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

Crest Advisory is a purpose-driven organisation dedicated to improving justice, policing and public safety.

Crest Insights is our think-tank for the whole of the criminal justice system. Our mission is to do the hard thinking which drives policy reform, improves the operating environment for agencies and organisations which deliver policing, justice and public safety and so makes communities safer.

Crest Consulting is our consultancy practice which improves outcomes and performance by quantifying, explaining and solving complex problems for clients across policing, the wider criminal justice system, local and central government and their partners. Much of our learning is informed by our practice with partners who deliver for the public and for victims.

We welcome the opportunity to submit our research and views to strengthen Ofcom's proposals, in order to build a safer online world for women and girls.

This response will draw on the following sources:

- Crest Advisory's nationally representative (on the basis of gender, age, ethnicity and region) Public Attitudes Survey (unpublished) exploring awareness of and attitudes towards deepfakes, commissioned by Office of the Police Chief Scientific Adviser (OPCSA). Data collected in April 2025. Insight is shared with their permission.
    - Due to our study design, it is not appropriate to generalise the results from this survey to the wider population. They do, however, offer useful insights into possible views or patterns that could exist more widely.
- Crest Advisory's rapid evidence review (unpublished) on deepfakes and deepfake VAWG, commissioned by Office of the Police Chief Scientific Adviser (OPCSA). Insight is shared with their permission.
- Crest Advisory and Dame Sara Khan's 'Societal Threats and Declining Democratic Resilience: The New Extremism Landscape' report

Question	Thoughts
Question 1: Do you have any comments on our proposed approach to 'content and activity' which 'disproportionately affects women and girls'?	We welcome Ofcom's focus on content and activity that disproportionately affects women and girls, and recognition that online misogyny, pile-ons and online harassment, online domestic abuse, and image-based sexual abuse are critical areas of focus. We also welcome Ofcom's recognition that these harms are intersectional, and co-occur and overlap both online and offline. Crest Advisory are currently conducting a programme of research on behalf of the Office of the Police Chief Scientific Adviser (OPCSA), examining the impacts of deepfake violence against women and girls (VAWG) on victims to build guidelines for policing. We consider that deepfake intimate image abuse, or deepfake violence against women and girls, should be considered especially relevant to Ofcom's guidance. As part of our research, we have identified that deepfakes have disproportionately impacted women and girls online from their inception. A 2019 report based on analysis of 14,678 deepfake videos across a number of platforms and sites found that 96% were sexual and of women (Deeptrace, 2019). A further 2023 study identified that deepfake pornography makes up 98% of deepfakes online, and 99%

	of those are of women (Security Hero, 2023). Almost all of these are non-consensual. Additionally, we know **that social media and online platforms play an outsized role in facilitating online harms against women and girls.** Our **unpublished nationally representative survey** (n=1700) of those who reported having seen a sexual and/or intimate deepfake of someone they did not know (n=243), found that 56% had seen one on a social media platform, followed by a pornography site (32%), on a messaging platform (18%), in-person (12%), and on a news platform (11%). Of those who reported having seen a sexual and/or intimate deepfake of someone they knew (n=160), 62% had seen one on a social media platform, followed by a messaging platform (30%), a news platform (21%), a pornography site (19%), and in-person (15%). We have identified that deepfakes cut across each of the four areas of focus for Ofcom, and therefore we suggest that they require specific attention. Online misogyny Crest Advisory has supported Dame Sara Khan's landmark review into extremism, examining the current landscape of extremism in the UK. This report identifies online misogyny as a key tenet of extremism, and calls attention to a recent survey of 7,500 adults which found that 15% of women have experienced online violence, 13% of whom say this progressed to offline violence (Deo et al., 2024). It also calls attention to global concerns over the rise in misogyny leading to Like Ofcom's guidance, this report also highlights the rise of misogynistic online influencers such as Andrew Tate, which has contributed to a growing normalisation of harmful attitudes toward women among young men, particularly within schools. A poll of 16-24 year olds found that 45% of young men have a positive view of Tate. Subject matter experts had repeatedly emphasised their concern over the influence of Tate in the context of extremism. For example, algorithms can promote extreme misogynistic content to *"impressionable young men"*, allowing these ideologies to spread (Hornle, 2025). Therefore, we welcome Ofcom's focus on this area in order to protect men from developing harmful views, and from these impacting women and girls. Evidence suggests that there is an explicit link between misogyny and deepfakes – in particular, that intimate deepfakes are deeply rooted in systemic misogyny (Ohman, 2020), and that they also perpetuate gendered violence by objectifying women through a "new voyeurism" (McGlynn & Toparlak, 2024). Instances of deepfake VAWG are therefore regarded by scholars as "inseparable" from systemic misogyny, since they uphold the "cultural scaffolding" which normalises sexual violence against women (McGlynn & Toparlak, 2024, p11). This is of concern to the British public; the Alan Turing Institute and Oxford Internet Institute survey (n = 1400) found that 90.4% of respondents were either very concerned or somewhat concerned about the spread of deepfakes, primarily due to child sexual abuse concerns, followed by distrust in information, manipulating public opinion, and increasing misogyny and online VAWG (Sippy et al, 2024).

