel that it has been placed there by malicious individuals. This offers a great opportunity not only to customise content, but to educate. There is mention of steps such as quick exit; however, a concern here is that this may give a false sense of privacy. If providing steps such as a quick exit, this should be accompanied by further information, such as deleting browser history and using private browsers. Similarly, applications that purport to conceal themselves when in the app carousel should be sufficiently tested and reviewed. We recognise that victim-survivors have extremely limited windows of time where they can take safety and security steps whilst within abusive

environments. Consequently, many rely heavily on the validity of the outlined security and privacy settings including 'quick exit' functionality. However, following a review of various social and safety applications - many pages remain visible within a device's app carousel if clicked away from, but not closed. This places victim-survivor's activity at risk of exposure when their device activity may be proximity monitored.

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

Even the safest design will never prevent all harm, so accessible, navigable and trauma-informed reporting is vital. Evidence is clear that many women, girls and non-binary people do not report abuse.

One area we believe is critical to strengthen is user communication, ensuring that when a report is made, the user receives timely confirmations and updates, as uncertainty can exacerbate trauma.

We also caution that reporting systems should avoid **re-traumatisation** by asking overly invasive questions. We agree that context is key to cases and that off-service reports should be able to be added. However, services receiving and requesting information that they cannot take action on may not be the best approach. For example, if dating websites take reports of incidents that have happened at in-person meetings, can these actually be investigated, and do their terms allow action to be taken as a result of events happening off-platform? If not, is it trauma-informed and proportionate to ask for and collect this data? Arguably, would seeking this data - when actions may not be within the breadth of action, be in conflict with data protection?

Similarly, users should **always have the opportunity to talk to a human** at these platforms. Many will not feel comfortable answering questions when they do not know who, or what, the answers are going to. An opportunity is also lost to ask questions for further context. At a minimum, if a user states that they believe the outcome provided by a platform to a report is incorrect, they should have the opportunity to speak to a human. We emphasise that victim-survivors of technology-facilitated abuse may distrust that they are speaking to a legitimate person when only receiving written replies. In addition, written-only support restricts numerous victim-survivors with additional needs and disabilities, where conversational support is best placed.

We commend the work of Trusted Partners such as our partners at Report Harmful Content, however, this relies on the victim-survivor knowing about, or finding, these services, which we know is rare as we signpost a number of our service users to them, they are often successful in escalating reports and supporting us in resolving cases.

However, in the case of Meta's Trusted Partner program, Trusted Partners are meant to hold Meta accountable; they are not paid to provide a service and do this voluntarily. Many of the participants are charities. However, evidence shows that the lack of human moderation at Meta means that Trusted Partners are becoming escalation pathways for reporting, draining their resources and acting, in all but name, as an outsourced, unpaid moderation team which those who need their support have to find on their own. This is not an acceptable form of moderation for victim-survivors, or for Trusted Partners. Members of our team have worked within Trusted Partner programmes historically, with their experiences depicting varying improvement in response time and correspondence

Online harms impacting women, girls and non-binary people often span multiple online platforms. Victim-survivors have to make a report to each platform, which may be difficult and different outcomes may be met by each. This could escalate behaviour on other platforms that do not take immediate action. Therefore, in particularly in high risk cases (but ideally all multi-platform cases), **multi-agency/multi-platform information sharing should be considered.**

Allowing users to give feedback on reporting processes is a necessary change, however, worthless if action is not taken on feedback and risks re-traumatisation by asking

victim-survivors to recount experiences. **Feedback systems should only be implemented if feedback really will be considered and acted upon.** As we have stated previously;

We suggest that final guidance encourages providers to take action in response to their findings, potentially, encouraging record keeping of the approaches and responses undertaken by services and transparency of their goals.

9. Take appropriate action when online gender-based harms occur

Our service users frequently express frustration at the lack of action taken by services when a report is made, and where action is taken, the ease at which it is circumvented. Therefore, we are strong supporters of the recommendations in this guidance.

That being said, we are passionate that this step should also include **cooperation with law enforcement where appropriate**. The guidance is focused on what companies can do internally, but platforms should have clear pathways to refer cases to police and preserve evidence. Across our teams, numerous caseworkers report service users expressing that officers in charge of investigations have expressed that they cannot or will not engage with online services due to an inability to communicate with the service's teams. This prohibits effective evidence collection, as well as misleads victim-survivors of the pathways that can support their investigations. Ofcom should remind providers of their duty to report certain content and reiterate the need for expedited assistance to users who go to law enforcement, and requests for information from law enforcement.

In the long term, we would be delighted to see a structured channel between platforms, the third-sector and law enforcement to reduce fragmentation, conflicting guidance and duplication in cases of severe harm. We are mindful that channels such as the 'Trusted Partner Programme' are in place with varying success. Consequently, we recommend that data is retained and shared with Ofcom on requests, response times, and outcomes for review. This would seek to ensure that structured channels are actively engaged with and operationally effective.

This action has reference to taking enforcement action against users who "continually violate" a service's Terms of Service. We would encourage further guidance on what "continually violate" means and a practice bank of enforcement actions and their effects.

