The Annual Report 2022

#BehindTheScreens

A deep dive into the digital and social emergency happening #BehindTheScreens, in children's bedrooms.

Internet Watch Foundation

Contents page

Introduction

Every one and a half minutes, IWF analysts assess a webpage. Every two minutes, that webpage shows a child being sexually abused.

If someone thinks they've seen a sexual image of a child online, they can report to us at iwf.org.uk, or through one of 50 portals in countries around the world, covering 2.6bn people.

We assess every report we receive. If it shows the sexual abuse of a child, we make sure the image or video is removed from the internet. And we provide bespoke services and datasets to our industry Members to prevent the imagery from re-appearing and make it harder for offenders to find and share.

With 70 dedicated staff, IWF is one of the biggest hotlines for tackling child sexual abuse imagery in the world, and the largest in Europe.

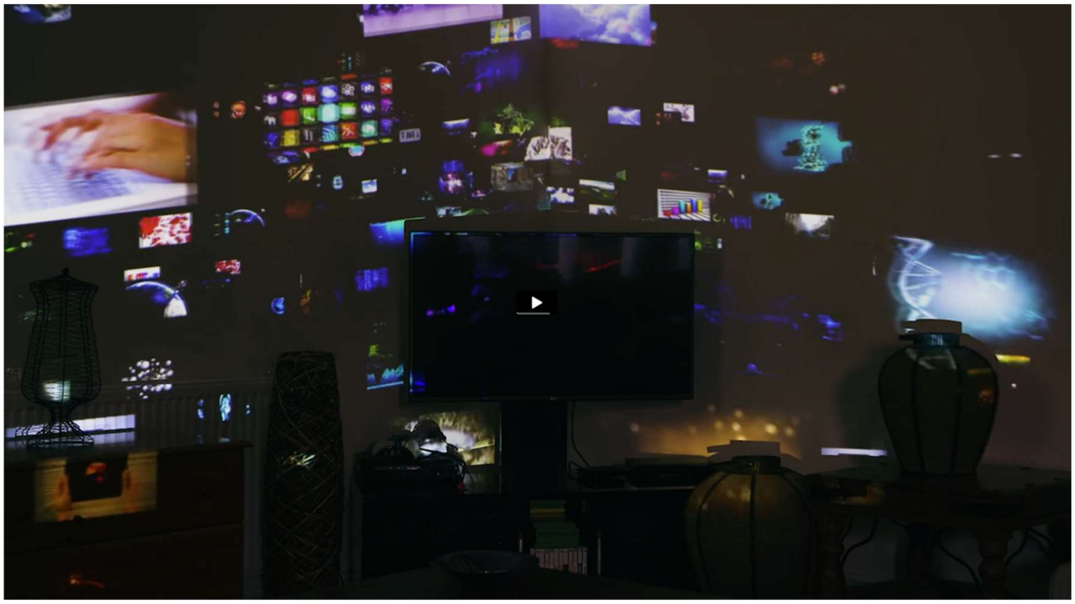
Our work is made possible by our 180+ Members and corporate partners, as well as funding support from Nominet, Thorn, the UK Government's Home Office, the Safe Online Initiative at End Violence and Oak Foundation.

In 2022:

- **375,230** reports were assessed by IWF (+4% on 2021)
- **255,588** reports were confirmed as containing child sexual abuse imagery, having links to the imagery, or advertising it (+1% on 2021). These reports are of websites and newsgroups.
- Total number of actioned reports that were tagged as including self-generated content was **199,363** (+9% on 2021 which was 182,281).
- There was a **13 percentage** point increase (from 23% to 36%) in sexual abuse imagery of 7-10 year olds, (regardless of how it was created) and a 10 percentage point decrease (68% to 58%) in sexual imagery of 11-13 year olds compared to the year before. However, imagery of 11-13s is still the most prevalent.
- We curated **1,663,106** quality-assured hashes – or digital fingerprints – of unique child sexual abuse images.

Welcome

About IWF



The Internet Watch Foundation (IWF) is a technology-led, child protection organisation, making the internet a safer place for children and adults across the world. We're a not-for-profit organisation working closely with police, governments and NGOs globally, who trust our work. We detect, disrupt, remove, and prevent online child sexual abuse material using our expertise and resources as effectively as possible.

What we do

Child sexual abuse images and videos are just as much a weapon as a knife. We actively search for this imagery and for the past 26 years, we've given people a safe place to report it to us, anonymously, now covering 50 portals in countries and 2.6bn people.

We assess every report we receive. If it shows the sexual abuse of a child, we make sure the image or video is removed from the internet.

To do this effectively, we develop technology-for-good: We provide bespoke services, products and datasets to our industry Members to prevent the imagery from re-appearing and make it harder for offenders to find and share.

With 70 dedicated staff, IWF is one of the biggest hotlines for tackling child sexual abuse imagery in the world, and the largest in Europe.

We care. Our work relies on compassionate and resilient staff members, who are highly trained and carefully looked after.

How you can support us

We encourage others to play their part, whether it is reporting to us, funding us, or collaborating on the best technology and research.

The children in these pictures and videos are real. The suffering captured in this imagery and the knowledge that it could be shared can haunt a victim for life.

That’s why it’s our mission to remove this material for good. And to show every child there is someone out there who cares enough to help.

Our work is made possible by our 180+ Members and corporate partners, as well as funding support from Nominet, Thorn, the UK Government’s Home Office, the Safe Online Initiative at End Violence and Oak Foundation.

2022 Highlights

February

Safer Internet Day 2022 celebration

Along with partners at the UK Safer Internet Centre, we proudly took part in the global celebration of Safer Internet Day 2022, which promotes the safe and positive use of digital technology for children and young people. The theme was ‘All fun and games? Exploring respect and relationships online’.

March

Prevention campaign for children with SEND

Children with special educational needs or disabilities (SEND) are three times more likely to experience sexual abuse online. That’s why we launched a campaign to help these children and their parents understand more about this crime and how they can better protect themselves. Read our article.

April

Gerson Nozea
Country Director, Rapha International, Haiti
The knowledge that this suffering could be shared again and again

IWF’s 25th anniversary

In our 25 years of service, our expert analysts have assessed over two million reports of child sexual abuse and helped to remove millions of child sexual abuse images and videos from the internet. Together with our Members, partners, law enforcement and government officials, we’ve helped save countless children from a lifetime of revictimisation.

MTN
Join our cause. Help children be children today, for tomorrow.
IWF Internet Watch Foundation
Meta

Africa Portal and Help Children be Children campaign launch

We joined forces with MTN, Meta, ICMEC and Child Helpline International to launch the Help Children be Children campaign and the Child Safety Online Africa Portal to increase public awareness of the impact of child sexual abuse material and help prevent its spread in Africa.

Read our press release.

May

IWF wins at British Data Awards
We were awarded Not for Profit of the Year at the British Data Awards 2022 which celebrates the organisations and people that are deeply passionate about data.
Read our press release.

June

Taskforce reaches one million hashes
One year since creation, our dedicated hashing taskforce marked the assessment and individual hashing of one million images of child sexual abuse from the UK Government’s Child Abuse Image Database (CAID) system.
Read our press release.

July

IWF launch new podcast

In July we launched our new ‘shortcast’ series, In Conversation With, starting with an in-depth discussion with Prof Hany Farid from the University of California, Berkeley, on the encryption vs privacy debate.

Read our article or catch up on the podcast.

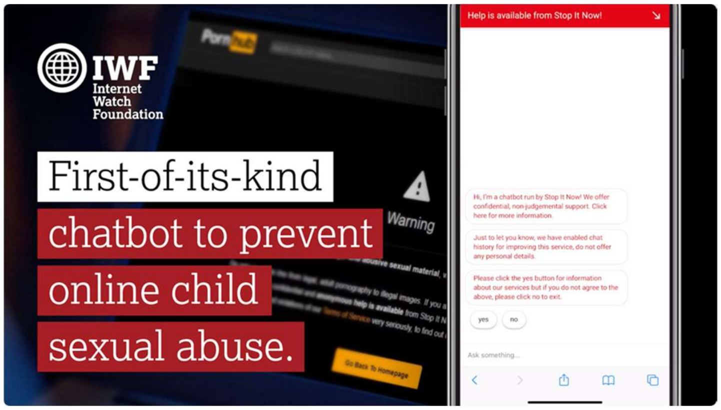
August

A new partner chooses IWF as charity of the year

Trenches Law made the IWF their Charity of the Year, supporting us by raising vital funds and spreading the word about our work.

Read our article.

September



Hi, I'm a chatbot run by Stop It Now! We offer confidential, non-judgemental support. Click here for more information.

Just to let you know, we have enabled chat history for improving this service, do not offer any personal details.

Please click the yes button for information about our services but if you do not agree to the above, please click no to exit.

Chatbot created to prevent viewing of child sexual abuse

Alongside our partners at Stop it Now! the IWF unveiled a first-of-its-kind chatbot, launched on Pornhub UK, designed to stop potential offenders searching for pictures and videos of child sexual abuse online and encourage them to seek help for their behaviour.

Bonus episode of our ground-breaking podcast released

We released a bonus episode of our ground-breaking podcast series, Pixels from a Crime Scene, which focused on a growing threat to children online.

October

CEO named in Computer Weekly's most influential women in UK tech list
Our Chief Executive, Susie Hargreaves OBE, was announced as one of Computer Weekly's top 50 Most Influential Women in UK Technology in 2022.
Read the article.

November

New 'crypto unit' announced
Our analysts identified a trend that showed cryptocurrency payments for child sexual abuse material doubled almost every year since 2015. In response, we launched a new 'crypto-unit'.
Read our press release.

THE NEW STATESMAN
POSITIVE
IMPACT AWARDS
6 DECEMBER 2022 | LONDON
CELEBRATING CHANGE FOR THE BETTER
IN POLITICS, BUSINESS AND SOCIETY.

Finalist in New Statesman Positive Impact Awards
The IWF was a finalist at the New Statesman Positive Impact Awards for Technology on account of our innovative contribution to the removal of child sexual abuse material online with IntelliGrade.
Read the article.

Independent Hotline Audit
We welcomed four independent inspectors into IWF at the request of our Board. They reported: "The IWF is an extremely professional and well-managed organisation led by a strong but caring and compassionate leadership team." Read the report.

December

A gala event to thank our partners, champions and advocates
The IWF hosted an event at Westminster that gathered guests from Government, the third sector, law enforcement and the tech industry to mark

another year of protecting children online. Read our article. Actor Samantha Morton spoke movingly of one parent’s experience trying to protect their child.

Welcome from our Chair

Andrew Puddephatt OBE, Chair of IWF

IWF occupies a unique place in the online safety landscape. It successfully nurtures positive and productive relationships with global technology companies, as well as other types of companies whose core values of protecting children reflect our own. Never has IWF's membership offering been so valued, and IWF's Members been so great in number.

We build and maintain the largest and most quality-assured database of illegal images which enables us to provide an unparalleled service to our Members. Our relationships with the UK Government, the incoming UK regulator, Ofcom, and law enforcement, particularly the UK's National Crime Agency are strong. Our partners recognise the crucial contribution we make to tackling online child sexual abuse. This is particularly evidenced by the role we've played over the past two years as the only non-law enforcement organisation with access to the national Child Abuse Image Database (CAID) where we have assessed and quality assured over two million images. We share those back with law enforcement to aid their work and also with industry to ensure duplicate images of child sexual abuse are not distributed on their platforms.

