Internet Watch Foundation response to the Protecting Children from Harms Online Consultation

About the Internet Watch Foundation

- The Internet Watch Foundation (IWF) is a charity that works in partnership with the internet industry, law enforcement and government to remove (with the co-operation of industry) from the internet child sexual abuse images and videos wherever they are hosted in the world and non-photographic images hosted in the UK.

- The IWF exists for public benefit and performs two unique functions in the UK:
  1. We provide a secure and anonymous place for the public to report suspected online child sexual abuse images and videos and;
  2. Use the latest technology to search the internet proactively for child sexual abuse images and videos.

- The IWF has a Memorandum of Understanding between the National Police Chiefs' Council (NPCC) and Crown Prosecution Service (CPS) that governs our operations. This ensures our analysts' immunity from prosecution and recognises our role as the "appropriate authority" for the issuing of Notice and Takedown in the UK.

- Operationally, the IWF is independent of the UK government and law enforcement. The IWF also plays a vital role in providing the internet industry with several quality-assured technical services to prevent the spread of known child sexual abuse images and videos online and to stop the uploading of new images in the first place. These include image hashing utilising Microsoft's PhotoDNA, a URL blocking list of live webpages, keywords list, domain alerts, payment brand alerts, newsgroup alerts and simultaneous alerts (for US companies only). Key to this is our trusted relationship with the internet industry, enabling us to act as a broker between them and government and law enforcement.

- In 2020, the Independent Inquiry into Child Sexual Abuse (IICSA) concluded: "*In the UK, the IWF sits at the heart of the national response to combatting the proliferation of indecent images of children. It is an organisation that deserves to be publicly acknowledged as being a vital part of how, and why, comparatively little child sexual abuse material is hosted in the UK*."

- Our work is funded almost entirely by the internet industry: 60% of our funding comes from our 200 global members which include providers of user-to-user services, search providers, Internet Service Providers (ISPs), Mobile Network Operators and manufacturers (MNOs), social media platforms, safety tech providers, content service providers, telecommunications companies, software providers, domain name registries and registrars and those that join the IWF for CSR reasons. Our members include some of the biggest companies in the world – Amazon, Apple, Google, Meta, Microsoft, Snap, X (formerly Twitter), and Discord. We also have the largest ISPs and mobile operators in the UK (BT, Talk-Talk, Sky, Virgin Media, the Internet Service Providers Association) and some of the smaller operators within the internet ecosystem who pay as little as £1,040 per annum yet are still able to access all the technical services and tools we have to offer.

- The IWF is a charity registered in England & Wales with an 11-person Board of Trustees of which, eight are independent members and three are industry representatives. The IWF Hotline 3 is audited by an independent team, led by a High Court judge, every two years and the report are published in full.

Summary

First, we would like to thank Ofcom for presenting the children's consultation to parliamentarians at the All-Party Parliamentary Group on Social Media on the day the draft Codes were launched. We appreciate Ofcom's flexibility and know it was appreciated by the Chair and other members of the group.

We also want to acknowledge the positive steps that have been taken. We are pleased to see Ofcom making progress and appreciate the high level of engagement with children. The combination of age assurance measures and new measures relating to recommender systems represents a significant advancement in protecting children.

Moreover, in comparison to the illegal harms code, the children's consultation is much easier to navigate.

Our response mirrors our submission to Ofcom's illegal harms consultation, as our analysis and feedback remain consistent.

Recommendations

The key recommendations we will highlight in our response are:

- **Reframe the codes to prioritise early-stage prevention and safety by design, applying this approach equally to all user-to-user services, including those offering end-to-end encrypted communications.**
- **Require services to prevent all children, or children in specific age groups, from accessing features or functionalities when risks cannot be sufficiently mitigated.**
- **Add to the Code of Practice a requirement for all services within scope to address harms identified in their risk assessments that result from features and functionalities, using best practices, even if Ofcom has not yet established an evidence base to support these recommendations.**
- **Establish measures to ensure age-appropriate access to content, features, and functionalities, rather than solely focusing on protecting children from 18+ content.**
- **Require services to specify a minimum age requirement in their terms and conditions and enforce it effectively.**
- **Expand guidance on age assurance to include age verification for age-appropriate services in addition to 18+ services**

Feedback

Safety by Design

As highlighted in our previous response, we would like to see a greater emphasis on challenging services to create platforms that are safer by design.

