# IWF response to Scottish Parliament’s Criminal Justice Committee

**Organisation responding:** The Internet Watch Foundation (IWF)

**Address:** Internet Watch Foundation, Discovery House, Chivers Way, Vision Park, Histon, Cambridge, CB24 9ZR, UK

**Contact details of person responding:** Michael Tunks, Senior Policy and Public Affairs Manager, mike@iwf.org.uk 07377449342

## About the Internet Watch Foundation

* 1. The IWF is a UK charity that works in partnership with the internet industry, law enforcement and government to remove from the internet (with the co-operation of industry) child sexual abuse images and videos wherever they are hosted in the world and non-photographic images[[1]](#footnote-1) of child sexual abuse hosted in the UK.
	2. In addition, the IWF has established reporting portals – places to report online child sexual abuse imagery anonymously and safely – in 49 countries around the world, serving 2.5 billion people.
	3. There is a [Memorandum of Understanding](https://www.iwf.org.uk/sites/default/files/inline-files/CPS%20ACPO%20S46%20MoU%202014%202.pdf) 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 Takedown Notices in the UK. Operationally, we are independent of UK Government and law enforcement but work closely with both.
	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 upload of 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.
	5. Our work is funded almost entirely by the internet industry: 90% of our funding comes from our members with the remaining 10% of our funding applying to our role as part of the UK Safer Internet Centre, coming from Nominet, who are a world leading domain name registry based in the UK and responsible for administering the .UK domain.
	6. The IWF has previously received additional Government funding for specific projects and is open to further diversifying its funding mix in the future.
	7. We are 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](https://www.iwf.org.uk/what-we-do/who-we-are/governance) biennially by an independent team, led by a family court judge, and the report published in full.

## Recommendations

2.1. That the Scottish Government works with the UK Government before seeking any amendments to Part 2 Schedule 6 of the Online Safety Bill to ensure that any amendments made are consistent with England, Wales, and Northern Ireland so that a consistent approach with how the four nations deal with CSE/A online can be maintained.

2.2. That the Scottish Government invests in preventative activity alongside the UK Government’s Online Safety Bill, that seeks to address both demand for Child Sexual Abuse Images online and prevent them from being generated and appearing online in the first place.

2.3. Encourages the Scottish Government to continue and further extend its support for the IWF. By both supporting the potential role it could play as co-designated regulator for CSE/A in discussions with UK Government and by encouraging Education Scotland to become IWF Members.

## Summary

3.1. The IWF has removed an increasing amount of Child Sexual Abuse Material from the internet over the last 25 years since we were founded. In 2021, we processed more reports than the entire first 15 years we were in existence and saw a **64%** increase in the amount of content we actioned compared with 2020.

3.2. The IWF is extremely concerned about the rise of self-generated Child Sexual Abuse Material, up **374%** in the last two years, and that this appears to be disproportionately affecting young girls.

3.3. Whilst the UK has a good track record on not hosting this content, it is concerning **that 550,000 to 8500,000** people pose a sexual threat to children in the UK.

3.4. The IWF has run several public awareness campaigns to raise awareness of these issues and we continue to play our part in the UK Safer Internet Centre and by running Safer Internet Day in the UK with the support of the Scottish Government every year.

3.5. Significant challenges remain, however, in how we improve online safety in Scotland and the UK. We welcome the UK Government’s forthcoming Online Safety Bill and acknowledge that the Bill does give Scottish Ministers some freedom to introduce new definitions of CSE/A. As the UK hotline, we want to ensure that there is consistency in how we deal with CSE/A online because companies deploy our services not only in the UK, but globally, there is a need to ensure that these services are able to interact with not only UK but global standards too. The IWF does, however, remain open to improving the response to this threat online.

3.6. We remain concerned about the increasingly encrypted nature of the internet and in particular, the challenges End-to-End Encryption brings for child protection online and the complex international nature of this crime.

3.7. We believe the UK Government’s forthcoming Online Safety Bill should build on best practice and strike a delicate balance in ensuring we do not push internet users into darker more complex online spaces to regulate.

