Witness Name: Derek Ray-Hill

Statement No.: 01

Exhibits: DRH/01 - DRH/32

Dated: 30 April 2025

UK COVID-19 INQUIRY

WITNESS STATEMENT OF DEREK RAY-HILL

I, Derek Ray-Hill will say as follows: -

Opening remarks

1. I joined the Internet Watch Foundation (IWF) on 09 September 2024, in the role of "Interim Chief Executive Officer (CEO)", pending the appointment of a permanent CEO.

2. I am providing this witness statement in response to a request from the UK-COVID-19 Inquiry. During the Covid period I was not an employee of the Internet Watch Foundation. The CEO at that time was Susie Hargreaves OBE. The content of my statement reflects my honest understanding of the events as they occurred, as has been relayed to me by the IWF team. The questions posed by the Inquiry involve several departments within IWF. As such, I have written my statement in the third person.

The nature, role, remit and purpose of the Internet Watch Foundation ('**IWF**').

3. The Internet Watch Foundation (IWF) is a charitable membership organisation that works in partnership with the internet industry, law enforcement and government to remove child sexual abuse (CSA) images and videos from the internet, 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:

- providing a secure and anonymous place for the public to report suspected online CSA images and videos; and
- using the latest technology to search the internet proactively for CSA images and videos.

4. The IWF has a Memorandum of Understanding between the National Police Chiefs' Council (NPCC) and Crown Prosecution Service (CPS) that governs our operations [DRH/01 – INQ000571098]. 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.

5. The IWF plays a vital role in providing the internet industry with several quality-assured technical services to prevent the spread of known CSA images and videos online and to stop the uploading of new images. These include the creation and dissemination to Members of

   - lists of hashes, created using image hashing techniques;
   - a URL blocking list of live webpages known to include CSA images or videos;
   - a 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.

6. Our Members include some of the biggest companies in the world, such as Amazon, Apple, Google, Meta, Microsoft, Snap, X, 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), as well as smaller operators which are still able to access all the technical services and tools we have to offer.

The structure of the IWF

7. We are an independent, non-profit charitable organisation working in partnership with a range of other organisations from the private, public and NGO sectors.

8. In January 2025, the IWF is made up of a team of over 80 people, working in a variety of disciplines. This team includes our front-line analysts and image classification assessors, who spend each and every working day assessing images and videos of children suffering sexual abuse.

9. The IWF team is led by our Senior Leadership Team under the executive management of Derek Ray Hill, our Interim CEO. Under our Interim CEO sit the Deputy CEO and Chief Operating Officer Heidi Kempster, the Hotline Director Chris Hughes, Communications Director Emma Hardy and Chief Technology Officer Dan Sexton.

10. Our strategy and long-term objectives are overseen by our Board of Trustees. They're a group of professionally and personally diverse individuals who are leaders in their own right, bringing varied and relevant experiences to the IWF. We are accountable to the Charities Commission and Companies House and submit the requisite documents to them as required. Our staff are supported by comprehensive and wide-ranging welfare structures and are subject to enhanced Disclosure and Barring Service checks (formerly called Criminal Records Bureau checks) before their appointment.

11. We were set up in 1996 by the internet industry to provide an internet hotline for the public and IT professionals to report potentially criminal online content within our remit and to be the 'notice and takedown' body for this content. Our Code of Practice for Notice and Takedown of UK Hosted Content within the IWF Remit [DRH/02 – INQ000571099] details our role in these takedown procedures. Once notified of the presence of such content on an internet site or platform, the relevant host or internet service provider (ISP) is duty-bound under the E-Commerce Regulations (Liability of intermediary service providers) to quickly remove or disable access to the criminal content.

The IWF's Governance:

12. The IWF is governed by a Board of 11 Trustees (currently 10 due to one vacant position). The Board comprises an Independent Chair, six Independent Trustees, three Industry Trustees plus one Co-opted Trustee (who is also independent of industry). It elects two Vice-Chairs: one from the Industry Trustees and one from the Independent Trustees. The Board monitors, reviews and directs the IWF's remit, strategy, policies and budget to help the IWF to achieve the IWF objectives.

13. Independent Trustees are chosen by an open selection procedure following national advertising.

14. The Industry Trustees are elected to our Board from the Funding Council. No Trustee may serve more than six years. All Trustees are subject to vetting including an Enhanced DBS check.

15. The IWF became a registered charity in December 2004 to improve its structure and accountability.

16. The IWF's governance arrangements are strengthened by a regular cycle of Board meetings and Executive meetings as well as a finance committee reporting to the main Board. The IWF regularly reviews and improves its governance documentation to ensure it meets current legislation and accurately reflects our independent status.

Summary of the online harms relating to children which the IWF was aware of prior to 31 December 2019 (including instances where children are groomed online leading to offline contact)

17. As the UK body identifying, disrupting and removing CSA images, videos and links to such content, and with a privileged position in law enabling our analysts to proactively search for this material, the IWF is often the first to see the abuse of children online. Outlined below are four key areas of concern relating to online harms relating to children that IWF had identified prior to 31 December 2019:

- **CSA imagery created when the abuser is physically present with the child and then uploaded online.** In 2019 this type of child sexual abuse imagery was the predominant type of child sexual abuse image and video we identified online [DRH/03 – INQ000571100].
- **Grooming, coercion and capture of sexual activity.** IWF analysts see on a daily basis the resulting CSA imagery of children who have been groomed online, coerced online, and exploited online, into sexual activity that has been captured by someone who is remote to them. This imagery is then shared on forums, websites, and sold for commercial gain. In 2019, almost a third (29%) of child sexual abuse imagery on URLs had been created in this way [DRH/03–INQ000571100].
- **Commercialisation of child sexual abuse imagery.** At this point in time, IWF analysts frequently (12% of webpages confirmed as containing CSA imagery in 2019) saw that CSA imagery, however it had been created, was being commercialised online [DRH/ 03[IWF Annual Report 2019, page 55]-INQ000571100]. That is, it was being sold. It was also being used as a currency in and of itself whereby people with a sexual interest in children would gain access to forums, or indeed more CSA imagery, by providing first generation, or 'brand new' CSA imagery, as payment. This practice put children at greater risk

of abuse and enabled first generation content to have a higher value than that of content which is more dated or already being frequently exchanged online.