Pile-ons and online harassment

Our evidence review has identified that most deepfakes hosted on mainstream sites are of public figures involved in the entertainment industry – in particular, female actresses and singers (Deeptrace, 2019). Increasingly, evidence suggests that female politicians (Waterson, 2024) and journalists (Roberts, 2025) have been targeted in the UK. This exemplifies the dangerous intersection between deepfake VAWG and the use of 'political' deepfakes to spread misinformation and to undermine the legitimacy of public institutions, and women in positions of power.

We also know that the impacts of deepfake VAWG are high. Psychologically, victims report high levels of stress, depression, anxiety, low self-esteem, insecurity, paranoia, obsessive behaviour, and suicidal thoughts (Huber, 2022). They may also report PTSD, depression, anxiety, suicidal ideation (Bates, 2017; Citron, 2019; Deeptrace, 2019; McGlynn et al., 2019,; Powell, et al., 2022), and damage to their sense of self (Clevenger & Navarro, 2021; Jankowicz, 2021).

Beyond the psychological impacts on the victimised individual, there is also research to suggest that there are serious social and professional impacts. Damage or fear of damage to reputation is frequently discussed in literature on deepfake VAWG. Where victims are afraid that family, friends, colleagues, and employers will see deepfake content of them – in particular, sexual deepfakes – they may withdraw from these relationships (Henry et al., 2017). Victims can experience fears about who they can trust, who has seen the deepfake, and paranoia about how the image may spread (Compton & Hunt, 2024). There can also be material repercussions with regards to a victim's job and relationships when family, friends, colleagues, and employers become aware of the deepfake content (Paris & Donovan, 2019).

Another study has identified that image-based sexual abuse causes victims to censor themselves and withdraw from online spaces, which has substantial implications for victims' online citizenship and the digital divide between men and women (Rigotti et al., 2024).

Therefore, **we welcome Ofcom's focus in this area, due to the wide-reaching impacts of online harassment.**

Online domestic abuse

We have not yet received enough evidence to draw a link between deepfakes and online domestic abuse.

Image-based sexual abuse

Deepfakes are a form of image-based sexual abuse, and as such, we also welcome Ofcom's explicit focus on the specific impacts of image-based sexual abuse and other forms of online harms on sex workers. In our research, it is evident that sex workers are substantially impacted by deepfake VAWG. Traditional pornographic deepfakes involve at least two victims, one of whom is likely to be a sex worker and/or performer whose image and likeness has been unconsensually taken for the purposes of victimising another woman (Cole, 2024). Studies involving sex workers and their experiences of deepfake victimisation are scant, and there is a clear evidence gap in this area.

Question 2: Do you have any comments on the nine proposed actions? Please provide evidence to support your answer.	**Action 1:** Ensure that governance and accountability processes address online gender- based harm, for example by consulting subject matter experts and setting policies that prohibit these harms We do not have any comments. **Action 2:** Conduct risk assessments that focus on harms to women and girls, for example by engaging with survivors and victims and conducting user surveys. We support Ofcom's recommendation that companies work to better understand the existing and emerging threats to women online, and that this work be led by the experiences of victims. It is only through direct engagement with victims and survivors and user surveys that the true scale and nature of the problem is revealed. In the wider VAWG space, there has been a concerted effort to create space for victims to lead the conversation around VAWG, influence policy decisions, and inform and run specialist support services. The guidance documents created by domestic abuse charities SafeLives and Women's Aid (2024) highlight best practices for working with victims and reflect the broader shift toward victim-led approaches in the VAWG space. **Action 3:** Be transparent about women and girls' online safety, for example through sharing information about the prevalence of harms on a service and the effectiveness of safety measures. We welcome Ofcom's good practice step on sharing information. However, we would encourage Ofcom to specifically consider how services can engage with policing and the voluntary sector to share this information. We know that victims are likely to take a range of different pathways to support. In our nationally representative survey, of a small group of respondents that said they had been a victim of a sexual and/or intimate deepfake, 51% (n=52) said they reported this to the police, 60% (n=62) contacted a support service or helpline and 61% (n=62) contacted the platform(s) the deepfake was on. We have, however, **identified serious issues regarding a lack of collaboration between technology companies, policing, and support services.** This has material repercussions for victims. One CPWO report has found that there is no established mechanism for reporting and data sharing between online platforms and policing, which makes it difficult for policing to build an accurate picture of the scale of online violence against women and girls (Bakina et al., 2025). This finding is echoed in the 2024 Strategic Threat Risk Assessment, which found gaps in data and information sharing between agencies which limits policing's ability to track online offending behaviour (VKPP, 2024). This was also of critical concern to subject matter experts with whom we consulted.