3.8. We also believe that the Online Safety Bill will need other measures to complement it, including a much greater emphasis on prevention and ensuring that we prevent the generation of these images in the first place and prevent their circulation. This will also require us to address the issue of the large volumes of people who pose a sexual threat to children in the UK.

## Scale and Nature of the CSE/A Threat

4.1. The IWF has just marked 25 years as a charity dealing with Child Sexual Abuse Material (CSAM) Online. Over that period, we have assessed **1.8 million** reports and actioned **970,000** reports for removal. Each of these reports can contain from one to thousands of individual images, meaning we have removed millions of child sexual abuse images and videos from the internet in the past 25 years.

4.2. In 2021, we investigated more reports of suspected child sexual abuse imagery than the entire first 15 years we were in existence. In the period 1996-2011 we assessed 335,558 reports and in 2021, we investigated **361,000** reports including from members of the public and our analysts own proactive searches. Of these reports, the IWF confirmed **252,000** reports as containing Child Sexual Abuse Material and the number of reports we actioned for removal in 2021, had increased by **64%** on 2020’s figures. We have also witnessed over the past decade a worrying increase in the number of Girls appearing in these images. Ten years ago, Girls appeared in 67% of the imagery we removed, in 2021, it was **97%.**

4.3. Another concerning trend seen in our data over the last two years has been the rise in what we call “self-generated” indecent images of children. This is imagery that has been produced by children themselves via webcam and then uploaded, shared, or streamed online. Compared with our 2019 statistics we have witnessed a **374%** rise in this type of imagery, with the **11-13 age range of young girls** appearing most in this type of imagery.

4.4. In 2021, **147,900** reports contained self-generated indecent images of children, and this now equates for **59%** of all the reports we actioned. Concerningly, we also saw a three-fold increase amongst **7–10-year-olds** in the last year. In 2020, we saw 8,000 instances of self-generated child sexual abuse material in this age range and in 2021, this had increased to **27,000** a **235%** increase.

4.5. The National Crime Agency’s recent Strategic Threat Assessment for 2021[[2]](#footnote-2), estimates that as many as **550,000-850,000** people in the UK pose varying degrees of risk to children either online or offline. Their assessment also states that the Covid-19 pandemic and associated restrictions triggered temporary and permanent changes to the offending landscape.

4.6. Despite the concerning figures relating to the scale and nature of the threat, both in the generation of the imagery and the demand for the imagery online, the UK continues to have a robust response to this threat. In 1996, the year the IWF was founded, **18%** of the world’s known Child Sexual Abuse Material was hosted in the UK. Today, that is less than **1%** and has been ever since 2003, thanks to the partnership approach that is taken between industry, civil society, Government and Law Enforcement.

4.7. **25 companies** in the UK were responsible for hosting Child Sexual Abuse Material in 2021 and **67 notice and takedown** requests relating to **350 webpages** were sent to these companies in 2021. Only 1 of these 25 companies was an IWF member.

4.8. The problem of where these images are hosted is largely an extraterritorial one. In 2021, we found **72%** of the content we actioned for removal was hosted in Europe (including Russia and Turkey) with the Netherlands responsible for **41%** of that content.

4.9. This imagery is often harvested from its original upload locations and then discovered by our analysts on image hosting boards and cyberlockers which account for **73%** and **10%** of the CSAM we removed from the internet respectively.

4.10. An image hosting board lets users upload images which are then available through a unique URL (webpage). These URLs can be made into online links, or be embedded into other websites, forums, and social networking sites.

4.11. A cyberlocker is a file hosting service, cloud storage service or online storage provider. They are internet hosting services designed specifically to host users’ files.

4.12. It is important to recognise, that there is no one single entity that can give you a true understanding of the scale and nature of the CSE/A threat online. It would be impossible for us to estimate how many images are in circulation, but we believe that there are two conclusions we can draw from the figures we have outlined above about the scale and nature of CSE/A.