Over the past few years we've worked hard on our programme of engagement. This is all critical, of course, as we expect to see the introduction of the Online Safety Bill (OSB) in the UK and new legislation in the EU.

As the largest hotline in Europe, contributing 63% of all illegal content items to the Inhope database, our participation and expertise has never been in such demand. The nature of the crime changes constantly which is why the IWF plays such a central role. As an example, I'm struck by a study within this annual report which details the complexity of removing images and videos of child sexual abuse from forums, and how forums are responsible for distributing a large amount of this content – a fact which is not immediately apparent in our data.

The scale of online child sexual abuse material, and the desire of abusers to see more of this content has anything but abated. Our challenge, alongside companies providing online platforms and services, is to make the internet as safe and abuse-free as possible. This is no easy task, but one that the whole of the IWF team is up for. That's why this past year we've embarked on our biggest recruitment drive to date. We've expanded our hotline analyst team, tech team and corporate functions to support those across the organisation. This area of work never stands still. We're creating new services for Members, new ways in which Members can receive our services and bespoke arrangements to support specific requests. It's testament to the quality and granularity of our datasets that they're in such demand.

It is also why, in 2023, we will highlight the need for a more sustained, high level national campaign focusing on preventing the abuse of children. We believe this should be a priority supported at the highest level of our Government and should consider the recovery response, in addition to prevention work, for children who have suffered online sexual abuse and exploitation.

As the data in this report reveals, the IWF has never been so important or so needed. For the past five years we have worked closely with the Government to ensure that the OSB delivers 'good' regulation that puts the interests of children at its heart and does not, however unintentionally, in any way compromise or diminish our work. That's why we're proposing IWF plays a central role, in partnership with Ofcom, to support the regulation of criminal child sexual abuse material online for the UK.

In the year ahead, we're ready to work with Ofcom to look at how best to scale up the deployment of our services and activities within scope of the UK's Online Safety Bill.

And as I begin my final year as IWF Chair, I can say that it’s been a privilege and I am really going to miss working with both the exemplary Board of Trustees and the IWF team. The executive and whole staff team consistently work hard to meet their enormous mission to eliminate online child sexual abuse.

In 2022, the IWF was once again put under a microscope by an independent audit team, led by retired High Court Judge Sir Mark Hedley, and were found to be an “extremely professional and well-managed organisation led by a strong but caring and compassionate leadership team”. Under Susie Hargreaves’ leadership they rise to every challenge to be a global beacon of excellence.

My overall aim in my final year is to ensure that the Government and Ofcom do the right thing and protect the legacy and crucial work of the IWF in the Online Safety Bill regime.

Welcome from our CEO

Susie Hargreaves OBE, Chief Executive Officer of IWF

Tackling online child sexual abuse has never felt more in the spotlight. We're all grappling with new and changing technologies and shifting behaviours of criminals online who seek to create and distribute child sexual abuse imagery, often for monetary gain.

It's heart-breaking to reveal, again, that in 2022 we've seen increases in the number of reports which include images and videos of the sexual abuse of children aged 7-10. And that sexual imagery created of children when they are online, often in the supposed 'safe spaces' of their bedrooms, now accounts for almost four in every five reports.

This is my 12th year leading the IWF and I am immensely proud of everything we have achieved and how we have grown to enable us to tackle the problem, but there's absolutely no satisfaction in knowing that we are seeing more and more children being abused and that they are getting younger.

At the IWF we've always been careful not to describe in detail what we see as we don't want to upset people, but we're starting to believe that we have to start being more upfront and honest about the extent of the abuse we find, as the public needs to realise that we are talking about seven year olds, naked, inserting items into their vaginas under the direction and coercion of nasty, manipulative individuals. The children are totally unaware that this has been recorded and will be shared time and time again on the internet by their abusers. And the truth is that it can affect any child from any background as all young children left unsupervised with a camera-enabled device and an internet connection are at risk.

This is why we need to do everything we can as a society to work with partners across the world to stop the abuse happening in the first place. We believe that this is possible and can be achieved by having three fundamental pillars in place: (i) proper legislation and well-resourced law enforcement, (ii) tech companies doing everything possible to prevent the upload and distribution of images so they can't be shared and (iii) a programme of education and awareness raising for both children and parents/carers so that they understand the dangers and how to keep themselves and their children safe online.

But we won't get there if we don't work together and put the needs of children first. This is why we are standing in solidarity with our child protection partners to oppose the introduction of end-to-end encryption on platforms without there being the necessary technically-possible child safeguards in place. Likewise, we have been working closely with colleagues across the UK Government to ensure that the Online Safety Bill does what it sets out to do and makes the UK a safer space to be online and as part of that, protect the critical work of the IWF, as without us it will be children who will suffer.

Empowering children, and those who care for them, is an absolute priority, and after the first full year of operating Report Remove with our NSPCC partners, we've seen how boys, many aged 16-17, are most often reporting sexual images of themselves to us. Cases of sexually coerced extortion are rising among this group, as criminals seek to extort money from their victims. Report Remove is clearly needed by young people and it has immense potential to be replicated in other countries.

The work of the IWF is a team effort and every single member of staff, regardless of their role, plays their part and always goes the extra mile to do whatever they can to stop these images being circulated. That's because they know that every image is a real child who has been abused in the most horrific way.

We won’t stop until every single image has been removed from the internet because children need to know we are out there fighting their corner.

European Commissioner for Home Affairs, Ylva Johansson

“Child sexual abuse is a heinous crime with lifelong consequences for the victims. The online space offers new opportunities for offenders to groom and abuse children and to exchange child sexual abuse material. We need a strong response. Targeted and robust prevention plays a key role in protecting children against child sexual abuse and exploitation. The new proposal for a Regulation to prevent and combat child sexual abuse focuses first and foremost on prevention by ensuring that digital spaces have the necessary protections to keep children safe from harm and to stop the distribution of child sexual abuse material that fuels demand for new abuses.

An effective fight against this crime requires a comprehensive, multi-stakeholder and global approach, with tools to facilitate reporting, investigations and assistance and support to victims. The Internet Watch Foundation plays a key role in finding, reporting and removing online records of child sexual abuse. This IWF report indicates that the threat of child sexual abuse online is on the rise, notably through the increase in “self-generated” content which frequently results from grooming and sextortion. The report provides important evidence to help prevent and combat these crimes.”

Image credit: photographer Claudio Centonze, European Union 2023

Minister for Safeguarding, Sarah Dines MP

Online child sexual abuse is an appalling crime that the UK Government is committed to stamping out, working alongside industry and civil society both in the UK and globally.

Worryingly, the scale and severity of online child sexual abuse has increased year on year as evidenced by IWF's annual reports. This year is no exception. The 2022 report shows the volume of detected child sexual abuse material has outpaced that of last year. There has also been a 60% increase in 7-to-10-year-olds appearing in these horrific images.

The Tackling Child Sexual Abuse Strategy, published in January 2021, sets out the UK Government's long-term ambition to tackle all forms of child sexual abuse, whether it takes place online or offline in the family home, institutions, or communities, in this country or overseas.

Since the publication of the Strategy, we have made progress on ground-breaking legislation, such as the Online Safety Bill and the Police, Crime, Sentencing and Courts Act 2022. We have also invested in the world-leading Child Abuse Image Database, which is helping to increase the efficiency of efforts to tackle cases of online child sexual exploitation. The Internet Watch Foundation has made meaningful contributions to these successes with their continued engagement on the Online Safety Bill and strengthening the potency of the Child Abuse Image Database with their hash sharing project.

Recently, I visited the Internet Watch Foundation’s headquarters and was impressed by the work that they do. For example, the development and maintenance of the Report Remove tool, which is giving children an opportunity to reclaim control over harmful imagery of themselves shared online. Or more recently the introduction of the ground-breaking chatbot in partnership with the Lucy Faithfull Foundation, which will not only discourage offending, but also encourage those displaying early signs of harmful sexual behaviours to seek help.

I am grateful for the Internet Watch Foundation’s continued collaboration in our mission to not only making the UK the safest place in the world to be online, but to make the internet a safer place for everybody.

Secretary of State for Science, Innovation and Technology, The Rt Hon Michelle Donelan MP

I am delighted to welcome the Internet Watch Foundation's annual report for 2022, which highlights their crucial role in protecting children every day from the horrific extent of child abuse and exploitation online.

The Internet Watch Foundation's highly dedicated team remains at the forefront of the rapid detection and removal of child sexual abuse online through the use of cutting-edge technology. The information in this report offers insights to Government, online services and organisations globally on the prevalence of content and advice on how we can protect children. This is especially crucial at a time when we are legislating for the UK to become the safest place in the world for children online via the newly strengthened Online Safety Bill.

Since I took control of the Online Safety Bill, I have added new child protection measures that make the Bill as a whole even more robust for children – showing that without doubt, the UK is committed to protecting children online. The Internet Watch Foundation's support for our work to strengthen the Bill for children has proven incredibly valuable, and we will make sure that these vital protections are implemented as quickly as possible.

Because fundamentally, I believe that the UK has a choice to make when it comes to the way our children interact with the online world. Either we allow the power for children's online lives to rest with social media giants, or we apply our longstanding norms and values when it comes to children by intervening to protect them. My firm view, and I am sure yours too, is that we must legislate now to ensure the latter is put into law. Transparency, accountability and robust protections for children – these are the principles that we are putting into law once and for all.

Backed-up by an independent regulator with unprecedented tools to hold social media companies to account for failing in their duties to protect children, we will be on a strong pathway to achieving the goals of the Internet Watch Foundation and of the Government: to protect children.

But I want to be clear that I do not see the Online Safety Bill as a silver bullet to the issues that children face online. In fact, I want this to be the first step in a wider package of action across Government that will mean future generations of children never have to experience some of the appalling content documented by the Internet Watch Foundation in recent years. I am determined to ensure that we never lose focus or become too self-congratulatory, but instead remain constantly vigilant to the threats posed by an ever changing online world.

This report reinforces how critical the Internet Watch Foundation's role is to making the UK the safest place in the world to be online, and I thank the Internet Watch Foundation for their continued vital work.

Our role in the UK Safer Internet Centre

UK Safer Internet Centre Directors, Will Gardner OBE, Emma Hardy, David Wright

The UK Safer Internet Centre (UKSIC) is a leading global partnership helping to make the internet a great and safe place for everyone.

We provide support and services to children and young people, adults facing online harms, and professionals working with children.

A bridge between Government, industry, law enforcement and society, we are the engine of the online protection landscape in the UK, dealing with both prevention and response.

We are unique. Formed of three foremost charities, Childnet, Internet Watch Foundation and SWGfL, we work together to identify threats and harms online and then create and deliver critical advice, resources, education and interventions that help keep children and young people, and adults, safe. We share our best practices across the UK and globally and we work alongside 30 other centres across the European continent.

In 2022, Nominet, the official registry for UK domain names, stepped up to support the UK's online safety sector by funding this work following the UK's departure from the EU. Prior to 2022, we had been funded by the European Commission as the Safer Internet Centre for the UK.

We focus our work around four functions:

- An awareness centre where we provide advice and support to children and young people, parents and carers, schools, and the children's workforce.

- Three helplines which provide support to professionals working with children and young people with online safety issues, and support to all adults facing issues with harmful content and non-consensual indecent imagery online.

- A hotline which provides an anonymous and safe place to report and remove online child sexual abuse images and videos wherever they are found in the world.