- **Children of all ages being abused.** In the period prior to 31 December 2019, IWF analysts frequently saw CSA imagery online featuring children, from newborns r to 17-year-olds). In 2019, the age they most often saw depicted in the imagery was 11–13-year-olds (48% of depicted children) followed by 7-10 year olds (34% of depicted children [DRH/03 – INQ000571100].

Summary of data trends in relation to online harms relating to children between 1 January 2015 to 31 December 2019, as previously published by IWF, CSA imagery created when the abuser is physically present with the child and then uploaded online.

18. Throughout IWF's history since 1996, the predominant type of CSA image and video has been created when an abuser was physically present with the child. Exceptions to this were beginning to emerge in the period before 31 December 2019, due to the changing nature of online CSA, as further explained below.

Grooming, coercion and capture of sexual activity

19. In 2012, IWF produced the world's first published report looking at self-generated sexually explicit images and videos featuring young people online [DRH/04 – INQ000571104]. It was produced in response to media reports that children were 'sexting'. IWF wanted to determine whether this content was making its way online and found that it was.

20. In 2015 a follow up, Microsoft-funded study [DRH/05- INQ000571105], IWF looked into this phenomenon further; finding that:

"What emerged from the data in this Study is an increasing trend for the distribution of sexually explicit content produced by younger children using laptop webcams which, due to the nature of the technology used, they are aware is being shared with at least one other party."

21. In 2018, the second part of the Microsoft-funded study was published [DRH/06- INQ000571106]. The Study aimed to examine characteristics of captures of live-streamed CSA in distribution online. Following the publication of 2018 report,

IWF began to log, as part of its standard practices, any URLs that featured at least one image or video that had been captured by a device where it was evident that the abuser was not physically present with the victim/s.

22. From 2018 onwards (recognising that 2018 was an incomplete year of data for the capture of what was termed 'self-generated' CSA imagery), data on this particular harm type has been published.

23. Please note that IWF assessed 'reports' which were essentially URLs/webpages. If 'self-generated' CSA imagery was present on the reported URL/webpage page, IWF analysts would add a marker to indicate that.

	Number of URLs logging 'self-generated' CSA imagery	Proportion (%) of total URLs that featured 'self-generated' CSA imagery.
Last six months of 2018	no figure published	27
2019	38,424	29

24. Through this data, and anecdotally via IWF analysts who were now seeing this type of content on a daily basis, IWF was aware that this was the start of a concerning trend.

Commercialisation of child sexual abuse imagery

25. Year-on-year IWF tracks the proportion of CSA URLs that fall within its definition of 'commercial'. Below is a summary of what IWF published in the period up to 31 December 2019. (Please note that in some years, data relating to subsets of 'commercialisation' was additionally published in annual reports and the data set out below sets out the high-level statistics only.)

26. In 2015, of the 68,092 webpages IWF confirmed as containing child sexual abuse imagery in 2015, 14,708 (21%) were commercial. This compares to 3,741 (12%) in 2014. [DRH/7- INQ000571107].

27. In 2016 of the 57,335 webpages IWF confirmed as containing child sexual abuse imagery in 2016, 5,452 (10%) were commercial in nature. This compares to 14,708 (21%) in 2015. That's a decrease of 62%. [DRH8- INQ000571108]

28. In 2017 of the 78,589 webpages containing child sexual abuse imagery, 8,974 were commercial in nature [DRH/9 - INQ000571109].

29. In 2018 of the 105,047 webpages we confirmed as containing child sexual abuse imagery in 2018, 6,941 (7%) were commercial in nature [DRH/10- INQ000571110].

30. In 2019 of the 132,676 webpages we confirmed as containing child sexual abuse imagery in 2019, 15,326 (12%) were commercial in nature. This is an increase on 2018, when we took action against 6,941 (7%) commercial webpages (IWF, 2020). [DRH/03 - INQ000571100]

Children of all ages being abused

31. As part of IWFs assessment of online CSA images and videos appearing on URLs, IWF logs the age of the youngest child depicted in any of the imagery on a webpage. Figures provided in the IWF Annual Report 2016 and the IWF Annual Report 2019 show the ages of children logged in CSA imagery found on URLs between 2014 and 2019 inclusive, illustrating that the abuse occurred in children of all ages.