4.13. Firstly, over the past 25 years, the IWF, our industry partners and law enforcement have taken strides forward in the detection of this imagery. The creation of PhotoDNA in 2009 has enabled us to revolutionise our response to this issue and enabled us to create digital fingerprints (Hashes) of known child sexual abuse images that can be shared with companies to help them detect and prevent the upload of known material to their platforms. This is particularly important as victims of CSAM face the traumatic scenario of their images being reuploaded to the internet again and again. Hash technology can stop this. Our image hash list now contains more than **1 million** **unique hashes** which we share with our industry members. Our webpage blocking list (around 8,000-12,000URLS) deployed by our members, blocked at least **8.8 million** attempts from UK users to access known child sexual abuse material in the UK across three ISPs in one month in April 2020. We have all invested in more staff, technology, and tools to better detect this imagery and that can be one of the factors behind the rise in these numbers.

4.14. Secondly, however, and sadly, there is probably more content out there for us to find. Social Media has accelerated our use of digital technologies and its ubiquitous use amongst children and young people has undoubtedly enhanced and enriched their lives, but also bought with it significant challenges and risk of harm. Ofcom’s Media Use and Attitudes report 2022, states that nearly all children (99%) went online in 2021 with the majority using a phone (72%) or tablet (69%) to do so. Their research also concluded 60% of children aged 8-11 had a social media profile, despite the minimum age being 13.

## CSE/A definitions

5.1. Each individual report the IWF receives is assessed by one of our highly trained analysts. All our analysts complete a rigorous training and assessment process before they can assess any imagery and receive both in-house IWF training and, in addition, training from the National 5.2. Crime Agency to be certified assessors as part of the Child Abuse Image Database (CAID). Their assessment and judgments are trusted by law enforcement and the industry all over the world.

5.3. The key pieces of legislation used to govern our operations are listed on the IWF’s website.[[3]](#footnote-3) Perhaps the most important are the Protection of Children Act (1978) and the Sexual Offences Act (2003), that both apply in England and Wales and of relevance to this Committee is the Civic Government Act (1982) and the Protection of Children and Prevention of Sexual Offences Act (2005) as these apply in Scotland.

5.4. The Protection of Children Act (1978) and Civic Government Act (1982) creates the offence in law to take, make, distribute, or possess indecent images of children. The Sexual Offences Act (2003) and Protection of Children and Prevention of Sexual Offences Act (2005) sought to modernise the 1978 and 1982 legislation creating new legal offences, such as sexual communication with a child for example, but is also of importance to the IWF as linked to Section 46 of the Sexual Offences Act (2003) is our Memorandum of Understanding with law enforcement which permits our analysts to carry out their duties whilst being protected from prosecution and recognises our role as the relevant authority for the reporting, assessment and removal of child sexual abuse imagery in the UK.

5.5. As we may also issue Notice and Takedown to companies who have hosting services based in Scotland, we have also sought clarity from the Crown Office and Prosecutor Fiscal Service that if we were to issue a notice to someone working in Scotland that they would not be prosecuted when acting in a professional capacity to remove CSAM. A letter[[4]](#footnote-4) published on our website provides that clarity.

5.6. The IWF assesses Child Sexual Abuse Material according to the criteria and assessment levels set out in the Sentencing Council’s: Sexual Offences Definitive Guideline (2014)[[5]](#footnote-5)

5.7. The Indecent Photographs of children section (page 34) outlines the different categories of child sexual abuse material:

**Category A**: Images involving penetrative sexual activity; images involving sexual activity with an animal or sadism.

**Category B**: Images involving non-penetrative sexual activity.

**Category C**: Other indecent images not falling within categories A or B.

5.8. This categorisation of content is of vital importance as any images identified by our analysts as being confirmed as Child Sexual Abuse Material will be graded and added to the national policing database (CAID) and could therefore be used in criminal prosecutions against people caught in possession of these images.