- A voice to young people: We operate a Youth Advisory Board, and we nurture youth participation, providing a focus on youth voice to give young people agency to make a difference in their school communities.

UKSIC is the proud coordinator of Safer Internet Day in the UK.

Trends and Data

Our Hotline Director: Children deserve more

By Chris Hughes

As another operational year in the Hotline closes, a new one quietly and seamlessly begins in the Hotline without fanfare or fuss.

As with all New Year's resolutions or end of year reports, date and time markers help us reflect and measure what we achieved and gives us focus to consider our goals and ambitions for the year ahead.

I am fortunate to head up an exceptionally dedicated team of analysts who, each year, commit to doing a job that is challenging at both a personal and professional level; their work requires resilience, courage, and a selflessness that few of us are expected to face in our daily jobs.

We should all rightly celebrate the work of the Analysts and Content Assessors; however, the sad truth is that as each new year quietly starts, we know that there will inevitably be much more to do in the year ahead, with many more children for the first-time becoming victims of online sexual abuse while their images are publicly traded and shared and treated as a commodity.

The insights and statistics provided in this report are important for the very reason that each statistic represents the underserved and abhorrent abuse or exploitation of a child by an adult.

I have a single ask of everyone reading this report; it is simply that in 2023 we should all find reasons for why we can and should do more. We should not settle or be comfortable with the idea that because we are doing something, we are doing enough.

Excellent and valued work is being done across different sectors by different stakeholders, and that is to be applauded, but let us all aspire to raise our game in 2023. Our children deserve nothing less.

Reports analysis

In 2022

We assessed a webpage every one-and-a-half minutes.

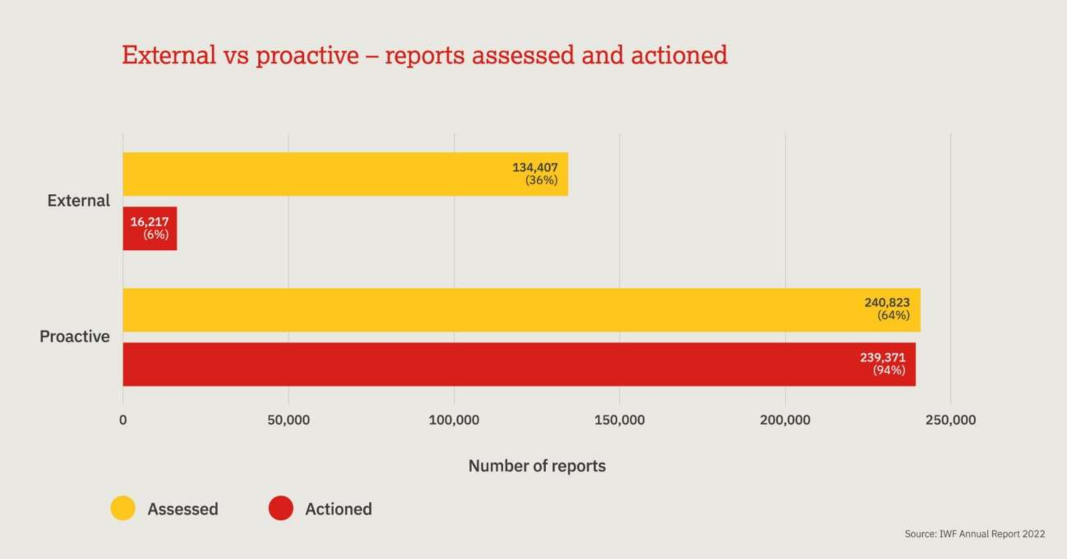
Every two minutes, that webpage showed a child being sexually abused.

People report to us at iwf.org.uk, or through one of the 50 Reporting Portals around the world, in multiple languages. All reports are assessed at our headquarters in the UK. We also actively search the internet for child sexual abuse imagery. We call this, ‘proactive searching’.

- **375,230 reports were assessed by IWF** (4% increase from 2021):
  - 375,153 were reports of webpages, and
  - 77 were reports of newsgroups
- 255,571 URLs (webpages) were confirmed as containing child sexual abuse imagery having links to the imagery or advertising it (1% increase from 2021). Each URL could contain one, tens, hundreds or even thousands of individual child sexual abuse images or videos.
- Additionally, 17 newsgroup reports were confirmed as containing child sexual abuse imagery.
- No reports were confirmed as UK-hosted non-photographic child sexual abuse imagery (prohibited images).

We use the term ‘**actioned**’ to indicate a report which was found to contain child sexual abuse material, which we therefore took a number of active steps to remove from the internet.

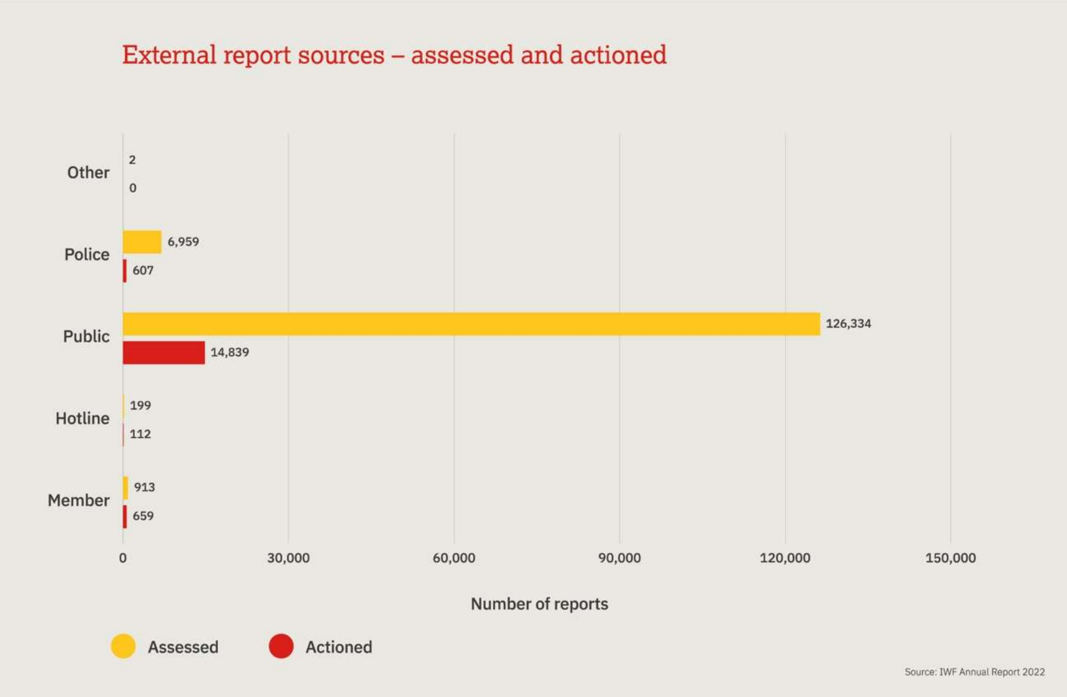
You can read more about UK-hosted and globally-hosted child sexual abuse material.



External vs proactive – reports assessed and actioned

Source: IWF Annual Report 2022

This chart compares proactively sourced reports (where our analysts search for content) and those reports which came to us via external sources.



External report sources – assessed and actioned

Source: IWF Annual Report 2022

This chart shows a breakdown of the external sources which report into us and report numbers from each source. The five sources are: Public, Police, Member, Other and Hotline.

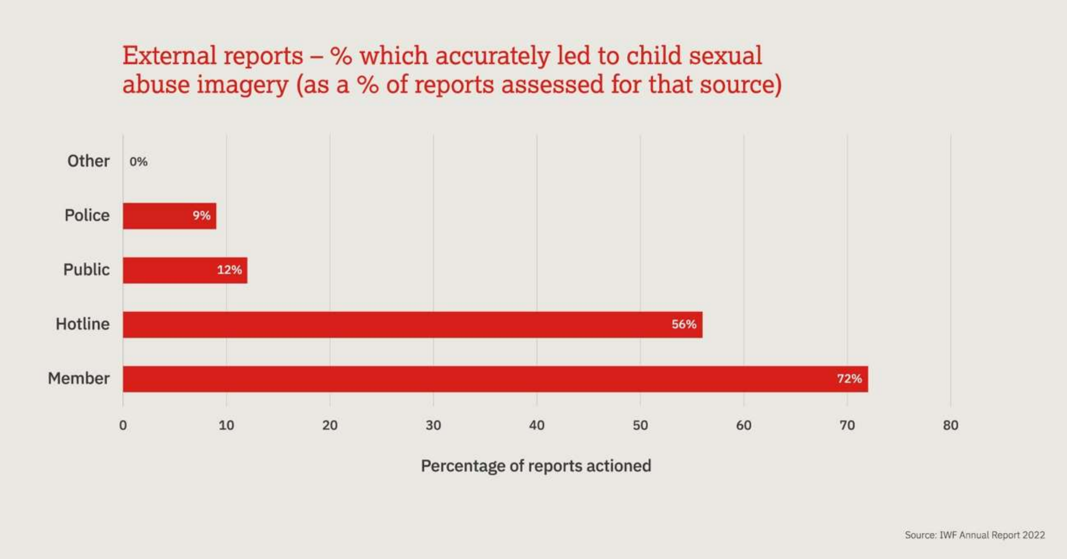
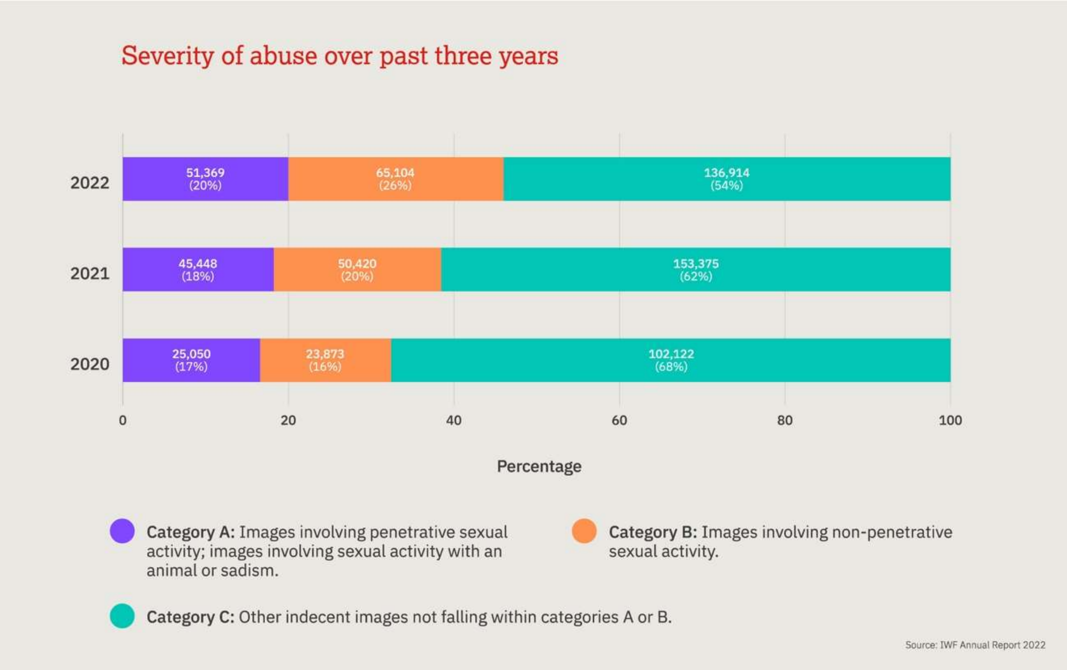


Chart showing the percentage of reports which were actionable (contained child sexual abuse material) from each external source. The five sources are: Public, Police, Member, Other and Hotline.