We agree that there needs to be a balance of implications for users who have been reported and had access restricted. Particularly when accounts are suspended and awaiting investigation, we suggest a **'read only' access approach** could be utilised in these circumstances. Ensuring access to information is still possible, given that social media is the primary form of media consumption, both for entertainment and news. As previously stated, delivery should be inclusive of additional needs and disabilities that may require alternative manners of information dissemination.

Like many, we were disappointed to see fact-checking coming to an end on Meta and the change to the X style of community notes. We believe that **independent fact-checking is vital in the fight against disinformation** and strongly encourage that Ofcom cites this as best practice. In the Community Notes model/upvoting system, we have seen this being used maliciously, often in the form of pile-on attacks and to further spread disinformation or biased rebuttals.

Finally, this action discusses the sending of high-risk reports to specialised teams. Two matters require clarification and best practices here. In regards to the identification of high-risk reports, it is important to understand who would be identifying them - would this be automated, user-defined or manually screened? Furthermore, how is high-risk defined and how is this assessed? However, as expressed before, we encourage exploration of how these risk assessments can be achieved in a manner that provides robust support to the services that will utilise them. Established gender-based violence risk assessments have increasingly been critiqued on their validity. With research indicating that the successful indication of harm is substantially reliant upon the professional recognition of the services involved

	(Messing & Thaller, 2013; Turner, Medina & Brown, 2019; Graham et al., 2021). Nonetheless the presence of **a standardised risk assessment** for individual cases to guide and assist with risk identification, akin to the(S-)DASH assessment utilised in stalking and domestic abuse that focuses on online harms and technology-facilitated abuse, with practitioners in moderation and trust and safety teams trained to deliver these risk assessments could save lives. Confidential? – N
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.	Overall, the good practice steps and case studies effectively show how the proposed actions can be implemented. For the most part, the case studies and good practices reflect approaches that The Cyber Helpline has also found to be successful. In terms of applicability, whilst it's acknowledged that services vary, most of the steps can be easily adapted to different platforms and we do not foresee any feasibility issues for providers, especially as many are already experimenting with these measures. However, we do advise that continued refinement is made on proportionality for large and smaller services. The guidance somewhat addresses this with "additional steps" and notes that some may suit high-risk and high-reach services more but perhaps the final document could provide **more tiered examples such as "basic, intermediate and advanced" steps so that all companies, regardless of size can do something in each area**. This would mitigate the risk that smaller providers feel that most or all practices are only applicable to the bigger players. As previously stated, we appreciate that larger companies and services may draw upon their own subject-matter experts and consultants to shape how this is delivered. For those that do not seek this guidance, a baseline configuration in collaboration with subject-matter expert testimonies as to *why* certain features are vital may provide valuable context to implore and product development to situate the victim-survivor first. A key concern for us within the guidance is the number of practice steps and case studies which reference engaging with survivors and victim-survivors. We believe this is a vital step, when done in a trauma-informed manner, and are strong supporters of the work Chayn has done in this space. Our concerns are that **best practices in survivor engagement may not be met by providers and engaging with them without proper safeguards could risk re traumatisation**. Best practices in this engagement should be provided. **Additionally, victim-survivors should be fairly compensated for their time, expertise and emotional labour.** Many survivors provide invaluable lived-experience insights that significantly enhance policy and platform safety measures, and they should not be expected to do so voluntarily, or at personal cost. Compensation acknowledges the value of their contributions. We recommend that Ofcom encourages platforms and policymakers to integrate these principles. For smaller platforms with less resources to be able to engage with victim-survivors and survivors in this manner, consideration should be given to working with NGOs to gain a victim-survivor's perspective. Secondly, there are a number of mentions of knowledge-sharing. This is a vital area and we believe that a knowledge base is important. Learnings should be taken from the College of Policing in this space. Although contributions will be harder to receive, perhaps there is a way this could be incentivised. This hub could also host information on subject matter experts in various areas who could be considered for consultancy work. As previously stated, by holding a database of this nature, Ofcom may seek the guidance and expertise from numerous individuals. This in turn ensures that collaboration is varied across subject matter experts, and refrains from a fixed panel approach which may restrict diversity of contribution. Some considerations we have already spoken about in Question 3, but we feel there are some good practices happening in the industry which have not been discussed. In regards to good practice within the tech space, we feel Apple's Lockdown Mode deserves some mention: https://support.apple.com/en-gb/105120. Whilst we have seen cases where this fuels hypervigilance, it allows those who may be traumatised by technology-facilitated