5.9. Before the IWF can issue a Notice and Takedown for the content, we must check with the National Crime Agency CEOP referrals bureau that to remove the content wouldn’t disrupt any ongoing police investigation. In most cases we receive permission to remove the imagery and that then enables the IWF to issue a notice and takedown request to the host of that imagery. The IWF has some of the fastest removal times anywhere in the world, thanks to our strong, collaborative relationship with UK industry, with our record for removing this content being **2 minutes** with **35%** of the content we actioned for removal in 2021, being removed **in under 2 hours** from the notice being issued.

5.10. The IWF is the only non- law enforcement agency with a connection to policing’s Child Abuse Image Database (CAID). Any imagery we assess as illegal we add CAID and we are currently assessing 2 million Category A and B images from CAID to pass on to the internet industry, so that they can prevent the upload of these images and their distribution online.

5.11. Under the proposals in the UK Government’s forthcoming Online Safety Bill, Scottish Ministers will have the power (by way of regulations) amend Part 2 Schedule 6 of the Bill which relates to Child Sexual Exploitation and Abuse Offences. We would encourage Scottish Ministers to have conversations with UK Government before amending this schedule to ensure that there is consistency in the way that online child sexual abuse offences are regulated and dealt with under the law, particularly as this will have an impact on how IWF removes content hosted in Scotland.

## Education, Awareness, and support

6.1. As stated earlier in this submission, one of the most concerning pieces of data from our recent statistics in the past two years has been the rise in “self-generated” indecent images of children appearing online. We have seen a **374% rise** in this content over the past two years and it mainly involves **11–13-year-old girls** and we have seen in 2021 an increase in younger children appearing in this imagery too**.**

6.2. In 2020, the IWF commissioned Zinc Network to work with us to create two public awareness campaigns to raise awareness and build resilience to the threat of self-generated Child Sexual Abuse Material online.

6.3. One campaign was aimed at parents and carers and was deliberately designed to shock parents about the scale and extent of child sexual abuse imagery online. The campaign’s video used data from the National Crime Agency about the number of people in the UK that pose a sexual threat to children and encouraged parents to ensure they knew what their child was doing online in their homes and bedrooms, where parents thought they would be safe, to ensure that their home wasn’t “an open front door to child sexual abusers.” The campaign encouraged parents to TALK to their child about the issue of child sexual abuse online and how to stay safe online and had a dedicated website with a guide for parents and carers to provide information and support about how to have these conversations with your child.

**T-** Talk to your child about online Child Sexual Abuse

**A-** Agree ground rules about the way you use technology as a family

**L-** Learn about the platforms and apps your child loves and take an interest in their online lives

**K-** Know how to use tools, apps and settings that can help keep your child safe online.

More information about the T.A.L.K. campaign can be found on the campaign website[[6]](#footnote-6) and the video designed to inform parents of the campaign can also be watched [here.](https://www.youtube.com/watch?v=OlCELNnd98o) The parents campaign was distributed on Facebook, You Tube, Twitter and Google.

6.4. The second campaign was aimed at children and specifically 11-13-year-old-girls. The aim of this campaign was to raise awareness of grooming techniques used online, understand the different stats, facts and definitions of this issue and know what to do in the event of them receiving unwanted advances online.

The aims of the campaign were to get girls to:

* Think that inappropriate requests and messages for sexual content are not normal; they’re abuse and a violation of their online spaces
* Feel outraged and motivated to keep their online space safe
* Not respond to inappropriate messages and requests, to block and report and tell someone they trust

6.5. The girls’ campaign was distributed on Snapchat, Instagram, Tik Tok, Google and You Tube which consisted of graphics with key statistics, facts and definitions and included a manifesto film and influencer films. The Girls campaign video can be viewed [here](https://www.youtube.com/watch?v=HcwP6H_GVkE) and the dedicated microsite is available to view [here](https://gurlsoutloud.com/)[[7]](#footnote-7).

6.6. Surveys to assess the campaign’s effectiveness were conducted one week before the launch of the campaign, one week after the initial six-week campaign phase and another after the conclusion of the campaign.