Public report source accuracy

126,334 reports were assessed by our Hotline which came from the public. **26% (29% in 2021) of these reports correctly identified child sexual abuse content.** This figure includes newsgroups and duplicate reports (where the same criminal URL has been reported multiple times).

Note: Each year, a number of these are adverts or links to child sexual abuse material.



Severity of abuse over past three years

Source: IWF Annual Report 2022

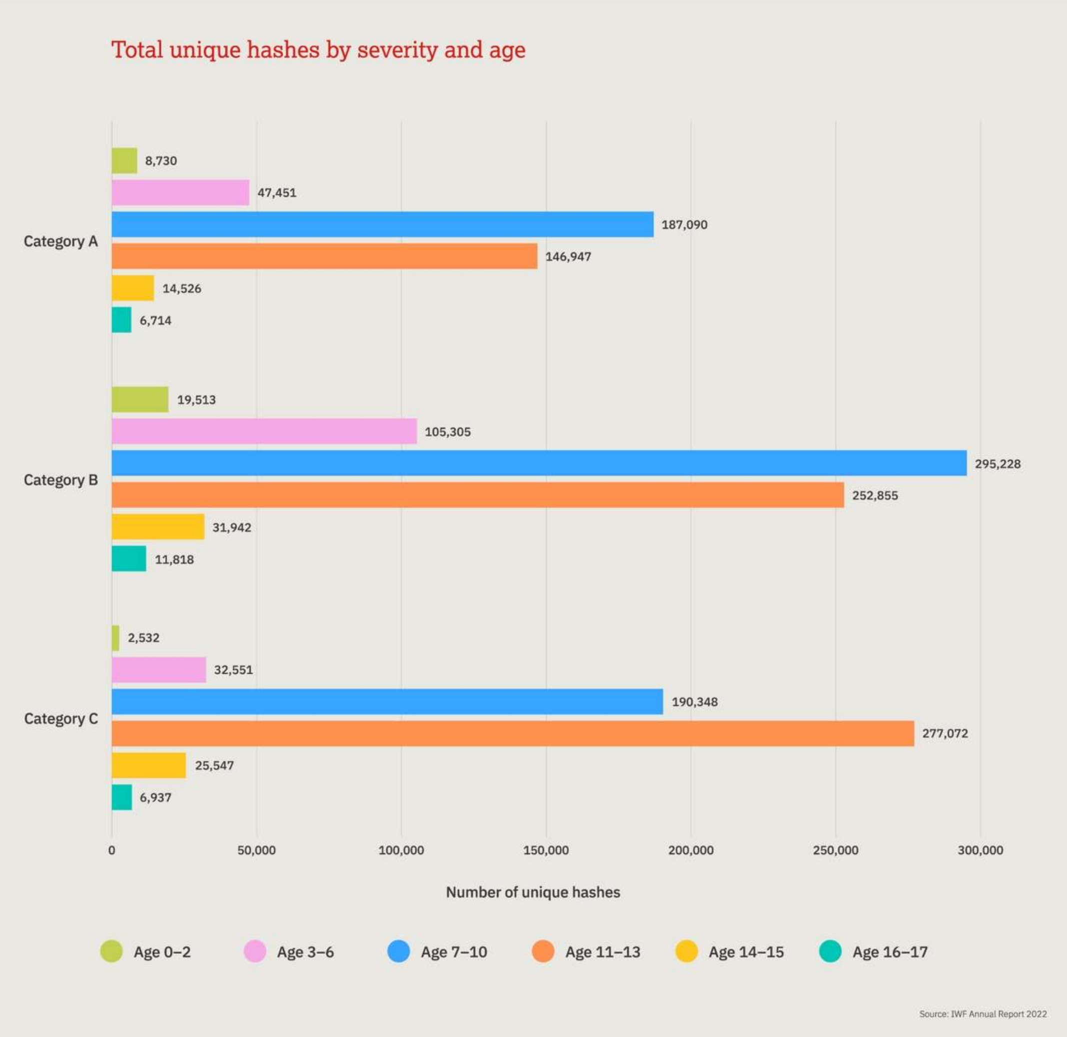
This chart shows the severity of child sexual abuse according to UK Category A, B and C.

Our quality-assured hash data

A hash is a type of digital fingerprint, or string value that identifies a picture of confirmed child sexual abuse.

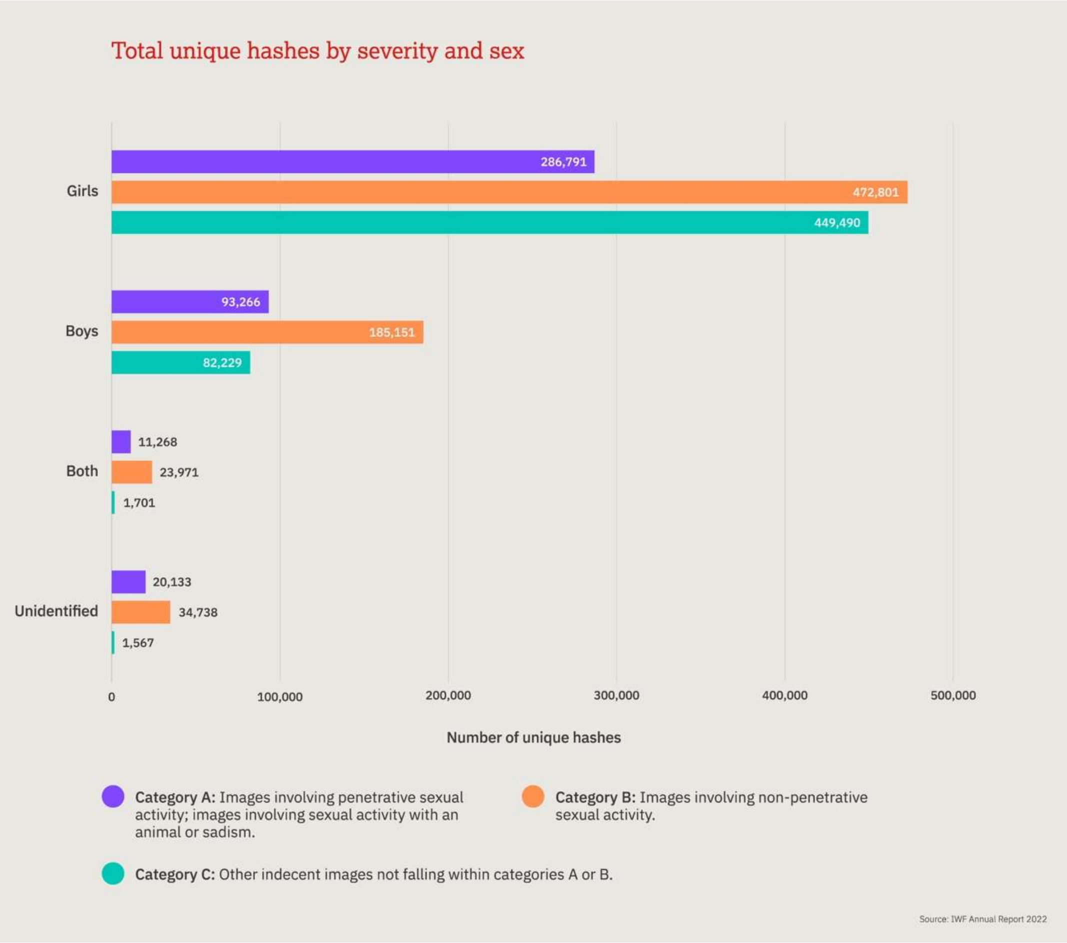
Each hash is completely unique. Once an image has been hashed, it can be recognised quickly. This means thousands of criminal pictures can be blocked from ever being uploaded to the internet in the first place.

By the end of 2022, the IWF had hashed **1,663,106** individual images since 2016. In 2021 we launched our Taskforce following some funding we received from Thorn to do this work. You can read more about this and our partnership with the UK Government's Child Abuse Image Database here.



Source: IWF Annual Report 2022

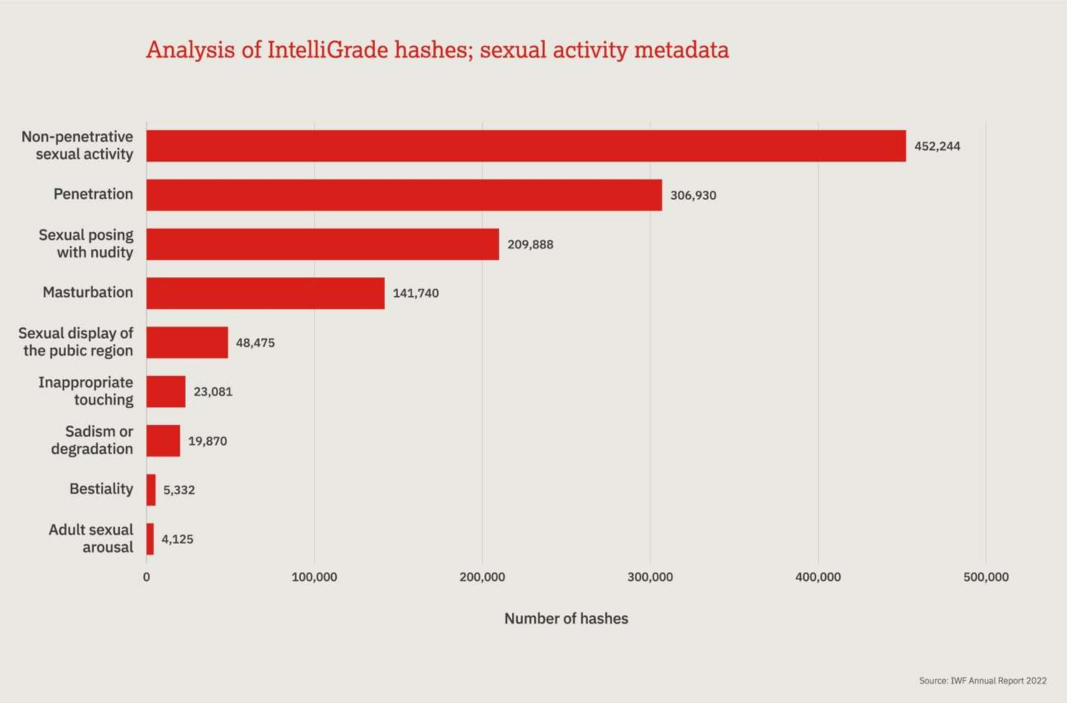
This chart details unique hashes of child sexual abuse split by age and severity (category). The majority of hashes in both categories A and B are of children aged 7-10 years old.



Total unique hashes by severity and sex

Source: IWF Annual Report 2022

This chart shows the unique hashes of child sexual abuse split by severity (category) of abuse and sex of the child. Most of the hashed images across all severity categories depict girls.

