

Briefing from the Internet Watch Foundation (IWF)

Westminster Hall Debate for Tuesday 12 November, 16:00-16:30: 'Tackling Image-Based Abuse'

Key Asks:

- 1. To highlight the growing threat of child sexual abuse online, referencing the latest statistics published by the Internet Watch Foundation (IWF).**
- 2. Ensure that child sexual abuse laws are updated in line with emerging harms, to prevent AI technology being exploited to create child sexual abuse imagery.**
- 3. Raising awareness of child sexual abuse online, how to report it and how it can be prevented.**

About the Internet Watch Foundation

The [Internet Watch Foundation](#) (IWF) is the official UK hotline for assessing and removing child sexual abuse material from the internet.

The IWF works closely in partnership with the internet industry, law enforcement, and governments globally to stop the repeated victimisation of people abused in childhood and make the internet a safer place, by detecting, removing and blocking illegal online child sexual abuse imagery.

The scale of online child sexual abuse

To give you an idea of the scale of the problem, last year the Internet Watch Foundation (IWF) assessed over 390,000 reports and **confirmed over 275,000 web pages containing images or videos of children suffering sexual abuse**, with each page containing hundreds, if not thousands, of indecent images of children.

The IWF report that [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 showed "self-generated"](#) child abuse where children are groomed or coerced into sexual activities via webcams and devices with cameras.

For the first time, the IWF encountered and analysed over [2,400 images of sexual abuse involving children aged 3 to 6](#). Of these images, 91% were of girls and mainly in domestic settings such as bedrooms and bathrooms. The abuse, which analysts have seen ranging from sexual posing to sadism, degradation, and even sexual acts with animals is directed by perpetrators and often recorded without the child's knowledge.

AI-generated child sexual abuse material

Artificial intelligence (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.

In October 2023, [the IWF revealed](#) the presence of **3,000 AI-generated child sexual abuse imaged on one dark web forum**.

Since then, the issue has escalated and continues to evolve. **In the past six months alone, analysts at IWF have seen a 6% increase in confirmed reports containing AI-generated child sexual abuse material, compared with the preceding 12 months.** Almost all of the content (99%) was found on publicly available areas of the internet and was not hidden on the dark web.

The creation and distribution of AI generated child sexual abuse is already an offence under UK law. However, 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.

Case Study: On 12 February 2024, the IWF downloaded a text only manual from a public report it had received. The manual was over **210 pages long** and contained detailed information and instructions on how to use specific devices, apps, and websites to extort images and videos from teenagers and protect themselves from detection.

The manual detailed how to make initial requests for imagery, and then exploit AI technology to 'nudify' the image. The manipulated image could then be used against the child to blackmail them into sending more graphic content.

This is the first evidence we have seen that perpetrators are advising and encouraging each

Action needed to tackle AI generated CSAM

The IWF is calling on legislators across the world, including the UK Government, to ensure that child sexual abuse laws are updated in line with emerging harms, to prevent AI technology from being exploited to create child sexual abuse material.

Tech companies must also prioritise the protection of children and the prevention of AI abuse imagery above any thought of profit, such as through rigorous model testing and safety by design, to minimise harm.

Further action by Government is also needed to tackle the escalating crisis of child sexual abuse online. Recommendations for the UK Government:

1. Introduce legislation to criminalise the possession and distribution of manuals which exchange hints and tips on how to utilise generative AI tools to create child sexual abuse material.

2. Make it an offence to own or possess digital models or files that facilitate the creation of AI or computer-generated child sexual abuse material.
3. Legislate to tackle the rise in generative AI chatbots which simulate the offence of sexual communication with a child.
4. Prevent nudifying technology from being available to UK based users and encourage other Governments globally to take similar measures.

Sextortion

In August 2024, we released [new data](#) highlighting an exponential rise in sexual extortion – known as sextortion - scams. In the first six months of this year alone, reports of child sexual abuse linked to sexual extortion increased by 19% compared to the same period in 2023.

[Boys are targeted most often in the reports](#) received by the IWF (91%), with analysts frequently seeing evidence of boys being blackmailed by criminals looking to extort money. Three in five (60%) reports involved 16 and 17-year-olds.

Case Study: Just last month, [catfish paedophile Alexander McCartney from Northern Ireland was given a life sentence with a minimum of 20 years in jail](#). Operating mainly on Snapchat while pretending to be a young girl, McCartney found and befriended girls all over the world. He used flattery to get a compromising photograph and then used it to blackmail and threaten the children into committing appalling acts or he would publish the images online.

He admitted 185 charges, including the manslaughter of 12-year-old Cimarron Thomas, who took her own life in May 2018.

Supporting young people to take down nude images shared online: Report Remove

Most of the sexual extortion reports (93%) seen by the IWF come through the [Report Remove](#) service run jointly by the IWF and Childline. The first-of-its-kind service empowers children in the UK to have sexual images of themselves removed from the internet, and provides support and counselling if requested.

Since Report Remove was first piloted in 2019, the IWF has removed 1,395 images and videos reported by young people from the internet.

Recommendations

We are calling on the Government to commission activities and campaigns aimed at raising awareness of child sexual abuse online, how to report it and how it can be prevented.

- The IWF's [T.A.L.K](#) campaign aims to empower young people and warn their parents and carers about the risks posed by online predators targeting children.
- The IWF's [Think Before You Share](#) campaign aims to help young people understand the harm of sharing explicit imagery online and encourage parents and educators to start conversations.