Ofcom VAWG Guidance Joint Sector Briefing

This briefing outlines the Online VAWG Network's joint response to Ofcom's draft VAWG Guidance. It reflects the key themes and priorities discussed at a purpose held meeting to inform a collective consultation submission to Ofcom.

Our message is clear: **Ofcom must be bolder.** The current guidance falls short in its ambition to prevent online violence against women and girls. We are calling for:

- **Stronger interventions** rooted in prevention and safety by design,
- **Greater transparency and accountability** from tech platforms, and
- **An upgrade of the guidance to a statutory Code of Practice**, to ensure it is enforceable and taken seriously by industry.

We invite organisations across the VAWG sector to endorse this briefing, to help ensure the final guidance reflects the urgency and seriousness of the harms women and girls face online.

Contributing organisations and experts:

End Violence Against Women Coalition (EVAW)

Maeve Walsh, Online Safety Act Network

Professor Lorna Woods, University of Essex

Professor Clare McGlynn, University of Durham

Glitch

Suzy Lamplugh Trust

Refuge

NSPCC

5 Rights Foundation

Zero Tolerance

Institute for Strategic Dialogue

UCL Gender and Tech Research Lab

CEASE UK

Endorsed by:

Welsh Women's Aid

Women's Aid Federation England

Make it Mandatory

White Ribbon UK

Action Breaks Silence

LMK Let Me Know

Birmingham and Solihull Women's Aid

Bold Voices

End Sexism in Schools

IKWRO - Women's Rights Organisation

Rene Cassin

Anawim - Birmingham's Centre for Women

Chayn

Center for Countering Digital Hate (CCDH)

Our Streets Now

Standing Together Against Domestic Abuse

Advance

Solace Women's Aid

IDAS (Independent Domestic Abuse Services)

Plan International UK

Everyone's Invited

Juno Women's Aid

Tender

SafeLives

National aEducation Union (NEU)

Stay Safe East

Respect

This briefing is now closed for sign on

Safety by Design

- Safety by design involves considering safety from the initial product specification and design, through deployment, maintenance, and retirement. While the guidance acknowledges this temporal scope, other aspects like technical scope are not covered robustly enough, including looking beyond just takedown measures to account creation, distribution, and user engagement. **The priority should be to design out risks before relying on mitigation and remediation.**

- Foundational steps in the guidance are linked to compliance with the legally required in Illegal Harms Code and the Children's Code. However, framing these as "foundational steps" could be interpreted as aspirational; **we therefore suggest changing this to "minimum steps" to clearly indicate they are a baseline standard that platforms must meet to be compliant with their duties as set out in the Codes**. The guidance should also more actively encourage platforms to go further to implement “good practice” steps. Case studies on priority offences like intimate image abuse and stalking, currently in the "good practice" section, should be moved to the "minimum steps" section to reflect platforms need to protect users from those priority illegal offences as set out in the Act.

- The guidance does not give sufficient consideration of how **business models themselves can be harmful**, driving design features that disproportionately impact girls beyond just advertising, such as beauty filters. The guidance must also recognise that services may need to **dedicate more resource to trust and safety teams to innovate in protecting women and girls**, especially given a general industry shift away from such resourcing. Additionally, **safety by design needs to be nuanced for age,** exploring whether the safest settings and defaults should be unalterable for the youngest children and considering which features are appropriate for different age groups.

Embedding prevention

- We welcome the systemic understanding of VAWG prevention, and the focus on media literacy and education in Chapter 4. Yet the guidance defers to Ofcom's media literacy

strategy, which is often unclear, lacking measurable impact or resourcing, and not robust enough for the challenging work needed. While the strategy recognises media literacy needs to be for all society, there is a lack of clarity on how this translates into practice.

- **Primary prevention which addresses root causes VAWG, such as gender inequality and cultural attitudes, should also be included in the guidance,** involving actions like deprioritising sexist content and promoting gender equality through algorithms and platform design. The media literacy strategy and the guidance should better speak to each other, with Ofcom taking a more proactive role and ensuring tech companies support these efforts.

Addressing gaps in the guidance

- **Experiences of girls:** There is a stark gap around the experiences of children and girls, who have different experiences of online abuse than women, including specific targeting and interactions with reporting systems, for example the fear of prosecution for self-generated images. The guidance's focus on domestic abuse in relation to adult women overlooks that girls also experience domestic abuse, requiring better age-appropriate language and training. The focus of the guidance primarily on social media also overlooks risks and recommendations specific to gaming sites, which have unique routes for grooming and establishing unequal power dynamics, particularly amongst young people. Child sexual abuse (CSA) should be introduced as a fifth harm category to bring out the nuance of girls' specific experiences of gender-based harm.

- **Intersectionality:** While welcomed, the application of the intersectionality framework needs clarification to ensure it is understood as a framework for accounting for multiple identity grounds in risk assessment, decision-making, and automated detection. Automated tools need more detailed recommendations on how to detect nuanced forms of misogyny and misogynoir, not just extreme hate speech.