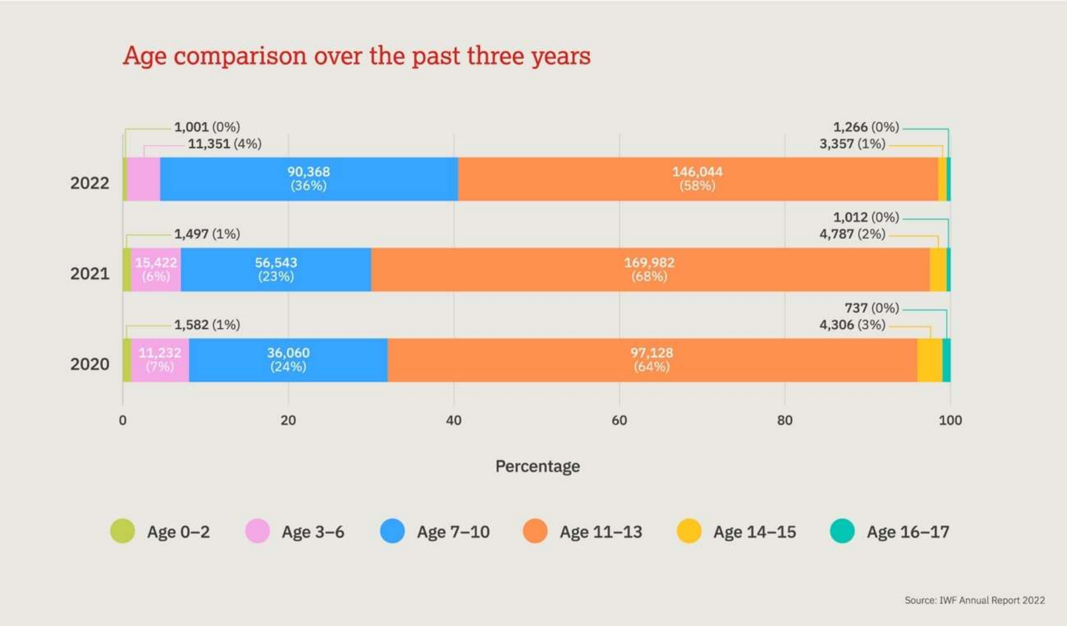


Source: IWF Annual Report 2022

This chart provides more detail on the exact nature of the abuse seen in an image which has been hashed by our analysts using our bespoke software, IntelliGrade. You can read more about IntelliGrade here.

Analysis by age

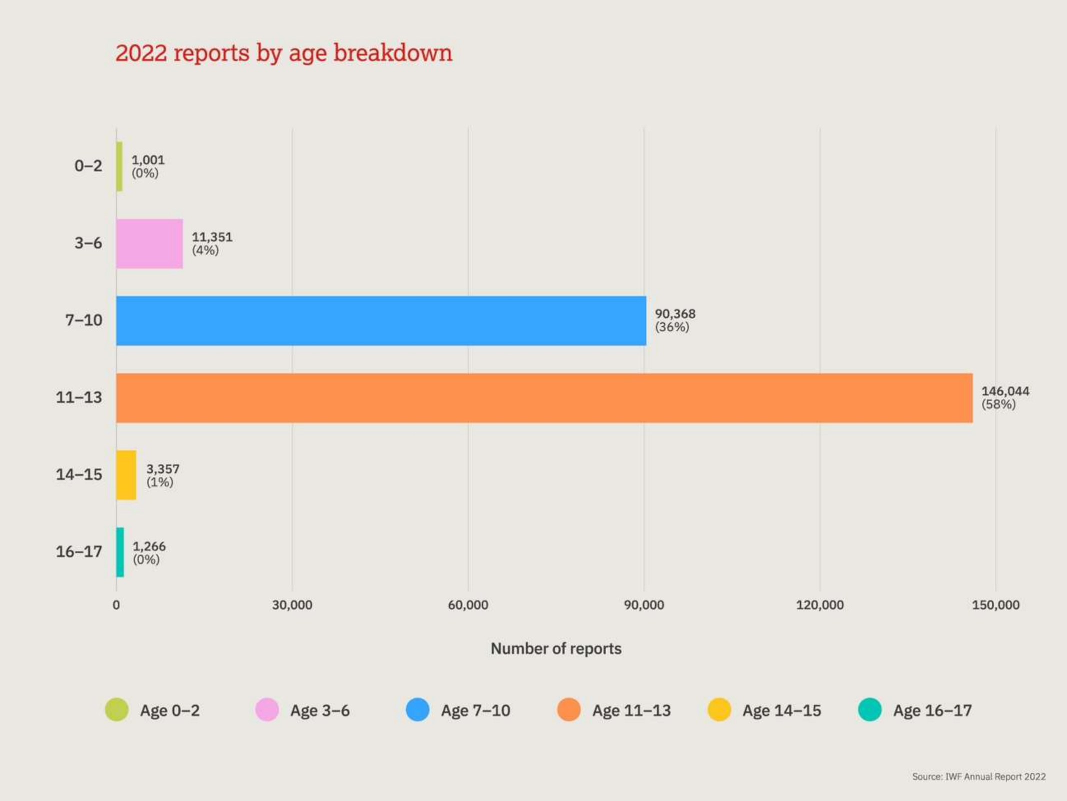
Overview


Age comparison over the past three years

Source: IWF Annual Report 2022

This chart provides a three-year look at the number, and proportion, of child sexual abuse URLs identified by IWF analysts split by age of the youngest child seen in any image upon that URL.

Over the past three years, children aged 11-13 are most often seen, however a 10 percentage point decrease was noted in 2022, compared to 2021. We also noted a 13 percentage point increase in the number of 7-10 year old children.

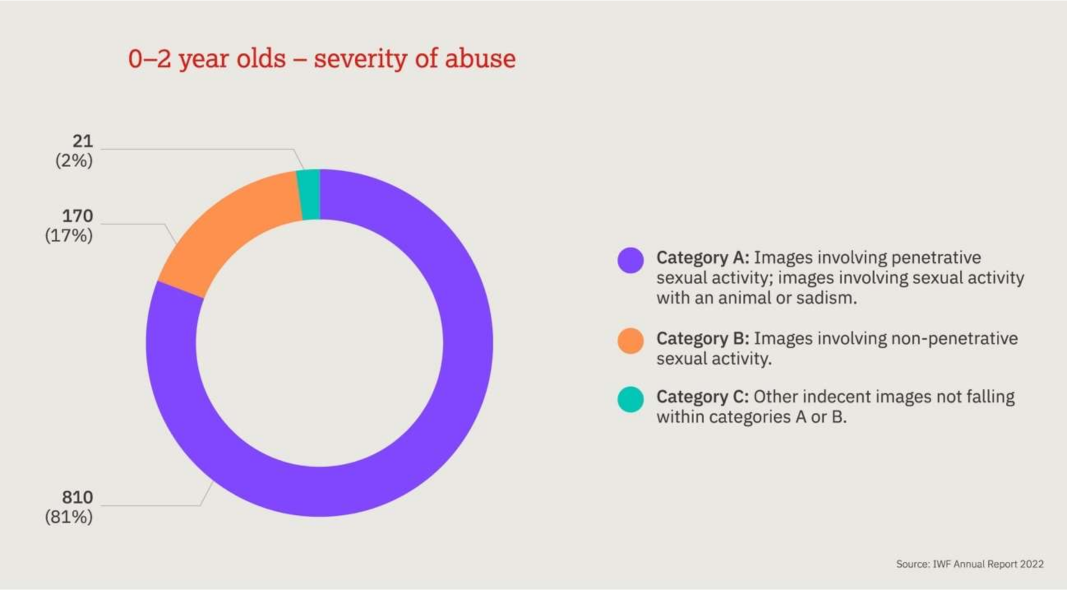


Source: IWF Annual Report 2022

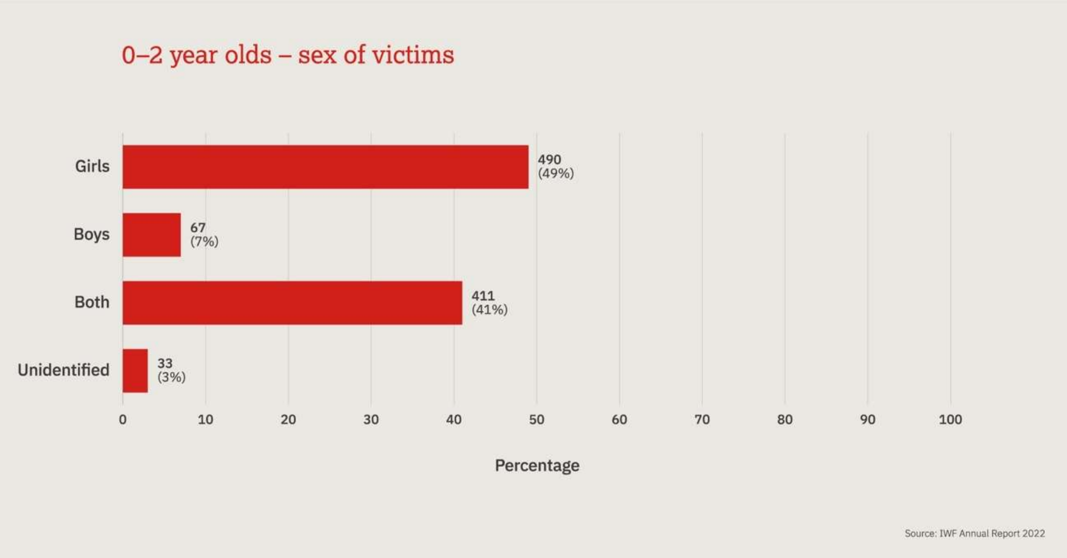
This chart provides a breakdown for all child sexual abuse reports in 2022, by age of the youngest child seen.

0-2 years: Babies and toddlers

Every year, we see a greater proportion of Category A images – showing the most severe, sadistic forms of sexual abuse – involving babies, toddlers and even newborns. In 2022, we also continued to see many Category B images, suggesting that in almost all images of infants, an abuser is present.