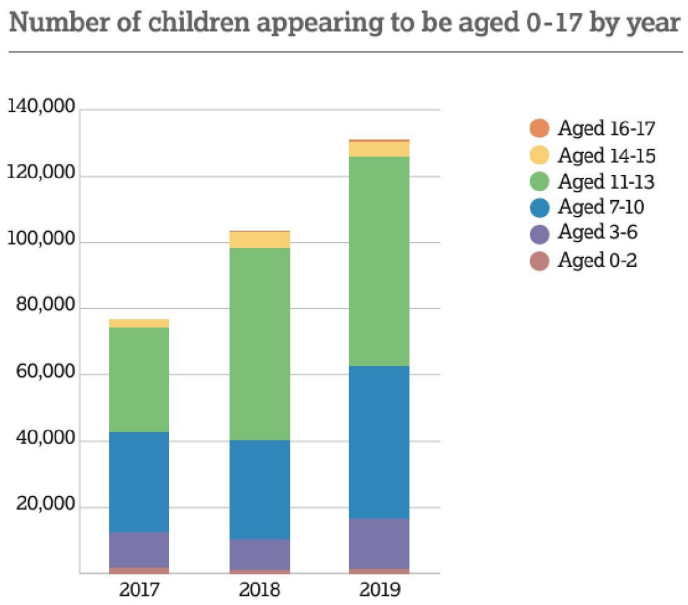

Figure 1 - chart taken from the IWF Annual Report 2019 showing the ages of children logged in imagery found on URLs between 2017 and 2019 inclusive [DRH/03 - INQ000571100].

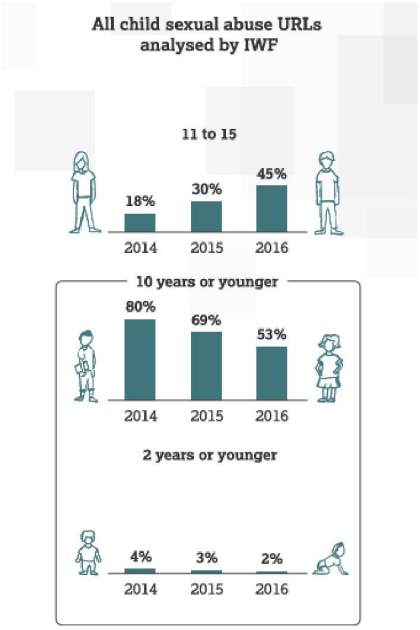

Figure 2 - chart taken from the IWF Annual Report 2016 showing the ages of children logged in imagery found on URLs between 2014 and 2016 inclusive [DRH/08- INQ000571108*].*

Measures and/or mitigations the IWF is aware of which were in place as at 31 December 2019 in order to protect children from online harms and ensure their online safety.

32. IWF is a charitable membership organisation. Companies, trade bodies and others join IWF and have access to all available datasets and services that IWF offers. These datasets and services comprise intelligence and information that IWF gathers during the course of its work identifying and removing CSA material online.

33. The measures and mitigations that IWF offered that were in place as at 31 December 2019 are detailed in the paragraphs below.

34. The IWF Image Hash List; containing a special catalogue of codes, or hashes which is updated daily and manually verified by IWF expert analysts. Each hash is completely unique and is a type of digital fingerprint or label that identifies a picture of confirmed CSA. Each criminal image has its own individual hash [DRH/11-INQ000571114]. Deployment of the IWF Image Hash List enables companies to stop the upload, storage and sharing of known CSA imagery on their platforms and services.

35. the IWF Keywords List; offenders often create their own special language or code for concealing criminal CSA material online. The IWF Keyword List compiles these

words, phrases, and codes and makes them available to IWF Members allowing them to stop this type of criminal content on their network or application [DRH/12-INQ000571115].

36. the IWF URL List provides a comprehensive list of webpages confirmed as containing images and videos of CSA by IWF analysts. Since each URL (Uniform Resource Locator) is a unique webpage address, IWF can be precise about the exact location of the criminal imagery to ensure that a legitimate website is never over-blocked [DRH/13/ INQ000571116].

37. the IWF non-photographic URL list which helps block access to cartoons, drawings, computer-generated images and other non-photographic representations of CSA. This service is similar to our URL List, but it only includes webpages or images that are not real photos of the suffering of child victims [DRH14/ INQ000571117].

38. IWF's takedown notices service whereby IWF sends takedown notices to companies when it finds CSA images, videos or *non-photographic imagery hosted in the UK, that break UK law [DRH02/ INQ000571099].

39. the IWF Domain Alerts service which helps registry operators stop their top-level domains (TLDs) from containing domains which host this disturbing criminal imagery. Our alerts notify registry operators when any confirmed criminal CSA images or videos are hosted on any domain using their TLD. This means they can take immediate action to suspend the domain in question, or contact the owner, for example, through the registrar. They can do this, while IWF is working to have the images removed [DRH/15- INQ000571119].

40. the IWF Simultaneous Alerts service provides the fastest way for companies hosting in the US to protect their networks from criminals who use legitimate services to share CSA imagery. The alerts are immediate warnings about CSA hosted on US networks. IWF analysts are experts at hunting down criminal images of children on the open internet. When they find child sexual abuse hosted in the US by one of IWF's Member's platforms, they send an immediate alert to them. IWF also notifies its US partner, the National Center for Missing & Exploited Children (NCMEC). This dual approach means that criminal imagery can be removed as quickly and effectively as possible [DRH/16- INQ000571120].

41. the IWF Virtual Currency Alerts are designed to give cryptocurrency companies real-time notifications when a virtual currency is used to buy CSA imagery. The alerts are immediate. When a virtual currency wallet (a type of storage for digital currency)

has been linked with any confirmed online CSA imagery, the provider is warned [DRH/17- INQ000571121].

42. the IWF Payment Brand Alerts help protect legitimate financial service brands from being used for payments for online CSA imagery. Essentially, they are a warning for payment service companies. IWF notifies the payment service company if their name, or brand is used to pay for CSA images or videos [DRH/18- INQ000571122].