	Action 4: Conduct abusability evaluations and product testing, for example by using red teaming to identify ways malicious actors may try to use service features to perpetrate harm. In our evidence review, we have identified very little research into the behaviours of perpetrators of deepfake abuse, and there is not yet enough evidence to suggest that the characteristics of perpetrators are similar to that of other crime types such as wider intimate image abuse. This is **likely to obstruct the ability of red teams to understand how to test exploitation of a service**. Our nationally representative survey identified that 5% of respondents (n = 79) had created a deepfake in the past, and 11% (n = 182) indicated that they had not previously created a deepfake but would. Of respondents who had not yet created a deepfake but indicated that they would, 28% (n = 51) wanted to create a sexual or intimate deepfake of someone they know. We r**ecommend that companies stay up to date with emerging research into perpetrators' behaviours and motivations, such as the work of the Open University's Centre for Protecting Women Online**. **Action 5:** Set safer defaults, for example by 'bundling' default settings together to make it easier for women experiencing pile-ons to secure their accounts. We do not have any comments. **Action 6:** Reduce the circulation of online gender-based harm, for example by using hash matching to detect and remove intimate images shared without consent. We do not have any comments. **Action 7:** Give users better control over their experiences, for example by providing the option to block multiple accounts at once. We do not have any comments. **Action 8:** Enable users who experience online gender-based harm to make reports, for example by building reporting systems designed in a way that is supportive and accessible for those experiencing domestic abuse The evidence on victims' experiences of reporting deepfake VAWG, and barriers to reporting, is limited. Our Public Attitudes Survey found that 61% of those who had been a victim of an intimate/sexual deepfake had contacted the platform that the deepfake was on. A 2021 study has further investigated barriers to reporting sexual deepfakes, classifying key barriers as: ● **System barriers,** including perceived gaps in the law and legislative framework for reporting, and jurisdictional challenges

	• **Practical barriers,** such as the onus on victims to produce and procure evidence of deepfake abuse, and to have the content removed (or, in some cases, to keep the content up to support investigations) (Glamour, 2024) and limited police resources • **Other barriers,** including victim-blaming attitudes. It is critical for companies to first understand which barriers victims experience to reporting to their platform, and second, to consider what outcomes victims want after they report or seek support, in order to establish evidence-based benchmarks for the effectiveness of response and create a victim-centred response. **Action 9:** Take appropriate action when online gender-based harm occurs, for example by taking action against users who repeatedly violate the service's policies. We welcome Ofcom's focus on taking action against online gender-based harms. In relation to the good practice steps set out in Action 9, including fact-checking and labelling, our evidence review found that there is mixed evidence on the benefits of an improved ability to identify deepfake content. Some literature calls for the public to improve digital literacy and be educated on how to identify a deepfake in order to discourage consumption (Umbach et al., 2024), or encourage the public to flag the content as deepfake and have it removed. However, other scholars argue that being able to identify an image or video as a deepfake has a minimal impact on the social and psychological effects of deepfake violence against women and girls. Clark & Lewandowsky's (2024) work demonstrates that the harmful influence of deepfakes on people's beliefs and behaviours remains the same regardless of the authenticity of the content. Beyond its use as set out in the guidance to address gendered disinformation, we recommend that Ofcom stay abreast of developments in this field in relation to deepfakes. Additionally, we welcome more specificity in Ofcom's good practice suggestion that services send high risk reports to specialist teams. We implore services to train all moderators to have specialist gender-based online harm awareness. We also strongly recommend that services work with policing where relevant and necessary. **Conclusion** In summary, we support the actions proposed by Ofcom to protect women online and **would welcome more emphasis and specificity around actions which place the responsibility for prevention and intervention on platforms rather than users.** Actions 5 - 9 can help to provide levers for users to take action against online gender-based harm, empowering users to protect themselves. Yet proactive measures from platforms are necessary to disrupt online gender-based harm closer

	to its roots and take a more preventative approach to protecting women and girls online. To illustrate this with the example of deepfake VAWG, a user can flag a deepfake and support its removal from hosting platforms, intervening by preventing further spread and viewership of that image. However, removing the image doesn't guarantee non-repetition of harm because the ecosystem of tools used to create this image remain intact. Our evidence review found that tools to create intimate deepfakes were readily available online, including available open-source code for creating deepfakes and apps marketed explicitly for this purpose (often called 'nudifying' apps). Tackling the ecosystem of tools used to inflict online abuse is vital to protect women online - a responsibility that lies with platforms rather than users.
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.	We do not have any comments.
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	We do not have any comments.

practice' recommendations?	
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.	We do not have any comments.
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.	We do not have any comments.