

Review of the RSHE statutory guidance: a call for evidence

11 July 2024

Name, position, and contact details of the person responding:

Bobbie Dennis, Policy and Public Affairs Officer, bobbie@iwf.org.uk

1. Background of the Internet Watch Foundation (IWF)

- 1.1. The 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.
- 1.2. The IWF exists for public benefit and performs two unique functions in the UK:
 - We provide a secure and anonymous place for the public to report suspected online child sexual abuse images and videos and;
 - Use the latest technology to search the internet proactively for child sexual abuse images and videos.
- 1.3. 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 immunity from prosecution for our analysts 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.
- 1.4. 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 which enables us to act as a broker between them and government and law enforcement.
- 1.5. Our work is funded almost entirely by the internet industry: 60% of our funding comes from our 200 global Members which include Internet Service Providers (ISPs), search engines, Mobile Network Operators, manufacturers (MNOs), social media platforms, 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 – as well as the largest ISPs and mobile operators in the UK as well as some of the smaller operators within the internet ecosystem who pay as little as £1,040 per annum yet still access everything we have to offer.

- 1.6. 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 is audited by an independent team, led by a judge, every two years and the reports are published in full.
- 1.7. The IWF is distinct and deliberately limited to tackling illegal content, specifically online child sexual abuse material (CSAM) hosted anywhere in the world and non-photographic images of child sexual abuse hosted in the UK. For this reason, our response is specific to this area of expertise.

2. Recommendations

- 2.1. **To promote campaigns, such as ‘[Think before you share](#)’, and tools, like [Report Remove](#), to help young people, parents, and carers understand the issues and warn of the harm that can come from the sharing and soliciting of nude images.**
- 2.2. **To adopt the recommendations made by the Independent Inquiry into Child Sexual Abuse (IICSA) report, including mandatory reporting of suspected child sexual abuse.**
- 2.3. **To recommend that schools communicate the laws about the use of nudification tools in schools to protect children from creating, making, or distributing abusive AI images.**

3. Scale of the problem

- 3.1. The scope of this response is related to our charitable mission, the eradication of child sexual abuse material online. The IWF’s 2023 [Annual Report](#) showed that we assessed **392,665** reports and identified **275,652** webpages, resulting in millions of images and videos of child sexual abuse being removed from the internet in a singular year.
 - 3.2. We know through [Ofsted’s recent review of sexual abuse in schools and colleges](#) that interviews with 900 children and young people, revealed that 90% of girls and 50% of boys had been sent unsolicited photos or videos, and 92% of girls and 74% of boys had endured sexist name calling. This included being shown pornographic content and was typically found on platforms such as WhatsApp and Snapchat. Other forms of peer-on-peer abuse could include, upskirting, sexting and “youth produced imagery”.
 - 3.3. Self-generated child sexual abuse images now account for 92% of the content that the IWF is removing from the internet. We are extremely concerned at how “normal” the exchange of these images has become online.
 - 3.4. The IWF has witnessed with horror how children at younger and younger ages are appearing increasingly in the material we remove from the internet. This includes 11–13-year-old girls appearing most prevalently in child sexual abuse content.
 - 3.5. The IWF has continued to observe an increase in the proportion of this type of imagery including children aged 7-10 in 2023, up 65% from 2022 (104,282 in 2023 vs 63,057 in 2022).
- Of the 275,652 webpages actioned during 2023, more than nine in 10 (254,071 or 92%) were assessed as containing ‘self-generated’ imagery.

- This is a 14 percentage point proportional increase on 2022 when 78% of actioned reports (or 199,363) were ‘self-generated’.
 - This represents a 27% increase in ‘self-generated’ reports from 2022 to 2023 in terms of the number of actioned webpages.
- 3.6. In April 2024, the National Crime Agency [sent an alert to schools](#) to warn pupils against the dangers of sextortion, a form of blackmail involving threats that intimate pictures will be shared. [The BBC has also reported](#) on the sad case of Jenn Buta’s son, Jordan, who died by suicide after being targeted by scammers who lured him into sending them explicit images of himself and then tried to blackmail him. Jordan’s tragic story has become a touch point in the fight against the growing problem of sextortion.
- 3.7. 7–11-year olds now account for the first growing age range and horrific new trends of criminal gangs attempting to “sextort” boys into exchanging their imagery and then seeking financial payments through their threat to share those images with people the child knows.