6.7. In the final evaluation of the campaign, we found that as many as **1 in 3 girls** had been affected by this issue, either directly or knowing someone that had received either a message requesting a nude or a message that had made them feel uncomfortable.

6.8. Amongst parents and carers, the term “self-generated online child sexual abuse” was low and once being shown a definition of the term, most agreed the issue was common, but only half saw their own daughter as being vulnerable.

6.9. Parents and carers ability to have a conversation with their child was linked to their knowledge. Parents who were more likely to have a conversation with their child knew about the terminology and had a better understanding of the tools they could use to restrict and monitor their child’s activities online.

6.10. Daughters who had been spoken to by their parents about the dangers of the online world, were also better equipped to deal with inappropriate requests and take appropriate action such as talking to their parents or reporting the issue to the police.

6.11. The film targeting parents was view **8.8 million** times with the T.A.L.K. checklist being downloaded over **3,250** times and the website being visited over 108,000 times. **31%** of parents who had seen the campaign said that they had a conversation with their child about the issue over the next month compared with just 20% who had not seen the campaign video.

6.12. The girls campaign received **17.6 million** impressions with the film being viewed in its entirety on **166,000** times and the dedicated microsite being visited on **26,000** occasions. Girls who had seen the film and campaign materials were more likely **(71%)** to ignore or block the request than girls who had not seen the film (66%).

6.13. Overall, 90% of girls suggested that they should tell someone if asked for a nude photo or video.

6.14. The IWF also makes up one third of the UK Safer Internet Centre alongside Childnet International and SWGfL and a responsible for co-ordinating Safer Internet Day in the UK each year.

6.15. In 2022, the theme for Safer Internet Day was All Fun and Games? Exploring respect and relationships online.

6.16. Research published on the day explored the relationships children have with online gaming. Of the children surveyed **71%** said that playing games made them feel happy and relaxed online and **66%** if children said that it had helped them to develop new skills such as determination and problem solving.

6.17. The research did, however, also highlight some of the downsides to life online. **78%** of children and young people had received friend requests from people they didn’t know and **46%** had received requests or invitations to meet up with strangers in person. **73%** also stated that they had also seen someone being mean or nasty online.

6.18. **59%** of children surveyed also said they want to learn more about how to play games online safely.

6.19. In 2022, **54%** of children aged 8-17 had said that they had heard of Safer Internet Day and as a result 80% said they feel more confident about what to do if they are worried about something online with 72% saying that they had a conversation with someone about how to stay safe online.

6.20. **32%** of parents and carers had also heard of the day with **67%** talking to their child about how to use the internet safely and **69%** saying they had a better understanding of how to keep their child safe online.

6.21. A record **3,424** organisations, schools, governments, police forces, charities and wider supporters signed up to support Safer Internet Day in 2022, with **936,666** views of the Safer Internet Day film and over **125,000** downloads of the education packs for use on the day.

6.22. 41% of teachers said the day also had led to an increase in safeguarding disclosures being made. The UK Safer Internet Centre is also grateful to the support it received from the Scottish Government who also participate in running workshops to help determine the theme for Safer Internet Day and this year also launched a new Parents Club Scotland Campaign to provide useful hints and tips for parents to help keep children safe online.

## Challenges

7.1. **European hosting of content-** As mentioned previously in this evidence, Europe is the global hotspot for the hosting of Child Sexual Abuse Material. **72%** of CSAM we removed from the internet in the last year was hosted in Europe and this is mainly hosted on image hosting boards and cyberlockers. We are looking forward to seeing the detail contained within proposals soon to be published by the European Commission on how to tackle child sexual abuse material in Europe, but the European Commission’s impact assessment for their forthcoming proposal also points to wider challenges with the implementation of the current directive by Member States, with the European Commission having opened infringement proceedings against 23 of the 27 for possible non-conformities.