Currently, the Codes are too focused on content, and there needs to be a shift towards consistent, proactive measures to prevent and disrupt harm. As noted by Ofcom in Volume 2(5.20), services prioritising growth often neglect safety measures, making them vulnerable to exploitation by CSEA perpetrators. Therefore, the codes should focus more on early-stage interventions, such as using proactive technologies to detect illegal and harmful content and implementing measures targeting perpetrator behaviour.

A pragmatic, precautionary approach to regulation is essential, focusing on long-term safety by design. This approach should apply equally to all user-to-user services, including those offering end-to-end encrypted communications.

Since private messaging is a primary channel for online grooming, it is crucial to design these communications safely for children. However, because the proposed measures only apply to public spaces, we are concerned that perpetrators will shift their activities to private spaces. Without applying safety by design to all user-to-user communications, this approach does not mitigate the risk but merely changes its location. Steps must be taken to ensure children are protected in private and end-to-end encrypted environments.

In addition to our concerns about end-to-end encrypted environments and private messaging, Volume 3 raises issues regarding audio and live streaming, which are not adequately addressed despite being identified as harmful functionalities in the children's safety duty risk register. Where a risk cannot be sufficiently mitigated, services should prevent all children or children in certain age groups from accessing the relevant features or functionalities.

Safe Harbour Provision

We also want to reaffirm our concerns about the codes being designed as a "safe harbour."

Due to the rules-based nature of these codes, services may abandon existing protective or mitigating measures, assuming they are no longer necessary for compliance. This risks disincentivising good practices and fails to raise the bar for safety and protection. We recommend that Ofcom adds to the Code of Practice a requirement for all services within scope to address harms identified in their risk assessments that result from features and functionalities, using best practices, even if Ofcom has not yet established an evidence base to support these recommendations.

Implementing additional measures not identified by Ofcom could, for example, enhance the detection of previously unidentified CSAM content. This approach would encourage innovation in response to identified risks and support the regulation of emerging technologies like Generative AI and Extended Reality, helping to future-proof the regulation.

Age verification and age assurance

We recognise the limitations of the Online Safety Act, which distinguishes between adults and children by defining a child as anyone under 18.

Based on this definition, the code currently imposes a blanket age restriction for those under 18 and does not require services to provide age-appropriate experiences for different age groups within this range. We are concerned that this one-size-fits-all approach fails to consider the varying needs of children at different stages of development.

We urge that services should be required to specify a minimum age requirement in their terms and conditions and enforce it **effectively**.

The Act emphasises the ‘consistent’ application of age verification rather than its effectiveness. This focus on consistency means that even when services identify significant risks to children, the Codes do not require them to effectively mitigate these risks. The current guidance allows services to document their actions without demonstrating the actual outcomes or changes resulting from those actions.

Code of Practice measures must be outcomes-based, addressing all identified risks of harm to children. Age-appropriate access to content, features, and functionalities should be established, beyond merely protecting children from 18+ content. To address this, we suggest that Ofcom align and expand the definition of a child with the Age Appropriate Design Code[1].

The GDPR and DPA 2018 specify that if you rely on consent for any aspects of your online service, you need to get parental authorisation for children under 13. Since 13 is the age of digital consent, it is crucial to prevent children of this age from accessing inappropriate services and to ensure default privacy settings protect them from grooming. As highlighted in our response to the Illegal Harms Codes, effective age assurance measures are essential for strengthening grooming mitigations. Safety-by-design measures for children's accounts are ineffective if they rely on self-declared ages that can be easily circumvented.

Address all risks

By applying the proposals from the illegal harms consultation to the children's consultation, Ofcom is allowing small companies to avoid removing illegal content and content harmful to children.

To ensure safety by design, the regulation should focus on small but high-risk platforms and ensure Ofcom’s approach to risk assessment includes not just large platforms, where much best practice currently exists, but also medium-sized companies.

The current approach means limiting safety measures to companies with a medium to high risk of CSAM, which is inadequate. A review of the definition of “large platforms” is necessary to capture some of the most popular platforms used by children and ensure medium-sized businesses are also included in training and development requirements for staff. Ofcom must enforce protections on small but high-risk platforms to ensure robust safety measures across all services.

[1] age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf (ico.org.uk) pg. 32-3