43. the IWF Newsgroup Services are lists and notifications of confirmed CSA imagery that is being hosted on newsgroup (internet discussion group) services. IWF provides its Members with a list of this illegal imagery. This means that hosts can take down any known criminal imagery that's being hosted on their platform [DRH/19- INQ000571123].

The understanding by Government departments (particularly DfE, the Home Office, DCMS), the Scottish Government; the Welsh Government, the Northern Ireland Executive, the National Crime Agency (NCA) and Police and other investigating authorities across the UK. of the impact of children using online technology, the risk in relation to online harms and the measures and/or mitigations outlined above

44. The Inquiry has asked IWF to consider whether the impact of children using online technology, the risk in relation to online harms and the measures and/or mitigations outlined above was understood by Government departments (particularly DfE, the Home Office, DCMS), the Scottish Government; the Welsh Government, the Northern Ireland Executive, the National Crime Agency (NCA) and Police and other investigating authorities across the UK.

45. The IWF is a charitable membership organisation. Whilst IWF is an expert in identifying and removing CSA imagery online, and curating services to disrupt and prevent the upload of this content, it is not possible to quantify what those groups specified knew of the impact, risks or mitigations. Additionally, the key IWF staff who were responsible for much of the liaison with those groups at the time have now moved on from the organisation.

Online safety and harm during and since the pandemic

The IWF published this article about initial work that indicated that children may be at greater risk of grooming during the pandemic:

https://www.iwf.org.uk/news-media/news/children-may-be-at-greater-risk-of-grooming-during-coronavirus-pandemic-as-iwf-braces-for-spike-in-public-reports/

46. In March 2020, the IWF published an article stating that children were likely to be at greater risk of grooming during the pandemic [DRH/20- INQ000571124].

47. The IWF is in a privileged position legally which enables it to proactively search for online CSA imagery, and to very often be the first to see new abuses of children online.

48. Since 2012, the IWF had been tracking the development of 'self-generated' CSA imagery (as explained in paragraphs 18 to 31 above). IWF could see a proportional increase in the number of URLs showing images or videos of a 'self-generated' nature and began to be concerned about the impact of lockdowns, and the increasing amount of time that children needed to, or wanted to, be online.

49. Given that grooming and coercion of children via online platforms resulted in the creation of CSA imagery that was captured via devices, and that people were being forced to spend more time indoors, perhaps online, IWF expected that more children may be exposed to sexual abusers online, leading to more CSA imagery being created, and that more people with a sexual interest in children will have the ability to spend more time online.

50. The IWF concluded that children would be at greater risk of online child sexual abuse during the pandemic due to the likelihood that they would be spending more time online, and due to the likelihood that more adults would be spending more time at home, not in their workplaces and likely online.

51. The IWF set out these concerns in the published March 2020 article. The IWF additionally used the statement to reassure people that it was still working and still taking reports and reminded people that searching for CSA imagery online is illegal.

52. Data collected by the IWF demonstrates the increase in 'self-generated' CSA imagery, as compared with 'not self-generated' CSA imagery, on URLs in the period during and following December 2019.

53. Beyond publishing the press release on the IWF website and talking to journalists about its concerns, it is not now possible to know what conversations may have taken place between IWF staff and government and law enforcement officials. These conversations and communications, if they happened, would have been between staff members who are no longer employed by IWF.

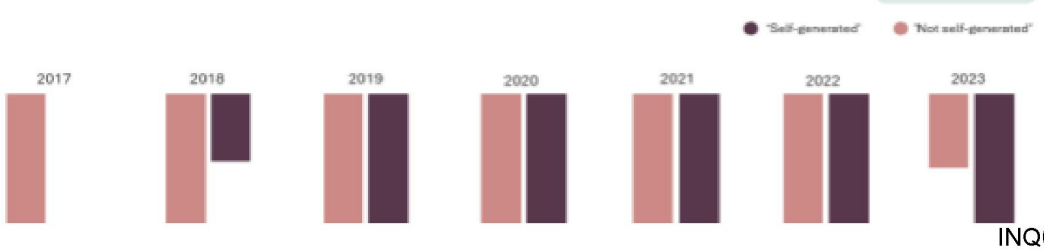

Figure 3- Graph showing the growth in 'self-generated' child sexual abuse content on URLs over time.

54. Note that the IWF regards the term 'self-generated' CSA as an inadequate and potentially misleading term which does not fully encompass the full range of factors often present within this imagery, and which appears to place the blame with the victim themselves. Children are not responsible for their own sexual abuse. Until a better term is found, however, the IWF will continue to use the term 'self-generated' as, within the online safety and law enforcement sectors, this is well recognised.

55. In April 2022, the IWF published an article about the increase in sexual abuse imagery of girls online following pandemic lockdowns [DRH/21- INQ000571125]. In coming to the conclusions reached in the article, IWF analysed the data that it had gathered over a 11-year period which logged the number of URLs showing CSA imagery of girls, boys and both sexes. This starkly showed how URLs showing CSA imagery of girls was more often being discovered by IWF analysts than that of boys. In 2021, IWF data showed that 97% of reports showed girls, compared with 1% showing boys and 2 % showing both sexes.