Source: IWF Annual Report 2022

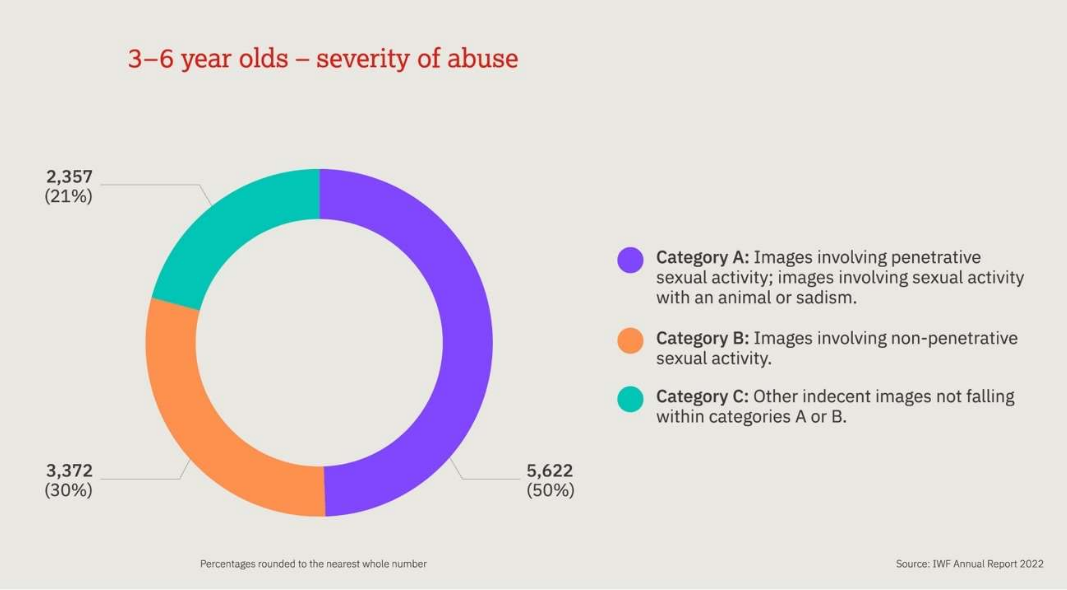


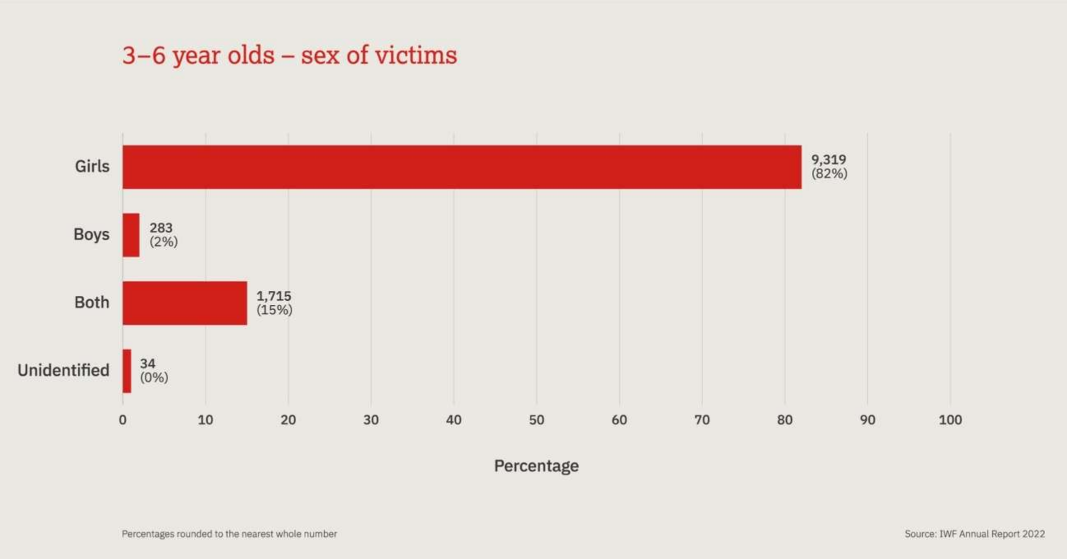
Source: IWF Annual Report 2022

3-6 Years old: Young children

Younger children continue to be abused and exploited by criminals for commercial gain: we saw a high proportion of ICAP websites using videos of 3-6-year-olds to 'advertise' the sale of child sexual abuse images.

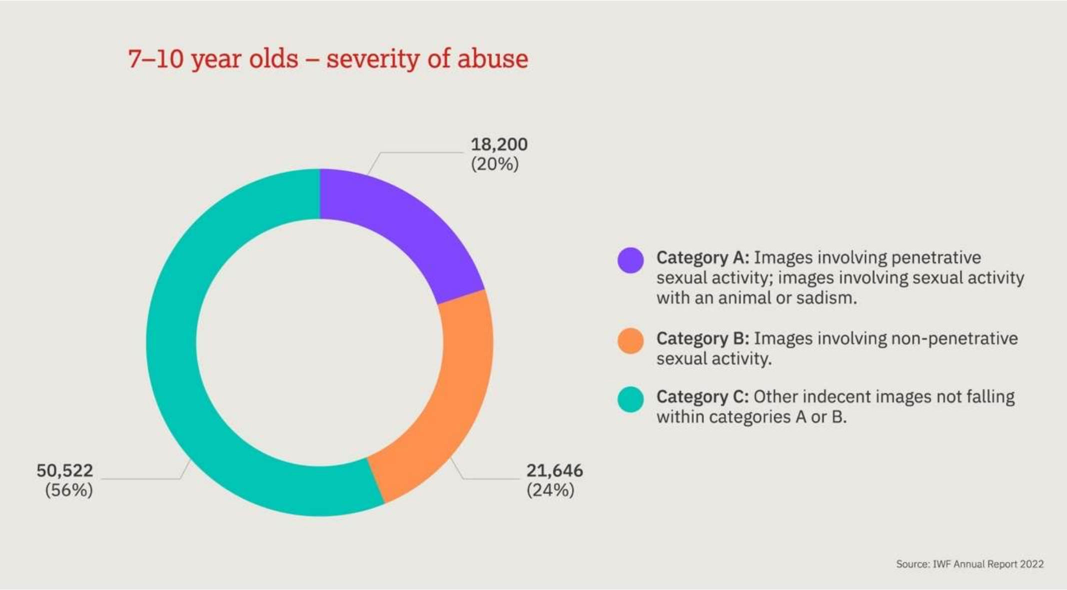
ICAP sites represent a new methodology of commercial child sexual abuse websites which we discovered in 2022. You can read more on ICAP sites here.



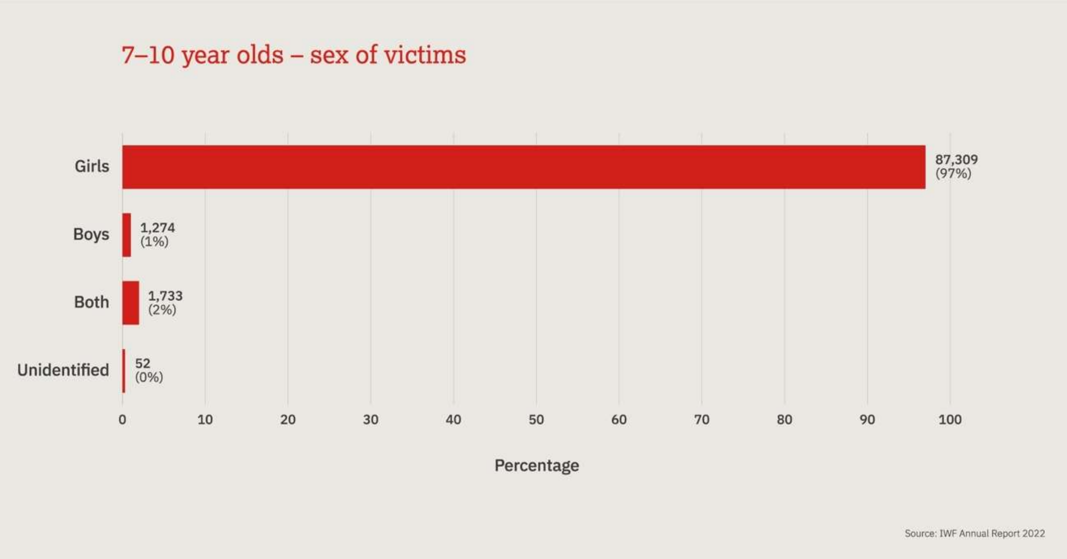


7-10 Years old: Pre-pubescent children

In 2022, we saw a 60% increase in the number of images including children aged 7-10 years old. As ever-younger children become more tech-aware and active online, they become more vulnerable to grooming and abuse by strangers – even in their own bedrooms.



