IWF
Internet
Watch
Foundation

Working together
to stop child sexual
abuse online

One Step Ahead

A manifesto for tackling child sexual abuse online

Introduction

The internet must be a safer place for children.

Over the past five years, the Internet Watch Foundation (IWF) has removed over one million web pages showing child sexual abuse images and videos. In 2023 alone, we assessed over 390,000 reports and confirmed over 275,000 web pages containing images or videos of children suffering sexual abuse. 2023 was the 'most extreme' year on record, with more Category A child sexual abuse imagery discovered than ever before.

92% of the imagery discovered now shows "self-generated" child abuse where children are being targeted and groomed or coerced into sexual activities via webcams and devices with cameras. **Heartbreakingly, a growing number of these children are aged three to six.**

At the IWF, we work to end child sexual abuse imagery online. For almost 30 years, since the early days of the internet, our job has been to help child victims of sexual abuse by hunting down and removing any online record of the abuse.

During the last Parliament, we along with other child protection charities campaigned and worked with the Government, Parliamentarians, technology companies and law enforcement to pass new legislation to make the UK the safest place in the world to go online. We have made important strides – particularly the Online Safety Act – but there is so much more to be done.

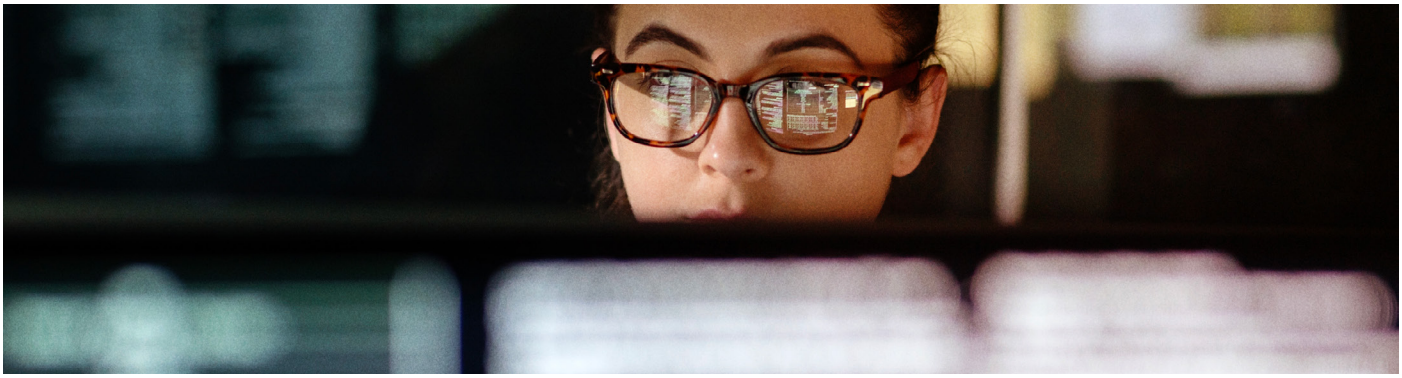
Amid growing new trends – such as the first reports of child sexual abuse material generated by artificial intelligence (AI) – we are calling on this Parliament to help us get One Step Ahead and take the necessary action to tackle child sexual abuse online.

Our Policy priorities

Over the next Parliament, we believe there are five priority actions the Government must take:

- Prevent AI images of child abuse spreading online
- Legislate for age verification to protect children
- Introduce mandatory reporting of suspected child sexual abuse
- Prevent illegal content – before it gets online
- Ensure no hiding place for abusers in encrypted messages

While we must continue to take a whole systems approach to tackling child sexual abuse from education to public health, these are important steps that the Government can deliver to help us get One Step Ahead.



1 Prevent AI images of child abuse spreading online

AI poses one of the biggest threats to online child safety in a generation. It's currently just too easy for criminals to use AI to generate and distribute sexually explicit content of children. To give just one example of the scale of the threat, our analysts detected a total of **20,254 AI-generated images of children posted to just one dark web forum in a one-month period.** Of these, 2,978 were found to be illegal images in line with UK law.

AI's capabilities have far outpaced our laws to the point at which paedophiles can now legally download the tools they need to generate images and can produce as many images as they want – offline, with a high level of anonymity that can be achieved through open-source technology.

Currently, it is not illegal to create and distribute guides on how to use generative AI to create child sexual abuse content; a clear loophole which is enabling the proliferation of child sexual abuse material. Moreover, increasingly AI chatbots are being used to simulate sexual communication with children.

On top of this, most **AI-generated content is now virtually indistinguishable from 'real' content** with text-to-image technology constantly improving posing more challenges to law enforcement agencies, the IWF, and children.

This new Parliament must act to tackle this and bring our laws up to speed for the AI age.

To help us get one step ahead, we need:

- The Ministry of Justice to commission as soon as possible a review of current child sexual abuse material (CSAM) laws to ensure that they are fit for purpose to tackle the threat of AI-generated content. This review should consider:
  - Making it an offence to use, create or share online digital tools which simulate sexual communication with a child.
  - Making "paedophile manuals" and the exchanging of hints and tips related to the creation of AI imagery illegal.
  - Making illegal AI models trained on or fine-tuned with illegal indecent images of children.
  - An extension of the IWF's remit to be able to scrutinise the datasets on which AI technologies are trained.
- Search services to de-index links to fine-tuned AI models known to be linked to the creation of AI CSAM.
- Proper regulatory oversight of AI models before they go to market or are made open-source and ensure appropriate risk mitigation strategies are in place. For closed-source models, protections must be in-built.
- Companies using and developing Generative AI and Large Language Models (LLMs), to place clearly in their terms and conditions that the use of these technologies to generate child sexual abuse material is prohibited.