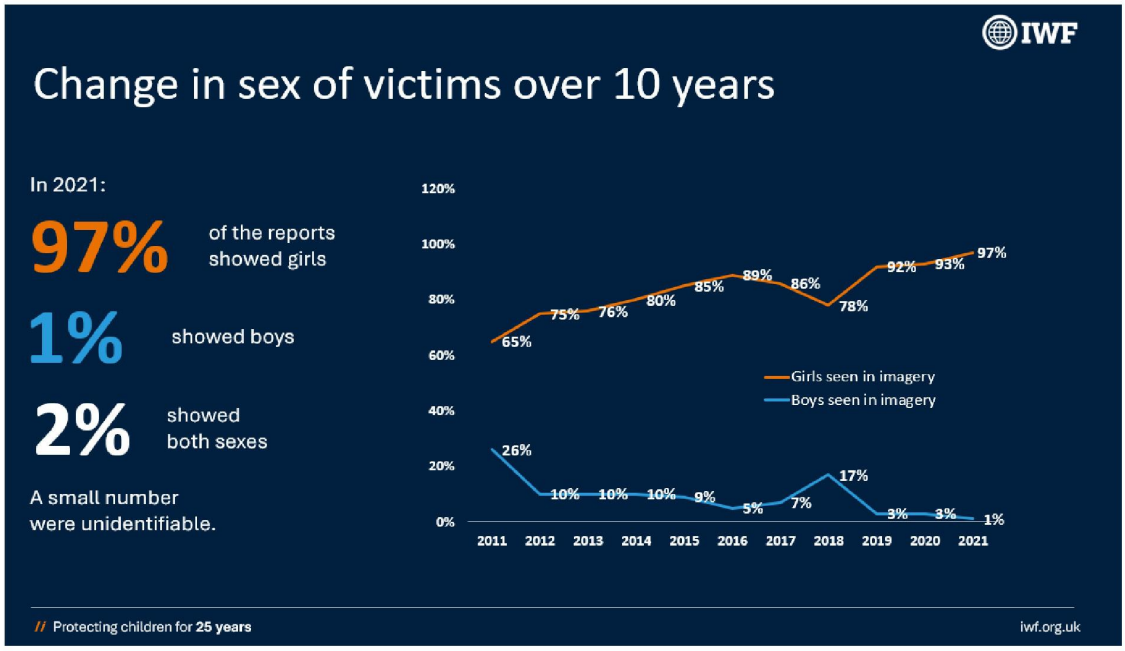

Figure 4 - graph tracking the proportion of URLs identified over an 11-year period that showed imagery of girls, and boys.

	Girls %	Boys %
2022	96	2
2023	97	1
2024	Not yet published	

56. As above, the most recent figures available, those for 2022 and 2023, remain relatively static and in line with the position in 2021.

57. In 2023, IWF published an article stating that sexual abuse imagery of primary school children was 1,000 percent worse since lockdown [DRH/22- INQ000571126]. In reaching the conclusions drawn in this article, the IWF analysed the data that it had gathered over the most recent years, and in particular the data that related to 'self-generated' CSA imagery. From the data, it was clear that the IWF had identified imagery of children aged 7-10 years old, who had been groomed and coerced into 'self-generated' CSA imagery, and that this was the fasted growing age group year on year.

58. Given that the opportunity for this crime is borne from children's unsupervised access to online devices, and more time and opportunity to be online for both sexual abusers and children, it was vital to raise awareness of this threat.

59. The data published in this article said:

- *In 2022, 63,050 reports related to imagery which had been created of children aged 7-10 who, in many cases, had been groomed, coerced, or tricked into performing sexual acts on camera by an online predator.*
- *This is a 129 per cent increase on the 27,550 reports in this category in 2021.*
- *The 2022 figures are a 1,058 per cent increase on the 5,443 such reports in 2019 before the outbreak of Coronavirus. Of the imagery made of 7-10 year olds in this way in 2022, 14 per cent (8,930 URLs) contained Category A material. This is the most severe kind of material and can include penetrative sexual activity, images involving sexual activity with an animal, or sadism.* [DRH/22- INQ000571126]

60. In IWF's 2023 Annual Report [DRH/23- INQ000572006] it was reported that:

- *children aged 11-13 continue to appear most frequently in 'self-generated' imagery, as in previous years. We also 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.*

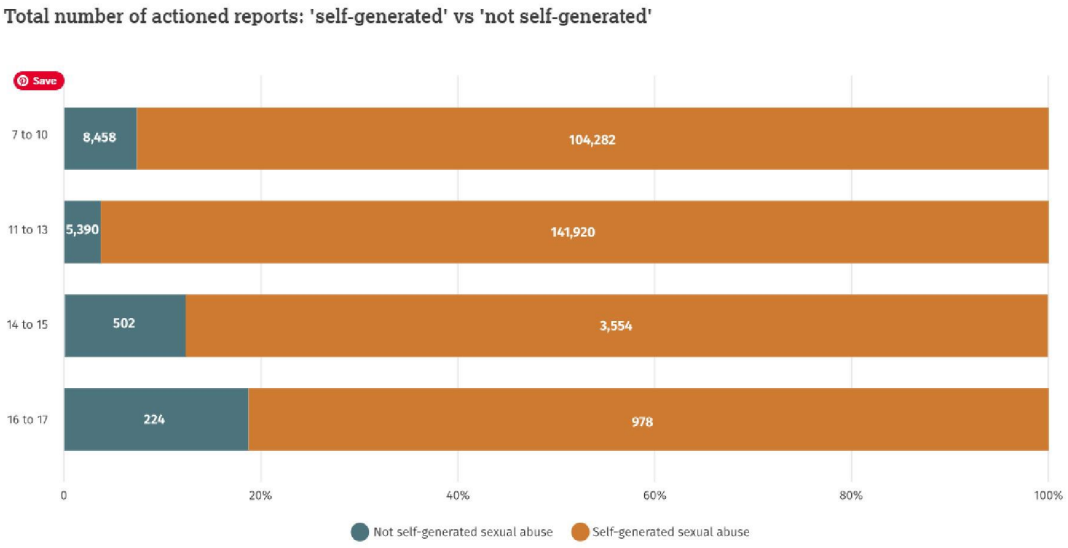

Figure 5 - graph that shows the most recently published age-related data (2023) for 'self-generated' child sexual abuse imagery found on URLs.