- **Stalking/Course of conduct crimes:** Stalking and other course of conduct crimes are not adequately covered by the focus areas, despite being priority illegal harms. Stalking is distinct from domestic abuse or pile ons, yet platforms often misunderstand that the course of conduct is the crime, not necessarily individual incidents. The guidance needs to emphasise the need for information sharing between platforms to help identify patterns of stalking across sites and better link online behaviours to offline risks.

- **Repeat perpetrators:** A common challenge is perpetrators setting up new accounts instantly after one is taken down. The guidance should strongly encourage tech companies to use information like IP addresses to prevent the creation of multiple accounts by known perpetrators.

- **Pornography and AI:** While acknowledging child protection concerns, there's a lack of focus on the broader role of pornography in shaping harmful norms, driving sexual

violence, and legitimising abuse against women and girls. This is relevant not just on dedicated porn sites but increasingly on social media. The guidance should cover all forms of choking and strangulation pornography as well as incest pornography, given the evidence of its link to harmful behaviour and harmful medical impacts. There is also an absence of a dedicated section on nudification apps, their accessibility, and disruption methods, beyond broad mentions of deepfakes. The guidance must go further to address the way algorithms promote harmful behaviours by prioritising these apps.

- **Law enforcement and evidence:** Survivors and police struggle to access data and evidence of online abuse from tech companies. The guidance should recommend timely cooperation with law enforcement (when survivors report) and require platforms to provide survivors with easy access to download records of abuse and reporting actions for evidence.

- **Human rights:** While the VAWG Guidance Annex mentions human rights impacts, it focuses predominantly on platform/perpetrator rights. It should be strengthened to explicitly state how online abuse breaches women's and girls' human rights under Articles 8 (privacy), 10 (freedom of expression), 2 (right to life) and 3 (freedom from torture). Ofcom should elaborate on how it balances conflicting rights, recognising that not all speech is equal, and some speech falls outside protection.

- **Perpetrator invisibility:** The guidance uses passive language that renders the male perpetrator of online VAWG invisible, failing to address the root cause of gender inequality and harmful masculinity. Active language identifying perpetrators and how technology is misused should be used.

<u>Future-proofing the guidance</u>

- Ofcom's guidance must move beyond addressing harm from individual users and instead **recognise the systemic role of platform design in normalising violence against women and girls.** Algorithms on platforms such as TikTok, YouTube and Instagram are not neutral, they actively recommend misogynistic and abusive content. These recommender systems are designed in ways that guide users, particularly boys and young men, down pathways that entrench harmful gender norms and promote misogyny. While the current guidance acknowledges algorithmic risk, **it does not yet go far enough in recognising that algorithmic amplification is itself a harmful activity that drives abuse at scale.**

- **We urge a broader and more inclusive understanding of how technology facilitates abuse.** The term "online domestic abuse" is too narrow and risks excluding harms that occur through connected technologies, including Internet of Things (IoT) devices in the home. We recommend the use of "technology-facilitated abuse" to align with other policy frameworks and better capture the full scope of harm.

- There is a need for recognition of emerging forms of abuse that are not yet fully covered under existing laws or guidance, including non-consensual sexualised use of avatars, abuse in immersive environments such as the Metaverse, and the use of chatbots that replicate misogynistic narratives. Additionally, the surge in deepfake and AI-generated imagery highlights the urgent need for proactive regulation and safety-by-design approaches in new and developing technologies. **The guidance must support forward-looking, flexible measures that can respond to these evolving risks and ensure robust protections are in place from the outset.**

Remit of the Guidance

- The guidance applies to regulated services, but its practical impact is affected by how the underlying legal framework is applied. A key concern is the impact of Ofcom's decision to base service categorisation primarily on size rather than risk. This means some small but risky platforms where high levels of abuse occur may be left out of scope of certain enforceable duties like transparency reporting and user empowerment tools. **There is a risk that focusing only on "in scope" services could lead to a worsening of safety for out-of-scope services**, therefore there is a need for clarity on which services will be assessed for adherence to the guidance.

- Regulated services that outsource functions, including safety measures or content moderation, must not avoid responsibility. **Risk assessments should include risks from business relationships, ensuring vendors adhere to standards and that outsourced user safety tools comply with the Codes.** This is particularly relevant for emerging tech like AI, where components are often outsourced.

Enforcement

- A central issue is the lack of enforceability of the guidance. Despite it containing many positive measures, its non-binding status undermines these. Whilst the guidance is statutory guidance, meaning companies are expected to engage with it and have a reason for not following recommendations, **Ofcom could strengthen its framing to emphasise this legal expectation.**

- There is a need for Ofcom to clarify how they will incentivise and track uptake of the guidance and measure its impact by using their transparency reporting powers, as well as survivor feedback, and an independent audit. **We strongly recommend that the guidance be made into a legally binding Code of Practice to give Ofcom the necessary power to ensure measures are introduced and enforced against companies prioritising profits over safety.** The "foundational steps" should be reframed as "minimum steps" because of their link to enforceable codes, and "good practice" steps should be clearly understood as existing industry standards rather than ambitious stretch targets.