7.2. Whilst this might not appear directly relevant to the UK situation or Scotland, the challenge is that this is a global problem. Just because Scotland and the UK has a good record on not hosting this content, does not mean that children in the Scotland and the UK cannot come to harm. A child in Scotland could be groomed by an offender in another country into creating self-generated material that may be hosted on a server located in the European Union. Only by working collaboratively and addressing these hosting issues will we be able to prevent harm occurring to children.

7.3. **Increasing moves toward greater encryption online-** For the last five years, the IWF has been warning about the dangers of the internet moving towards greater encryption online without considering the need for child safety online.

7.4. It is important to say from the outset that the IWF is not against strong encryption. Encryption is not simply a good thing to be pursued at all costs or a bad thing to be avoided. Improvements in encryption have, for the most part, been a good thing. Standard encryption has revolutionised the way we browse the web, access banking and government services, and how we communicate via email and messaging apps.

7.5. Until recently, privacy and security developments have largely been compatible and complementary with the systems that have been protecting the safety of our most vulnerable web users. This includes systems used by social media, messaging, and data storage platforms to automatically detect images and videos of child sexual abuse material.

7.6. Deploying End to End Encryption (E2EE) in communication and social media platforms, is however, different. E2EE extends standard encryption so that only the sender and receiver can view the content of the messages. This prevents the platform themselves from accessing any data being hosted on or passed through their systems. It is important to remember that all popular messaging platforms are already using standard encryption which prevents our data from being intercepted by third parties.

7.7. Whilst encrypting messages so the tech provider can’t see the content might appear to be a good thing, “turning off the lights” as the National Crime Agency puts it, also means technology platforms lose the ability for lawful access, and crucially, will not be able to automatically detect images and videos of child sexual abuse being hosted or shared through their systems.

7.8. We have seen that social media companies are doing some amazing work to detect known child sexual abuse images. In 2020, Meta reported 20.3 million reports of known CSAM to the National Center for Missing and Exploited Children (NCMEC) in the United States using mainly hashing technology to detect these reports. But we have also seen the impact of what happens when they do not scan for content, when changes to EU privacy rules in the first half of 2021, saw them switch off voluntary scanning leading to a 58% reduction in reports from EU accounts.

7.9. We must ensure that the pursuit of individual privacy online is not at the expense of victims of child sexual abuse or their right to privacy and their right not to have their images and videos of their abuse freely circulating online. We must ensure that efforts to protect privacy do not compromise child safety.

7.10. The problem of online child sexual abuse and exploitation is a growing problem, and we must be careful to ensure we do not take steps backwards, giving up some of the best technological solutions we have in the fight against it.

7.11. The IWF would urge technology companies to take a balanced approach to user privacy and child safety. We would like to see industry leaders taking other steps to improve user privacy before adopting E2EE or at least develop effective tools for detecting CSE/A content and child safety tools that are compatible with E2EE environments.

7.12. We would like to see tech companies focussing on how we resolve current challenges such as the rise in self-generated content before and the identification of new content and moves towards E2EE will simply make responding to these challenges even harder in the future.

7.13. We believe that the joint committee appointed to scrutinise the Government’s draft Online Safety Bill made a sensible recommendation to include E2EE as a specific risk factor in risk assessments and profiles and that service providers should be required to mitigate risk arising from the encrypted nature of their services under the safety by design requirements.

7.14. **Virtual Private Networks (VPNs)-** Linked to E2EE, the IWF is also concerned about the increasing prevalence, availability and easy access to VPNs which can often be used to circumvent parental controls and other content filtering solutions provided by ISPs. We need to ensure that content blocking mechanisms, such as those proposed through Clause 124 in the Online Safety Bill do not see unintended consequences such as individuals downloading VPNs and ending up in more extreme parts of the internet and on the dark web. We would recommend that Government ensure VPNs are also putting in place protections to ensure they are not allowing customers access to CSAM.

7.15. **Online Safety Bill and co-designation-** The UK Government will shortly be introducing its Online Safety Bill aimed at making the UK the safest place in the world to go online and in ensuring the strongest possible protections are in place for children.