61. Our data shows that between 1 January 2020 and 28 June 2022, the IWF found an increase in URLs containing CSA imagery that had been created when sexual activity was captured of children by devices (webcams or smartphones) remotely, and shared online.

62. The IWF has not carried out any research to establish whether there is a statistically significant correlation between the amount of unsupervised time children and young people spend online and the increase in this material as this would be beyond the IWF's scope. It is also worth noting that the CSA imagery identified by the IWF may depict children from all over the world; it is not often possible to establish which

country the victim comes from. Therefore, the trends that we have identified may be impacted by the policies of multiple jurisdictions.

63. IWF has outlined in this response where it has data to suggest an increase in 'self-generated' child sexual abuse imagery found during the pandemic. It has not, however, placed resources into discovering if there is a statistically significant correlation that suggests that there have been changes and/or developments to online harms either caused by, exacerbated by or accelerated by the pandemic, including any measures taken by Government, including the devolved administrations, in response to the pandemic regarding: the online sexual abuse or exploitation of children during the Specified Period; the volume or nature of indecent images or material showing the abuse of children during the Specified Period; the number of people accessing indecent images or material showing the abuse of children during the Specified Period; the extent to which children were exposed to harmful online material during the Specified Period; and / or the way that children have been impacted by any of the above.

Measures to mitigate any negative impacts on children and young people identified above as related to the pandemic in relation to online safety since 1 January 2020

Harm reduction campaigns

64. To mitigate the harm caused to children and young people from being groomed and coerced online, IWF launched an awareness and behaviour change campaign in June 2021. It received relatively modest amounts of funding from Microsoft and the UK Government's Home Office. Home Truths and Gurl Out Loud was seen as a successful way to help bring families together to talk about keeping safe online, and to empower parents to help protect their daughters online. [DRH/24- INQ000571080]

65. It found that:

> *Viewing more campaign materials was associated with more positive outcomes. However, this did not increase the likelihood that girls would tell someone if they received a request for explicit material. Daughters are more willing to disclose a request for explicit material when they have stronger ties with friends and family and weaker ties with strangers and when parents are open to seeking information and employing multiple strategies to respond* [DRH/25-INQ000571128].

66. Since then, the IWF has continued to work with its academic partners, the International Policing and Public Policy Research Institute (IPPPRI), to commission

research to inform public harm reduction campaigns, the latest being *Think Before You Share* [DRH/26- INQ000571081].

Provision of datasets and services to technology companies

67. The IWF continues to build and make available to industry internationally its suite of datasets and services. Notably, the IWF Hash List has grown considerably during this time and is used to prevent the upload, storage, and sharing of known CSA images and videos. This service is limited, however, by technology companies' willingness to build their platforms and services in a way that enables them to prevent the upload of CSA imagery through the use of this type of dataset. The IWF has responded most recently to the UK Government's Statement of Strategic Priorities for Online Safety. An Excerpt from IWF's response is included below. This relates to the Online Safety Act (OSA) which is now law, but which, in the IWF's expert opinion, does not go far enough yet to mitigate against the risks outlined above.

68. It is IWF's view that the OSA does not go far enough as there are gaps in the legislation that could amount to 'get out' clauses for technology companies. **The IWF has not stress tested our solutions to this against the event of a further pandemic or civil emergency.** It has, however, written to the Prime Minister [DRH27- INQ000588681] on 22 January to explain the concerns and solutions proposed.

69. An excerpt from this letter states:

    a. *However, we are deeply concerned that the Codes allow services to remove illegal content only when it is 'technically feasible', which will incentivise platforms to avoid finding ways to remove illegal content in order to evade compliance. This undermines the Act's effectiveness in combatting online child sexual abuse. We urge you to instruct Ofcom to urgently review and mitigate this blatant get-out clause. The publication of the Codes also highlights the weaknesses within the legislation itself. For example, the Act does not mandate companies to moderate content uploaded in private communications. As a result, illegal content that is blocked elsewhere on the internet can still be freely shared in private online spaces.*

    b. *Furthermore, the rules-based nature of the regulations means that platforms will be in compliance with their duties if they follow the measures in the Codes, rather than needing to effectively and proactively address the harms identified in their risk assessments.*

c. *We call on your Government to remove the safe harbour inadvertently offered to platforms by the Act, especially those that facilitate the sharing of child sexual abuse material. Additional legislation should be introduced to ensure there are no safe havens for criminals in private communications.*

70. IWF has communicated its concerns to the Prime Minister's office and Ofcom. Communications with Ofcom have taken the form of face-to-face meetings and online meetings. In addition to writing to the Prime Minister, we have had discussions with the Home Office and Department for Science Innovation and Technology, including hosting a visit the DSIT Secretary of State Peter Kyle on 17 March [DRH28-INQ000591827]. We have not yet received a response from the Prime Minister's Office.