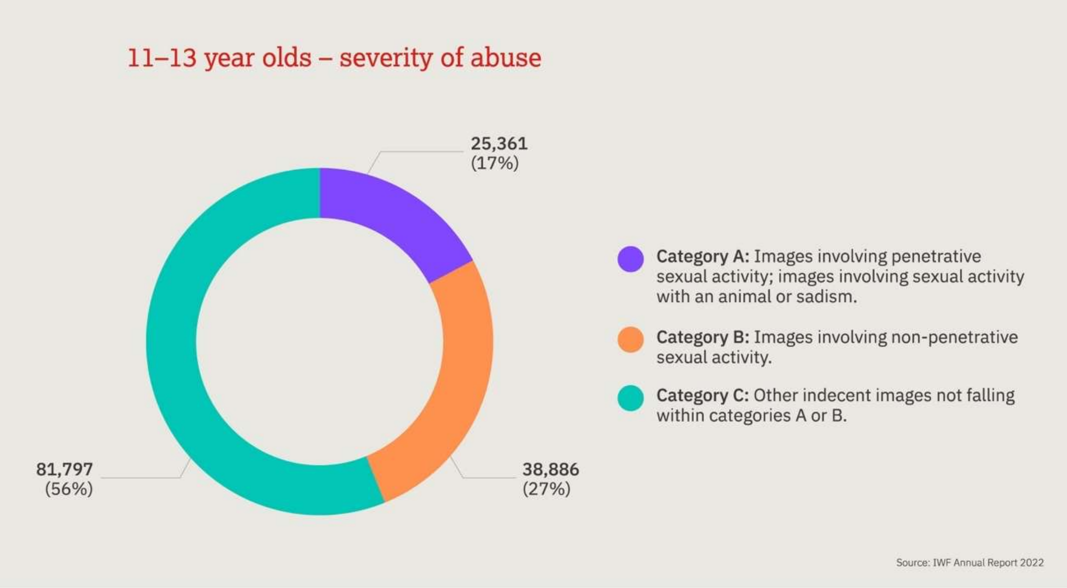
Source: IWF Annual Report 2022

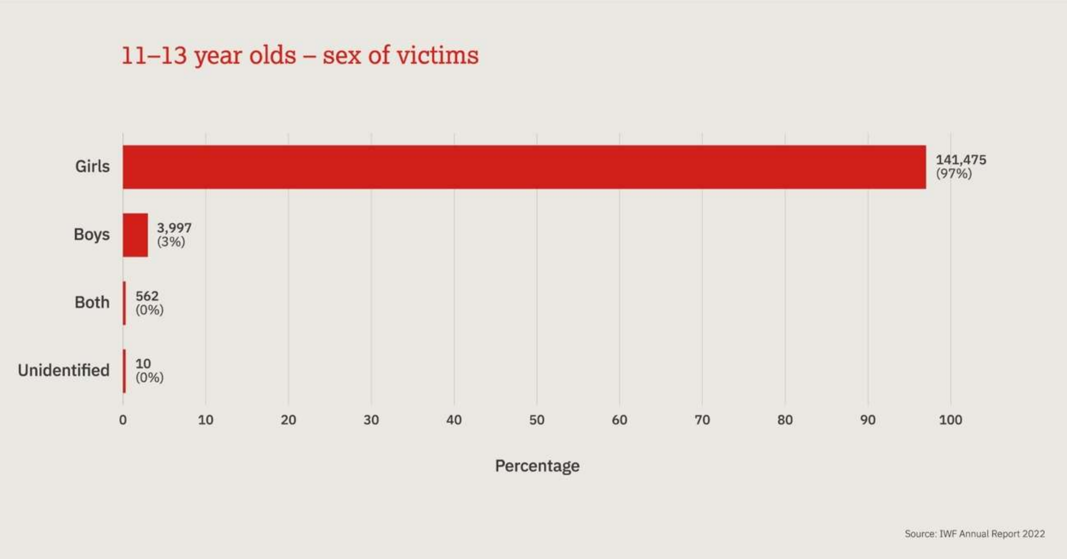


Source: IWF Annual Report 2022

11-13 Years old: Older children

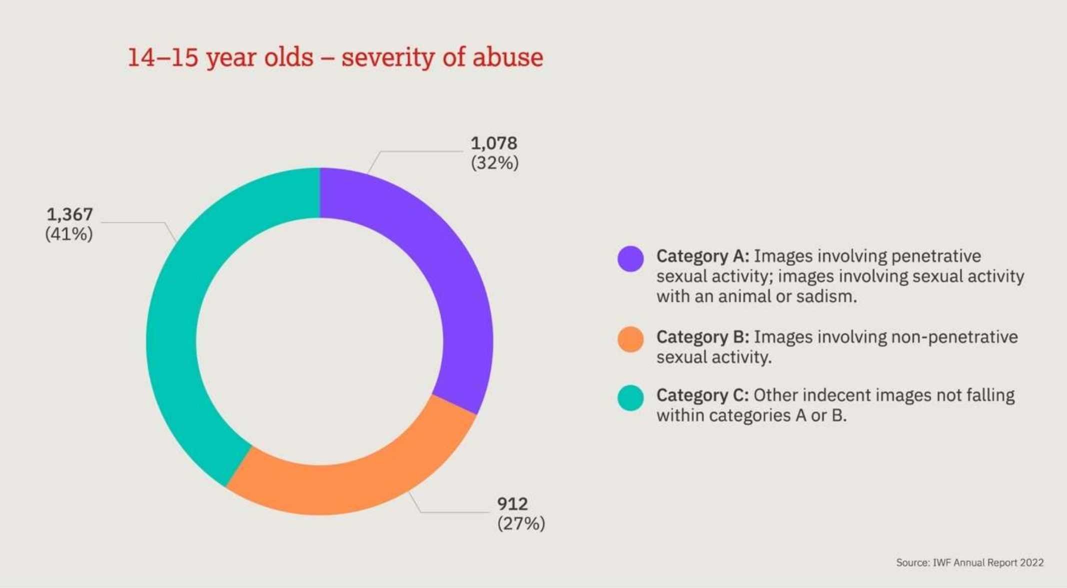
As in previous years, we saw more sexual abuse images of children aged 11-13 than of any other age group. Older children can be curious about the online world and keen to explore. Unfortunately, adult abusers – sometimes pretending to be children themselves – exploit this by manipulating children into performing sexual acts on camera, via a smartphone, tablet or laptop. In 2022, we saw a 14% decrease in imagery of this age group.



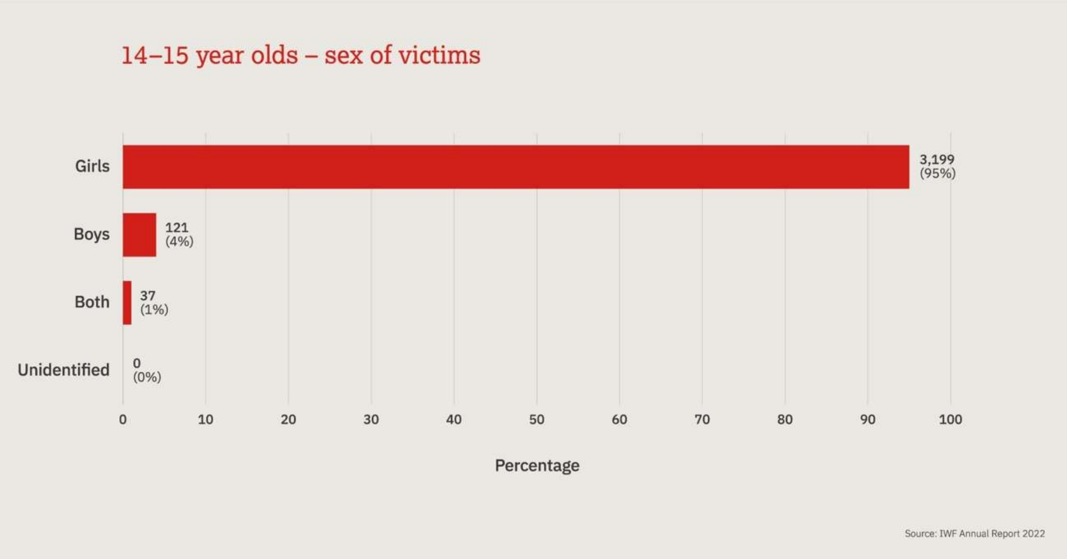


14-15 Years old: Younger teenagers

Girls are especially likely to be targeted and abused online; within this age group, girls account for 95% of the children we saw. The abuse doesn't stop when the child logs off – if images have been captured and saved, they can be shared across the internet again and again. Hashing helps prevent revictimisation by identifying images as they are uploaded.



Source: IWF Annual Report 2022



Source: IWF Annual Report 2022

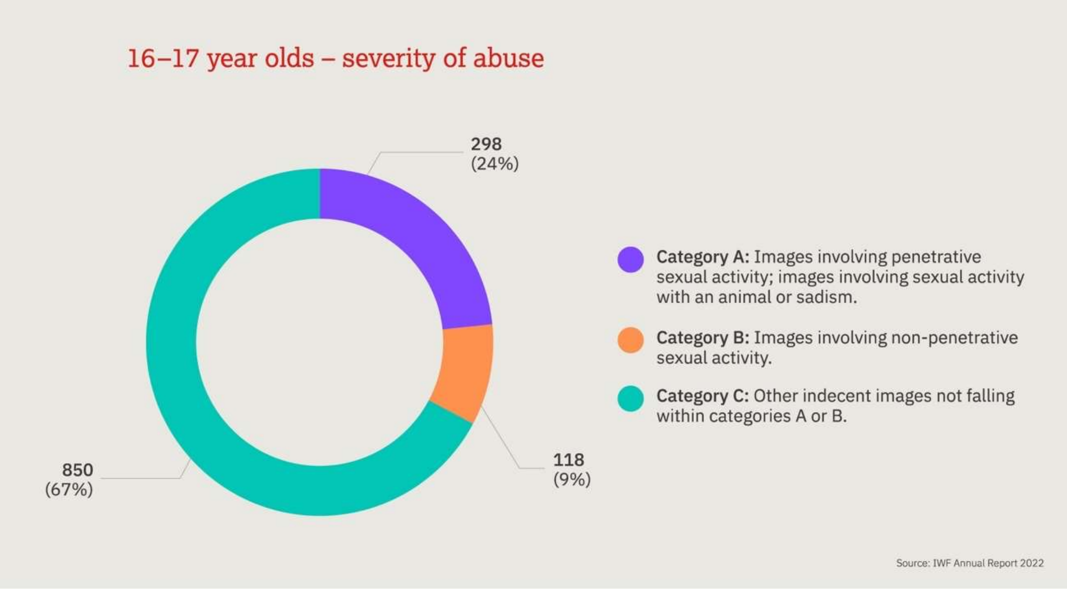
16-17 Years old: Teenagers

Increasing numbers of teenagers are using Report Remove to flag intimate images and videos to us that have been shared online without their permission. These are often cases of sexually-coerced extortion, where an image is stolen from the child and money is demanded in exchange for that image not being distributed.

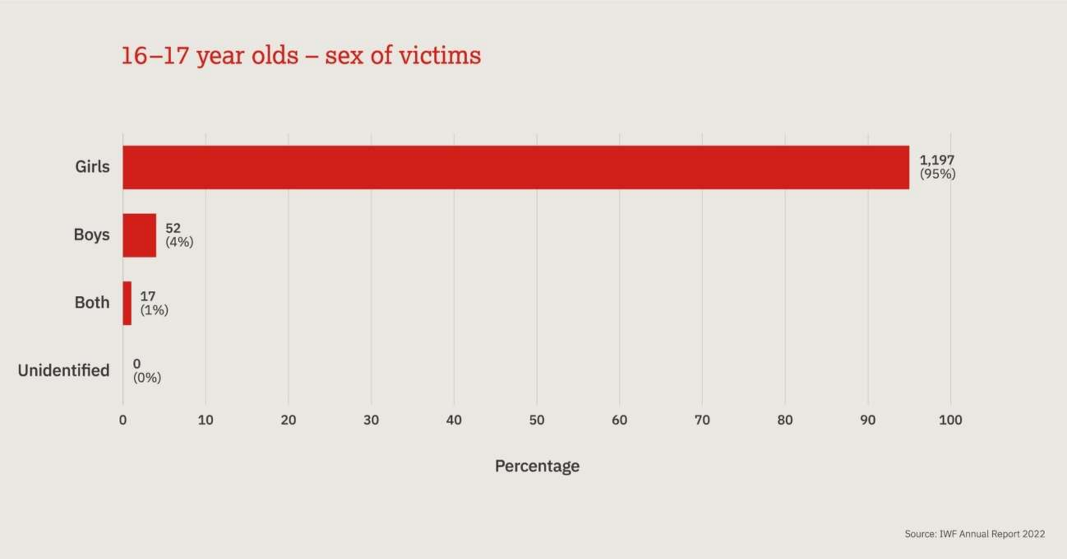
We know that sexually coerced extortion for financial gain seems to be more prevalent with boys rather than girls. Boys are typically lured into what they believe are mutual exchanges of sexual images where boys mistakenly believe they are sharing images with a girl or older woman.

Empowering children to reclaim control of their images also helps us remove images where the child's age might be unclear without verification.

Learn more about Report Remove here.