7.16. The IWF is supportive of the UK Government’s ambitions to improve online safety and we have been actively engaged with Government on the development of the legislation and been in consultation with the Scottish Government around some of the responsibilities contained within the Bill which are devolved matters and where we believe the Bill can be strengthened further.

7.17. We believe that the Bill should build upon current best practice, consider the technical expertise that will be required to effectively regulate this space, and ensure it respects current international collaboration that already exists in this space.

7.18. The IWF wants to ensure that its skills and expertise is reflected in the forthcoming regulatory environment, and we believe this is best achieved through co-designation to regulate CSE/A with Ofcom. The Government’s Online Harms White Paper, the Government stated:

*“It would work with Ofcom to ensure that the regulator is able to work effectively with a range of organisations. This includes through a range of means including co-designation powers, memorandums of understanding, forums, and networks.”*

7.19. However, the current draft of the Online Safety Bill does not explicitly mention either co-regulation or co-designation or how the Government and Ofcom intends to achieve this. The Draft Online Safety Bill committee recommended that Ofcom should be given the power to co-designate efficiently and effectively and stated that the IWF had

*“Made a persuasive case that they should be co-designated by Ofcom to regulate CSE/A content an argument which had been supported by both the Crown Prosecution Service and Talk-Talk.”*

7.20. The IWF is continuing its discussions with Ofcom, Government, and the National Crime Agency about how we continue to work with these partners in the future, but believe more clarity is needed ahead of the Bill becoming operational on how all these functions will work together and work collaboratively. We support the suggestion made by the draft Online Safety Bill committee that more information is required on how co-designation may be achieved.

7.21. **Mandatory Reporting-** The IWF is also supportive of the introduction of mandatory reporting in the forthcoming Online Safety Bill. This requirement will be placed on all companies in scope of the Bill as well as Internet Service Providers (ISPs) and other infrastructure providers not covered in the Bill’s definition as either providing User-to-User or search services.

7.22. The mandatory reporting element will require companies who are not currently reporting elsewhere to report any CSE/A content with links to the UK to the National Crime Agency as the designated body.

7.23. The IWF believes the benefits of introducing mandatory reporting will include an ability to better understand the scale and nature of the threat along with transparency reports from companies which are also required within the Online Safety Bill. The IWF is, however, keen to ensure that the reporting structure complements existing international structures, such as US companies reporting to the National Center for Missing and Exploited Children (NCMEC) in the United States and plans in Europe for a new Centre to tackle Child Sexual Abuse and its own introduction of mandatory reporting in plans to be announced by the European Commission on 11 May 2022.

7.24. **Membership of IWF-** In November 2021, the IWF welcomed the Welsh Government’s Digital Learning Division as a Member, becoming the first Government to join the IWF through membership. The IWF is currently in discussions with Education Scotland, and we look forward to hopefully welcoming them as Members soon.

1. Non-Photographic Images include cartoons, drawings, computer generated imagery (CGI) and other non-photographic depictions of child sexual abuse that are deemed to have breached sections 62-69 of the Coroners and Justice Act (2009). [↑](#footnote-ref-1)
2. <https://nationalcrimeagency.gov.uk/who-we-are/publications/533-national-strategic-assessment-of-serious-and-organised-crime-2021/file> [↑](#footnote-ref-2)
3. <https://www.iwf.org.uk/about-us/how-we-assess-and-remove-content/our-mou-the-law-and-assessing-content/> [↑](#footnote-ref-3)
4. <https://www.iwf.org.uk/media/5pmf45dp/legal-guidelines-for-hosting-companies-and-their-employees-in-scotland.pdf> [↑](#footnote-ref-4)
5. <https://www.sentencingcouncil.org.uk/wp-content/uploads/Final_Sexual_Offences_Response_to_Consultation_web1.pdf> [↑](#footnote-ref-5)
6. <https://talk.iwf.org.uk/> [↑](#footnote-ref-6)
7. <https://gurlsoutloud.com/> [↑](#footnote-ref-7)