71. IWF has not placed any resources or capacity into testing whether, in the event of a future pandemic and/or other civil emergency, the current statutory framework and regulatory regime would be sufficient to mitigate against any increase/acceleration/exacerbation in exposure to online harms experienced by children. It is beyond IWF's scope to answer this question.

72. In response to the question: "In the event of a future pandemic and/or other civil emergency which requires an increase in the amount of time which children spend online, provide your opinion as to what, if any, additional systems, processes, guidance and/or measures should be implemented to ensure that children are able to engage safely with online technology," IWF has not placed any resources into being able to answer this question; it is beyond IWF's scope.

73. In response to the question: "Is IWF aware of any proliferation in the sharing/production of CSA due to the pandemic? If so, please provide details. As drafted, it is my understanding that the IWF are not able to draw any such correlations - is this correct?" It is correct that IWF cannot draw direct correlations between the sharing/production of CSA due to the pandemic and the proliferation of this imagery. IWF has not placed resources into testing this theory but has simply reported the data that it has in its possession over this timescale.

74. In answer to the question: "What impact did the pandemic have on children's exposure to online harms? As drafted, it is my understanding that the IWF are not able to draw any such correlations - is this correct?" It is correct that IWF has not carried out any research or analysis about children's exposure to online harms and can therefore not draw any such correlation.

75. Excerpt from IWF's response to the Statement of Strategic Priorities for Online Safety, January 2025 [DRH/29- INQ000571079]:

"Introduction and Overview

The Online Safety Act (the Act) is a crucial child protection measure with the potential to transform children's safety online. We welcome the Secretary of State's strong Statement on the importance of the online safety agenda, and the call for greater pace, urgency, and ambition in Ofcom's implementation process.

It is encouraging to see that the recommendations we provided, in partnership with four other leading children's charities, have been incorporated into the draft Statement. It is essential to establish strong, ambitious foundations that place children's safety at the core of regulatory efforts. Children must not bear the burden of technological failures.

The consultation on the draft Statement is particularly timely given the recent publication of Ofcom's Illegal Harms Codes. We are concerned about several areas within the Codes, which we will address in detail in our response to the Statement of Strategic Priorities (SSP). We look forward to further collaboration and continued engagement with Government to ensure the Act delivers for children's online safety.

Recommendations

- Introduce a clear definition of Safety by Design (SSP Priority 1).
- Deploy stronger, more decisive language about safe havens for illegal content—replacing "work towards" with a more ambitious commitment (SSP Section 1.4).
- Explicitly recognise harms occurring in private communications and/or end to end encrypted environments, which Ofcom has recognised as a risk factor for CSAM (SSP Priority 1).
- Amend the language regarding the evidence base for age-appropriate experiences from "developing" to "building upon", to reflect the significant progress already made (SSP Section 1.1).
- We are concerned that Ofcom's Illegal Harms Codes require services to remove illegal content only when "technically feasible" (ICU C2). The Government must direct Ofcom to a) require providers to implement systems and processes to swiftly detect and remove illegal content as part of their moderation functions and

b) engage with a range of experts to determine how technical feasibility is assessed.

- Acknowledge the critical link between robust age assurance and the effectiveness of grooming mitigations (SSP Section 1.2).
- We remain concerned about the codes being designed as a "safe harbour" as this risks disincentivising innovation and investment in safety technology. The Government should recommend that Ofcom a) adds to the Code of Practice a requirement for all services within scope to effectively and proactively address harms identified in their risk assessments; and b) make it clear that it is the responsibility of businesses providing services to the public to ensure that those services are safe and do not facilitate the exploitation and abuse of children.
- Revise the language in Section 1.4 of the SSP to emphasise that terrorism content and CSAM must be actively tackled across all platforms and functionalities, utilising Section 121 of the Act.
- Adopt a more ambitious stance in its direction to Ofcom regarding the enforcement and transparency of Terms of Service (SSP Section 2.3).
- Introduce additional regulation to address emerging harms, such as those posed by AI (SSP Section 3.2).
- Acknowledge that stricter duties imposed on larger, mainstream platforms may unintentionally drive users to smaller platforms, which are not required to use hash matching technologies to detect and remove CSAM (SSP Section 3.4).

Additional Regulation

The Secretary of State notes that there may be areas where the Act may need to be amended to easily enable the delivery of these objectives. We urge the Government to take the following steps to address what we perceive as gaps within the Act:

- The current legislative framework provides “safe harbour” for companies who comply with the Ofcom Codes, even if their own risk assessments show that further action is needed to address the harms and risks within their platforms. The legislative framework needs to be adjusted to place responsibility for harm reduction and risk mitigation more explicitly with the companies involved.

- If platforms are unable or unwilling to enforce age limits effectively, then further legislation should be introduced to make this requirement explicit, including the implementation of minimum age requirements.
- The current exemption of "private communications" from the Act means platforms are not required to prevent the spread of illegal material, such as through hash-matching in spaces determined as private. This enables, and could encourage, abusers to take their activities into unregulated spaces where they can share CSAM (companies offering E2EE can still screen content at upload to ensure CSAM and other illegal content is not being distributed).
- Further measures are needed to keep pace with threats from emerging harms. For example, safeguards must be introduced in forthcoming AI legislation to prevent against the creation of AI-generated CSAM, such as by requiring AI models to be assessed before they go to market, to ensure models do not have the capabilities to generate this material. Additional measures are needed to tackle AI generated chatbots which facilitate or encourage criminal behaviour."