4. IWF campaigns and tools

‘Think before you share’

- 4.1. The IWF has recently launched a new nationwide [campaign](#) which aims to help open a dialogue between parents and teens amid warnings the sharing and soliciting of nudes is becoming “normalised” among young people.
- 4.2. The IWF launched the campaign in response to the increasing proliferation of imagery which has been captured on a device by the child or young person themselves. Most of this so-called self-generated child sexual abuse imagery discovered by the IWF features girls aged 11 to 13.
- 4.3. These images and videos can quickly get out of hand and can even end up being shared by strangers on dedicated child sexual abuse websites. It comes amid warnings that sending and soliciting nudes is becoming “normalised” in UK schools.
- 4.4. The campaign, called ‘*Think before you share*’, warns young people about the pitfalls of sharing their own and others’ explicit images and is supported by [new research](#) from the International Policing and Public Protection Research Institute (IPPPRI - formerly PIER – Policing Institute for the Eastern Region), will help young people, parents, and teachers to “talk about it”.
- 4.5. The research warns that the taking and sharing of nudes has become normalised among young people in schools and that in some cases groups of pupils, mainly boys, are engaging in a “football card collection culture” of nudes of their female peers. IPPPRI also warns that pupils are being exposed to unsolicited “dick pics” online on a “very regular basis”.
- 4.6. The IWF’s campaign will help young people understand the issues and warn of the harm that can come from this imagery being shared. It will also offer help for parents in broaching this difficult topic, and assistance for anyone having imagery used against

them in a range of situations, including sexually coerced extortion, or sextortion, attacks.

Home Truths

- 4.7. In 2022, the IWF developed a campaign to build resilience to the threat of self-generated sexual abuse of children to reduce the number of incidences.
- 4.8. The campaign, backed by the UK Home Office, Microsoft, TikTok and supported by Snapchat and Twitter aimed to empower young people and warn their parents and carers about the risks posed by online predators targeting children.
- 4.9. The purpose of the campaign was for young people to have an increased awareness of how to safely respond to requests online for self-generated child sexual abuse material; and for parents and carers to have an increased awareness of this crime and feel motivated and equipped to protect their children.
- 4.10. Home Truths targeted parents and urged them to T.A.L.K. to their child:
- **T**alk to your child about online sexual abuse.
 - **A**gree digital boundaries.
 - **L**earn about online platforms your child loves.
 - **K**now how to use tools and safety settings.
- 4.11. Now in its fifth iteration, the campaign has been evaluated to show it successfully encourages conversations in the family home and amongst the public about the scale of child sexual abuse.
- 4.12. The campaign aimed at young people received 50.96 million views and won the Purpose Driven Communications Award at the Digital Communications Awards in 2021.
- 4.13. The campaign aimed at adults has received 9.5 million views.

Gurls Out Loud

- 4.14. We also ran another strand called Gurls Out Loud which aimed to build young girls' resilience to help them spot the signs of grooming or coercion. The main message was to block, report, and tell someone you trust. Key Conclusions from the campaign evaluation found:
- Around 1 in 4 girls have been affected by the issue, either knowing someone who has received a request for a nude or themselves receiving a message that made them feel uncomfortable.
 - One good quality conversation about online grooming can make all the difference to both parents/carers and daughters – daughters who had been spoken to were more open to the possibility of their parents talking to them again.
 - Girls who saw the campaign were more likely (than those who had not) to react positively to the thought of a conversation with their parents about self-generated online child sexual abuse.
 - Parents are more likely to speak to their daughters about grooming and online sexual abuse if they have knowledge of the issue

Report Remove

- 4.15. To support young people to remove sexual images of themselves online, the IWF and NSPCC developed the [Report Remove](#) tool, in partnership with age verification app, [Yoti](#). Report Remove can support a young person in reporting sexual images or videos shared online and enables them to get the image removed if it is illegal.
- 4.16. The NSPCC's Childline service ensures that the young person is safeguarded throughout the process and the IWF assesses the images:
- Young people aged 13+ can choose to prove their age using the age verification app Yoti, to help get the content removed from even more places. They will need some ID if they want to do this.
 - Log into or create a Childline account so they can receive updates on their report, which allows them to be safeguarded and supported throughout the process.
 - Young people are then taken to our dedicated IWF portal where they can securely upload images, videos or URLs (website addresses.)
 - Our IWF analysts assess the reported content and take action if it meets the threshold of illegality*. The content is given a unique digital fingerprint which is then shared with internet companies to help prevent the imagery from being uploaded or redistributed online.
 - The outcome will be conveyed to Childline who will then contact the young person via their Childline account to keep them updated and offer further support.
- 4.17. This solution provides a child-centered approach to image removal which can be done entirely online. The young person does not need to tell anyone who they are (their ID is not linked to their report), they can make the report at any time, and further information and support are always available from the Childline website.
- 4.18. Each hash is tagged as originating from 'Report Remove'. This ensures that law enforcement bodies are aware that this is a self-referred image, plus the NCA can assess whether any further action is needed.
- 4.19. As the Report Remove tool develops, we hope it may be possible to gain further information on those images that are at the lower end of the severity grading to see how this process and the laws surrounding it could be improved to better protect children.