	harms to continue use of their device in a safe environment, where they may have otherwise turned to feature phones or stopped using technology altogether. This requires further research and ideas, but it is a good example of having a restricted, feature-poor version of services to create safe online environments. Furthermore, we commend Discord's sensitive content filters https://support.discord.com/hc/en-us/articles/18210995019671-Discord-Sensitive-Content-Filters which can be turned on (or is automatically on for teens) and allows users to choose whether sensitive content is shown, blocked or blurred. This can also be changed based on who the media is coming from (friend, others etc.). We would recommend this goes one step further and can also be tuned for individual contacts. This is great practice in prevention of cyberflashing and the same feature could be used to recognise where large amounts of sensitive content are being shared by an individual to take action. Whilst Discord has had this feature for a number of years, we have been surprised at a lack of similar features rolling out elsewhere. Relating to action 7 is the ability to curate audiences. We have seen good practice of this scattered across Meta platforms. On Instagram, users can select a 'Close Friends' list and share certain posts or stories to only this group. Similarly, Facebook allows users to exclude/include specific people from seeing certain posts. These features can be valuable to individuals experiencing online abuse or coercive control who may need to maintain contact with a perpetrator for various reasons. We would be glad to see features like this rolled out into more expansive feature packages, allowing multiple groups (akin to the close friends groups) to be made. Outside of the online safety space, there are other learnings to be had, as an example, the Online Fraud Charter (https://www.gov.uk/government/publications/online-fraud-charter-2023) provided an opportunity for firms to commit to take steps to reduce fraud on their platforms. This is something that could be easily replicated. **Finally, good practice should be recognised from other industries, especially those who have had more experience in becoming a regulated sector, such as the gambling sector,** which has implemented harm-reduction strategies, proactive risk assessments, user protection tools and intervention measures that could serve as a model. As an example, the use of behaviour analytics in this sector to detect patterns of harm which trigger automated interventions. **Another key practice to be taken from this industry is the strong reliance on partnerships with the third-sector to support at-risk users and shape policies**. For example, in this sector operators work closely with organisations such as GamCare and GambleAware as well as self-exclusion schemes. These partnerships ensure that the platforms themselves are not exclusively responsible for user safety but work collaboratively to understand the complex impacts of harm. If this model is taken to the online safety space, platforms could allow victim-survivors to automatically be signposted to specialised support services. **Additionally, gambling companies also fund research and harm reduction initiatives led by NGOs and charities, ensuring that their policy decisions are grounded in expert insights and lived experience** - referring back to an earlier point this helps ensure that consultation is effective, practical and trauma informed. Recognising the work of colleagues across industries and effective initiatives that support victim-survivors of gender-based violence is vital. Homicide reviews consistently emphasise the importance of multi-agency partnerships. These collaborations need to continue to develop and incorporate the substantial role technological platforms may have held within a victim-survivor's life for the future prevention of gender-based harms. Confidential? – N

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 ?	We greatly appreciate that the guidance is not binding and, thus, requires persuasive strategies. We believe the proposed method of a published assessment to review uptake is a smart approach to create accountability and leverage reputational incentives. We encourage Ofcom to name and praise top performers, incentivising their information sharing and success. Tech companies should be fighting to be the leaders in this space. Beyond the 18-month review, we encourage the use of Ofcom's convening power to keep this issue on industry agendas. Regular roundtables and working groups could maintain momentum and making exchanges permanent would allow companies to share best practices and commit to progress. We also recommend that Ofcom publicly track progress in specific areas. For instance, if by the 18-month review, few companies have implemented a recommendation, additional guidance in these areas should be ramped up and consideration given as to whether aspects need to become part of future codes. This work would be complimented by Ofcom establishing manners that will support companies ability to connect with subject-matter-experts. Our view is that transparency and morality will push many to act, but a few may ignore guidance until compelled. Ofcom should be prepared to advocate for change with continued guidance, research publications and ultimately **underscore that this guidance is an expectation**. Without sufficient monitoring and data collection the effectiveness of the proposed guidelines will lack validity. The trickle down effect of establishing initiatives without granular review of practicality, adoption and action would ultimately weigh upon the victim-survivors that require support the most. Highlighting the possibility now that if voluntary uptake is insufficient there might be calls to incorporate some measures into future updates of regulations might encourage proactive adoption. Confidential? –N
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.	Ofcom clearly shows an understanding of awareness of business realities within the assessments. We have no concerns with the impact assessment's methodology or conclusions. We were pleased to see a robust rights assessment which contextualises the guidance as enabling a wider exercise of rights by curbing abuse, but also by giving users more control over their environment. We believe the guidance appropriately covers safeguards for the ECHR and agree that any interference is proportionate. We envision that a criticism for the guidance will be encouragement of "censorship" and would suggest Ofcom consider publishing a summary of the rights assessment in the final guidance's forward to reassure stakeholders that measures have been scrutinized for compliance with rights and found to be justified. We are satisfied that the equality assessment shows due regard to the Equality Act. Safer and more inclusive environments will support other protected and marginalised groups and it was important to us to see that Ofcom considered intersectionality. We agree with this assessment and believe this guidance will advance equality with no negative impact on others. 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	The guidance sets good practice that Welsh-speaking users (and other linguistic minorities) should not be left behind in online safety. We have no concerns that any proposal would treat Welsh speakers less favourably if the guidance was followed. That being said, we recommend that Ofcom continue to engage with Welsh-speaking communities and highlight any specific nuances (such as any lag behind English in automated tooling and Welsh-speaking moderation teams). This would include assurance that any spoken dissemination of the material is cognisant of Welsh regional variations within British Sign Language. Confidential? – N

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.	

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