'Lessons learned' arising from the pandemic in relation to the impact on children in relation to online safety and harms

76. The IWF continues to see an increase in 'self-generated' CSA imagery on a higher proportion of total URLs containing identified CSA imagery year on year. It is affecting younger children, even as young as three to six, as evidenced by a snapshot study that the IWF published in 2024 [DRH/30- INQ000475194].

77. Widespread awareness and harm prevention messaging should be adopted at a national level, bolstered by age-appropriate education to build digital resilience skills. It should be accepted that these skills are needed by children from the earliest moments that they begin to use internet enabled devices with cameras. Therefore, appropriate consideration should also be given to national-level messaging to parents as well.

78. IWF has not placed any resources into assessing how such a widespread national harm prevention effort might operate in practice, or whether there should be any legislative mechanism requiring it.

79. The laws around online safety move much, much, slower than the diversification of tradecraft of abusers online. For example, in 2024, the IWF discovered a 'sextortion handbook' which provided around 200 pages of tutoring to people who wanted to extort children for sexual imagery.

80. The IWF has not placed any resources into assessing how this could be overcome in the event of a future pandemic and/or other civil emergency.

What, if anything, could be done differently in the event of a future pandemic in relation to online safety and protecting children from online harms

Awareness and harm reduction activities

81. Teaching online safety, and specifically the skills that children need to help them spot the signs of grooming and coercion is needed at an ever-younger age. Awareness by parents of the very real risks to children from abusers online needs to increase. If a future pandemic was to take hold, and if schools moved once again to teaching at home online, with lockdowns mandated, then strong, sensible and well-funded messaging to parents, young people and teachers to mitigate the potential risks to children is needed.

82. IWF has not placed any resources into assessing how this might operate in practice and any legislative mechanisms requiring it.

83. In answer to the question: "The Inquiry is that aware on 22 April 2020, the Minister for Security and DCMS' Minister of State for Digital and Culture co-hosted a virtual roundtable on child online safety in the context of Covid-19. In attendance were representatives from the National Society for the Prevention of Cruelty to Children ("NPCC"), Barnardo's, Parentzone, UK Safer Internet Centre, the Samaritans, and the Internet Watch Foundation. The Security Minister outlined the Home Office's work with law enforcement to understand the changing threats to children and to prioritise action to protect vulnerable children. He also asked for information on the experiences of the charities and for advice on further action the UK Government could take to protect children online. Please explain: a. What concerns, if any, were raised by IWF; b. Did the IWF suggest any actions the government could take to protect children? If so, please explain what action was suggested and why the IWF were of the view it would mitigate impact on children." Any IWF staff that attended that meeting are no longer with the IWF. It is not possible to know what the speaking points were of attendees.

84. In answer to the question: "Did the IWF take part in any other roundtable events/or any other events with the government during the Specified Period which focuses on protecting children from online harms. If so, please provide details and the contributions made by the IWF and copies of any meeting minutes," The key staff members who took part in any meetings of this nature are now no longer with IWF. It

is not possible to know what the talking points were or to provide any copies of minutes.

Safety by Design, including prevention upload of known CSA material in private spaces

85. The government and regulators can get ahead of potential future issues by ensuring that platforms online are designed in the safest possible way to prevent harm to children, and that there is no 'safe haven' created for abusers or CSA content.

86. This could work in practice by ensuring that, for example, hash matching technologies such as the IWF Hash List are used to prevent the upload of known child sexual abuse imagery at all possible opportunities across messaging and user-generated online spaces, even before a message is sent through an end-to-end encrypted space.

87. To answer the question: "Do you believe that other services providers such as social media companies did all they could to protect children from online harms during the pandemic. If not, please explain why and what could have been done." This is a complex and large question and IWF has not placed resources into looking at this issue. We are not best placed to provide an answer to this, and the question falls wider than the scope of our work.

88. To answer the question: "Did you raise any concerns with service providers during the pandemic which related to protecting children from online harms? If so, what response did you receive?" IWF liaises with online service providers on a daily basis regarding the removal and prevention of online child sexual abuse which is narrower in scope than all online harms. IWF has not conducted any analysis regarding concerns raised, or responses received, as regards service providers during the pandemic.

89. Studies have shown that offenders opt to use end-to-end encrypted spaces to groom and coerce children and share the resulting imagery [DRH/31- INQ000571129].

90. In IWF's response to the Government's Statement of Strategic Priorities, IWF says:

> "We welcome the Government's recognition that *"the goal should be to prevent harm from occurring in the first place, wherever possible."* We fully support this preventative approach, which should include robust upload prevention measures in private communications and **end-to-end encrypted** (E2EE) environments. Particularly given Ofcom's recognition that end-to-end encryption is a clear risk

factor for the protection of children and the distribution of CSAM. The technology to detect known CSAM prior to upload already exists, and it must be deployed to maximise child safety." [DRH/32- INQ000571130]

91. The IWF is concerned that Ofcom's Illegal Harms Codes require services to remove illegal content only when *"technically feasible"* (ICU C2). It is crucial that Ofcom directs providers to implement systems and processes to swiftly detect and remove illegal content as part of their moderation functions. It is also vital that Ofcom engages with a range of experts to determine how technical feasibility is assessed.

92. It is also vital that the Government directs Ofcom to use all powers possible to make the safest online environment for children, and not inadvertently create safe spaces for abusers, and abuse imagery, to thrive. That would be a huge failing, particularly if presented with another pandemic-like scenario.

Statement of Truth

93. I believe that the facts stated in this witness statement are true. I understand that proceedings may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief of its truth.

Signed Personal Data

Dated 30 April 2025