5. Independent Inquiry into Child Sexual Abuse (IICSA)

- 5.1. The IWF welcomes recommendations made by the [IICSA report](#), including mandatory reporting of suspected child sexual abuse.
- 5.2. The IICSA inquiry's investigations have 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 to inform the relevant authorities.

- 5.3. Individuals who failed to report abuse to the police or social services in these and other examples may have failed to meet their professional or moral obligations, but they did not break any laws in doing so.
- 5.4. Commonly referred to as ‘mandatory reporting’, numerous countries have introduced legislation which places specified persons, or members of the public, under a statutory obligation to report child abuse or neglect to a designated agency. This includes the majority of countries in Europe and some parts of the US, Canada and [Australia](#).
- 5.5. The introduction of mandatory reporting in other jurisdictions has led to an increase in the number of referrals made about child abuse to authorities and in the number of children subsequently identified as being in need of protection from sexual abuse.
- 5.6. [Similar long-term improvements have been observed in Canada](#) in the identification of children who were in need of protection and received support, as a result of mandatory reporting.
- 5.7. The report also highlights the importance of Report Remove, an online tool launched in 2021 by the IWF and Childline which allows children and young people to report sexual images and videos of themselves.
- 5.8. The report reads: “Given the growth in self-generated imagery, Report Remove is likely to become an increasingly useful tool to help prevent children being harmed by the knowledge that an image of them is available online to be viewed and shared with others.”

6. Artificial Intelligence (AI)

- 6.1. In June 2023, the IWF started receiving its first reports from members of the public concerned that the content they may be seeing online were indecent images of children that had been created using Artificial Intelligence. In a five-week period, our hotline received 29 reports of suspected AI-generated child sexual abuse imagery and was able to confirm that 7 webpages contained criminal imagery.
- 6.2. Of the material we assessed and removed in that period, we found Category A and B material as defined by the UK Sentencing Council Guidelines of 2014, with the children in those images being depicted as young as the ages of 3-6 years old. Our analysts also discovered material where offenders were helping each other refine their prompts to train AI to return more realistic imagery.
- 6.3. In the past year, the technology used to create AI-generated images, based on user text inputs or prompts (text-to-image-based models), has developed astounding accuracy levels. A year ago, it would have been easy for our analysts to distinguish between an image that had been generated using AI or was computer generated compared with an image which had not. By June, this was clearly becoming more difficult for our analysts, with often the only tells in the images we were receiving being the children in the images only having three toes, the fingers or hands not being quite the way you would expect, or beds blurring into the background in photos. In the last six months, many of these imperfections have been corrected, meaning it is now challenging to tell the difference between a real child and one generated using AI, which presents clear challenges for law enforcement and victim identification.

- 6.4. Concerned by this trend we were seeing among the public, the IWF [published a complete report](#) on how AI is being used to create CSAM. In one month, between September and October 2023, we discovered that 20,254 AI-generated images had been posted in just one dark web forum. Of those images, we were able to discount around 9,000 images as not being criminal and we decided to take a closer look at 11,108- that we deemed most likely to be criminal as defined by either the Protection of Children Act (1978) or the Coroners and Justice Act (2009).
- 6.5. Of the 11,108 images we selected for assessment by our analysts, 2,978 were confirmed as being child sexual abuse. 2,562 of these images were assessed as criminal pseudo photographs and 416 as criminal prohibited images.
- 6.6. This research demonstrates this is not a hypothetical issue, but one that has real-world implications and is already causing issues relating to the safeguarding of children today. We would argue that Generative AI is very much a risk that requires oversight if the problem is not to get any worse.
- 6.7. There is [further evidence](#) that these images are causing real-world harm as the BBC has reported from Spain, where 20 girls between the ages of 11 and 17 had become victims of having their fully-clothed imagery manipulated to depict them without their clothes on, with the police investigating 11 boys for sharing the images within WhatsApp and Telegram groups. Recent cases in the [United States](#) and [Australia](#) demonstrate the global nature of AI image abuse. Our UK Safer Internet Colleagues, SWGfL, have identified this as an issue also now affecting schools in the UK. We believe that many children do not know that using nudifying tools of their peers would be creating, making, and then distributing offences under the Protection of Children Act (1978).
- 6.8. We recommend that schools communicate the laws about the use of nudification tools in schools to protect children from using or distributing abusive AI images.