2 Legislate for age verification to protect children

We're seeing an alarming rise in the number of children using phones and other digital devices to carry out sexual acts in domestic settings. In 2023 alone, we found **2,401** 'self-generated' images and videos of abuse involving children aged between **3 and 6.**

Recent developments such as virtual worlds known as the metaverse have the potential to become a tool for the sexual abuse and exploitation of children. Offenders can hide behind anonymous avatars as users' identities are not verified and **children can access adult-only features simply by ticking a box to declare that they meet the minimum age requirements.**

Under the Online Safety Act, sites and apps that display or publish pornographic content must ensure that children are not normally able to encounter pornography on their service.

To do this, they must introduce 'age assurance' – through age verification, age estimation or a combination of both – which is 'highly effective' at correctly determining whether a user is a child or not. We also believe that on-device protections and advice and age verification at the point of sale are sensible ways of building on existing legislation as part of a "layered" approach to online safety.

Ultimately, we need to ensure children have more age-appropriate experiences online. We need a national debate about what age children access social media. Currently, the UK has adopted the lowest possible age for digital consent at 13 – but it is possible to raise this age and is something to urgently consider.

To help us get one step ahead, we need:

- To raise the legal age that children can access and use social media accounts.
- Telecom providers and device manufacturers to be required to verify the age of their users and issue clear, simple, online safety advice and information about parental controls.
- Ofcom to examine age-gating content and utilise age verification, estimation, and assurance technologies so children can have a tailored experience online - in much the same way they do with broadcasting and film regulation today.

3 Ensure no hiding place for abusers in encrypted messages

Recently, social media companies have announced plans to roll out end-to-end encryption (E2EE) on their messaging services, including Facebook Messenger and Instagram Direct. E2EE overrides controls that help to keep your children safe and potentially poses a huge risk in the distribution and coercion of children to create images of child sexual abuse.

At the moment, social media companies scan their platforms to find and report child sexual abuse material (such as images, videos, and grooming conversations) to law enforcement, so that abusers are arrested, and children are protected.

If E2EE is rolled out more widely without necessary child safety measures, social media companies will no longer be able to find and report child sexual abuse material in the same way - **it will make it harder for social media companies and law enforcement to detect child sex abusers** who are looking to manipulate, groom, and sexually abuse potential victims.

Ultimately, we want an environment where it is simply impossible for adults to communicate with children through E2EE.

We are encouraged that Ofcom's recent illegal harms consultation stated that end-to-end encryption was a clear risk factor for the protection of children and the distribution of child sexual abuse content. But simply more needs to be done to respond to this growing threat.

To help us get one step ahead, we need:

- To raise the age at which children access end-to-end encrypted applications. Should adults want to interact with children on platforms that use E2EE for adult users, they should forgo their right to having their messages E2EE to ensure child safety.
- Ensure Ofcom is making the most of its powers under Section 122 of the Online Safety Act to compel companies to use their best endeavours to prevent images from circulating in E2EE environments.

4 Introduce mandatory reporting of suspected child sexual abuse

The Independent Inquiry into Child Sexual Abuse (IICSA) demonstrated that systemic change is needed to ensure allegations of child sexual abuse are reported. The Inquiry heard of many instances in which children who were being sexually abused made disclosures or presented information to someone within an institution, but no action was taken.

Individuals who failed to report abuse may have failed to meet their professional or moral obligations, but they did not break any laws in doing so.

Several countries – including the majority of Europe, Canada and Australia – have introduced so-called "mandatory reporting" requirements. These place specified persons, or members of the public, under a statutory obligation to report child abuse or neglect to a designated agency.

Across these countries, the introduction of mandatory reporting has led to an increase in the number of referrals made to authorities and in the number of children subsequently identified as needing protection from sexual abuse.

In the last Parliament, the Government accepted this recommendation and intended to enact it through legislation, but agreed with victims' groups and the chair of the IICSA review that more needs to be done now.

To help us get one step ahead, we need:

- A mandatory reporting duty for instances of Child Sexual Abuse. The failure to meet this duty must be a criminal offence, punishable through the court system.
- This must be designed in partnership with those practitioners subject to mandatory reporting to ensure it is effective and does not create unintended consequences.

5 Prevent illegal content – before it gets online

While mandatory reporting is an important step, we must also do more to ensure images of child sexual abuse never reach the internet in the first place.

At the IWF, this goes to the core of what we do. When the IWF was set up in 1996, the UK hosted 18 % of the worldwide total of online child sexual abuse imagery. By 2018, the figure was 0.04 %.

While we are proud of this success story, there is still more to do. As reported by the National Crime Agency and in the IICSA report on the Internet, finding these images on normal search engines is as close as three clicks away.

There have been some significant developments in technology that ensure this content never gets online with industry playing an important role in this effort. This is invaluable but we need to go further.

We are therefore calling for mandatory pre-screening by the industry of content on their platforms or systems. This is backed by not only the NCA but IICSA and other victims' groups.

This should not be a burden on the industry and is well within technical capabilities. The IICSA report, for example, found that while it may provide some challenges for these companies, there is no technological reason why it cannot be achieved. Given how easily and readily available this content is, this is a necessary step we must take.

To help us get one step ahead, we need:

- **Mandatory pre-screening or pre-filtering of known child sexual abuse images** before the material is uploaded. This should be delivered by Ofcom as part of their implementation of the Online Safety Act and their code of practice – but should be legislated for if not enacted.

How you can help

While we have made important strides in the last Parliament – the scale of the challenge is still vast. We need your support to help us get one step ahead with new legislation, regulation and action from the Government.

If you want to help us tackle these issues head-on, we have a separate briefing with draft parliamentary questions, debate titles and Early Day Motions to be tabled in Parliament.

And if you would like a further conversation about how you can support us, please do contact **Bobbie@iwf.org.uk**