Source: IWF Annual Report 2022



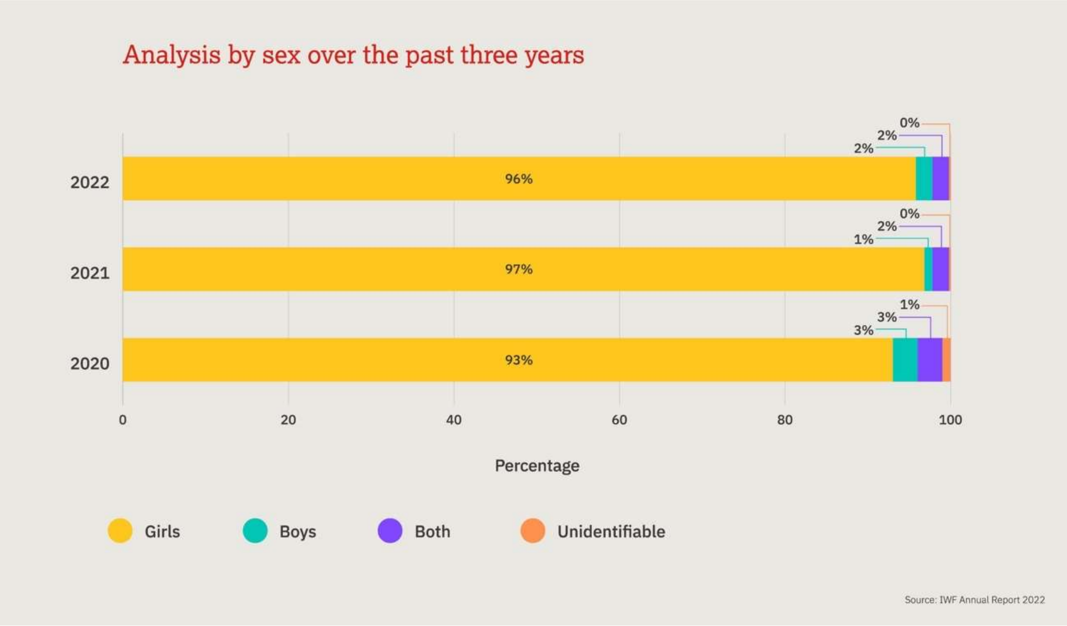
Source: IWF Annual Report 2022

Analysis by sex

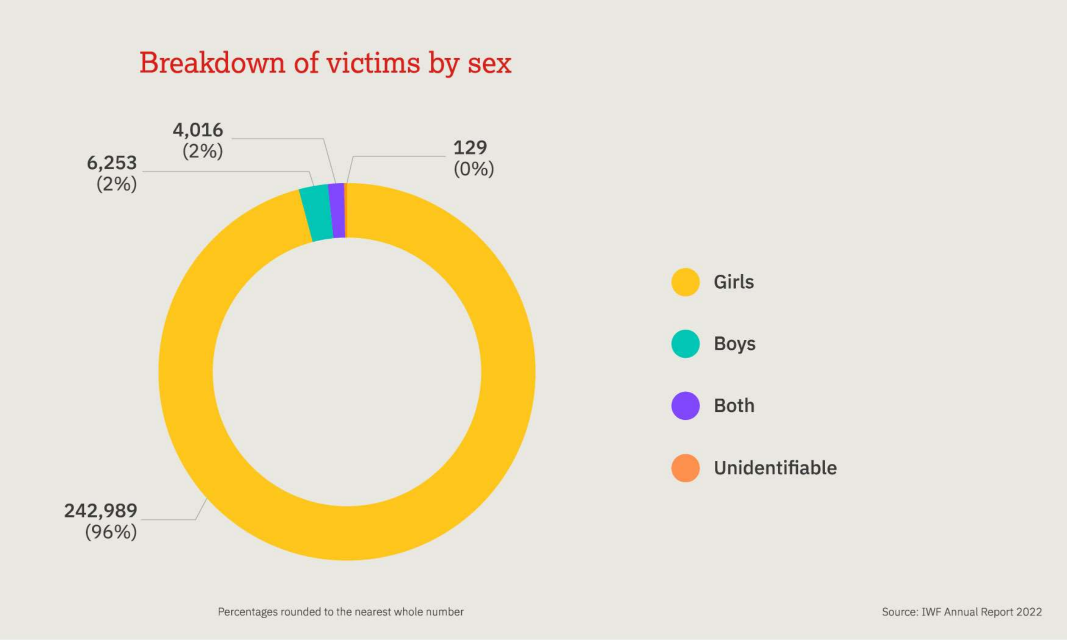
Overview

In 2022, as in previous years, most of the child sexual abuse images we saw showed girls only. We did, however, observe an increase in the number of images of boys this year compared to 2021. Images including both girls and boys continued to make up a small proportion of the criminal images we took action on; some of these were commercial in nature, shot in a studio, and others were where children had been groomed and coerced with their siblings or friends in their bedrooms at home.

A focused analysis of Report Remove data is available here which shows how boys are making the majority of reports to remove sexual imagery of themselves.


Analysis by sex over the past three years

Source: IWF Annual Report 2022

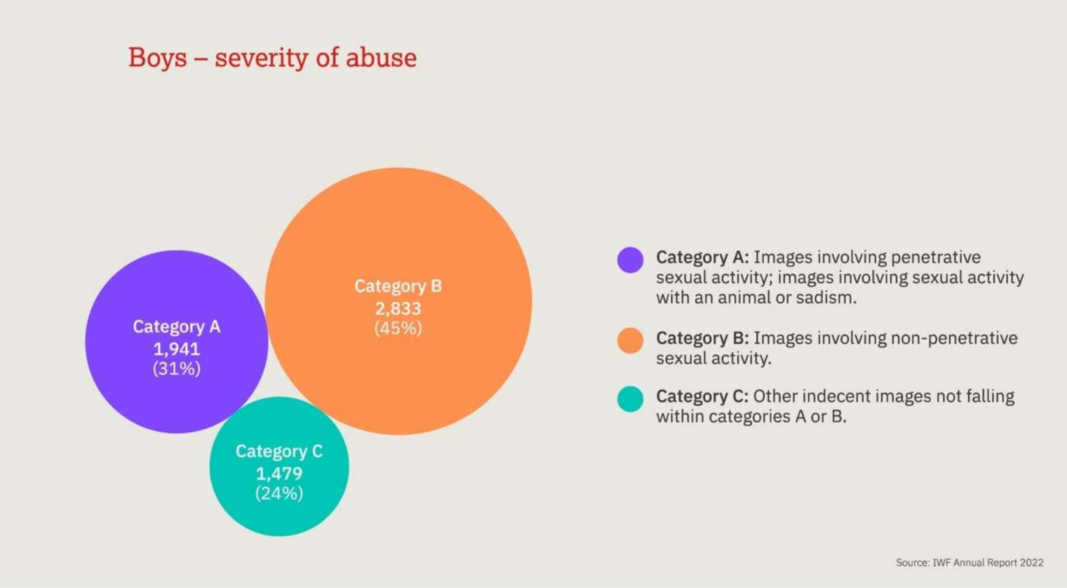


This chart shows the number and proportion of child sexual abuse URLs in 2022, split by sex of the victim.

By sex

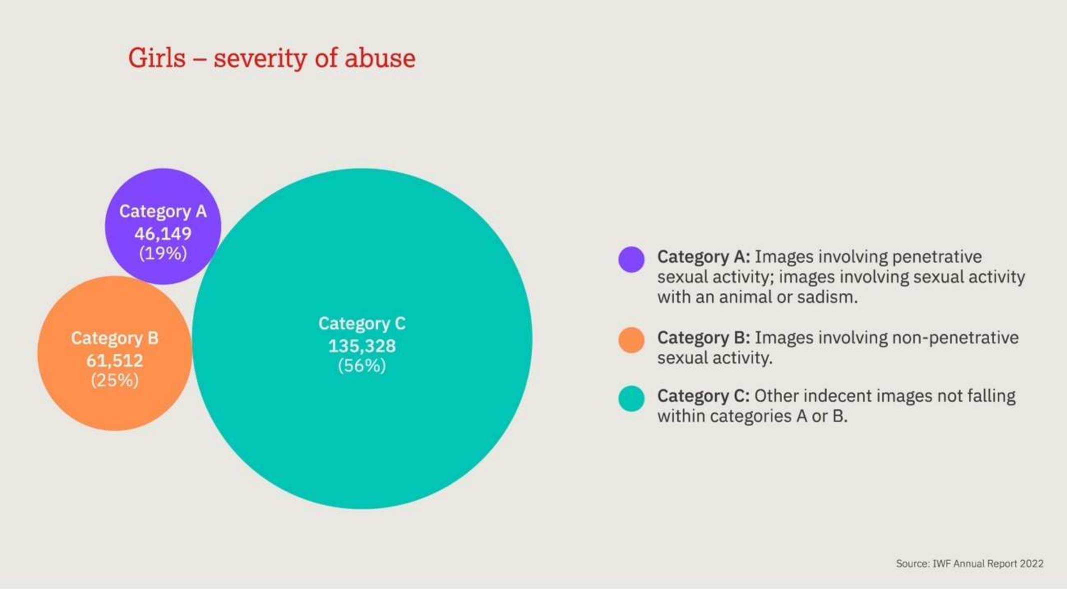
In 2022, we saw an increase in the proportion of Category A images: these most severe images accounted for 20% of the child sexual abuse images we actioned, up from 18% in 2021 and 17% in 2020. Here, we take a closer look at how the category analysis applies to child sexual abuse reports featuring girls and boys separately.

You can read more about self-generated imagery here.



Source: IWF Annual Report 2022

In 2022, 2.5 % or 6,253 reports showed the sexual abuse of boys only. This is a 137% increase on 2021 (2,641 reports). Within this subset of data, we can see that a higher proportion of the imagery of boys shows Category A child sexual abuse compared to girls: 31% for boys compared to 19% for girls.



Source: IWF Annual Report 2022

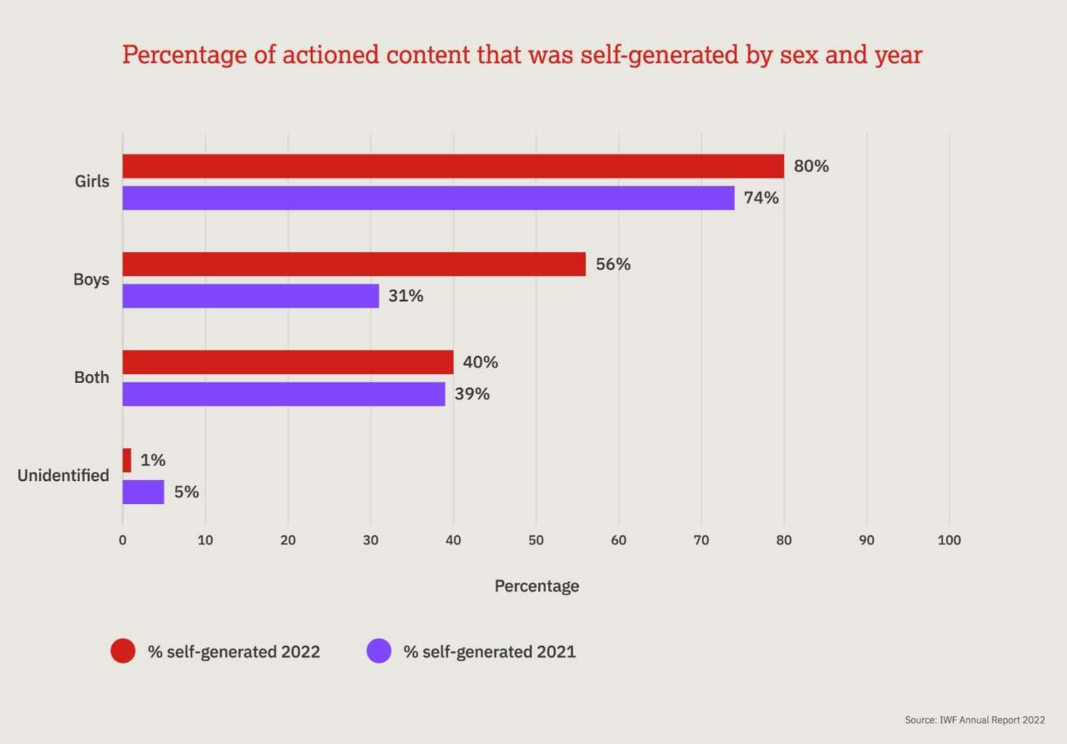
In 2022, 96% or 242,989 reports showed the sexual abuse of girls only – an increase of 1,045 reports on 2021. While the category of this material in 2022 and 2021 is similar, Category C has decreased from 63% (152,821) in 2021, to 56% (135,328) in 2022, which is a 7% decrease. Category A has increased by 2%, and Category B by 5%, showing the severity of the abuse in the imagery identified has increased.

Self-generated

We saw a significant increase in the number of 'self-generated' child sexual abuse images of boys. 'Self-generated' images of boys accounted for 31% (831) of all boys' child sexual abuse images in 2021, while in 2022 this rose to 56% (3,504) – an overall increase of 25%.

In 'self-generated' Category A images, we have observed household objects like hairbrushes and pens being used to penetrate, with children often being coerced to do so by a remote abuser.

You can read more about self-generated imagery here.



Source: IWF Annual Report 2022

Report remove

To support young people to remove sexual images or videos of themselves online, the IWF and NSPCC developed the world-first Report Remove tool which was launched in June 2021.

The NSPCC's Childline service ensures that the young person is safeguarded and supported throughout the process and the IWF assesses the reported content and takes action if it meets the threshold of illegality. The content is given a unique digital fingerprint (a hash) which is then shared with internet companies to help prevent the imagery from being uploaded or redistributed online.

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, they can make the report at any time, and further information and support is always available from Childline.

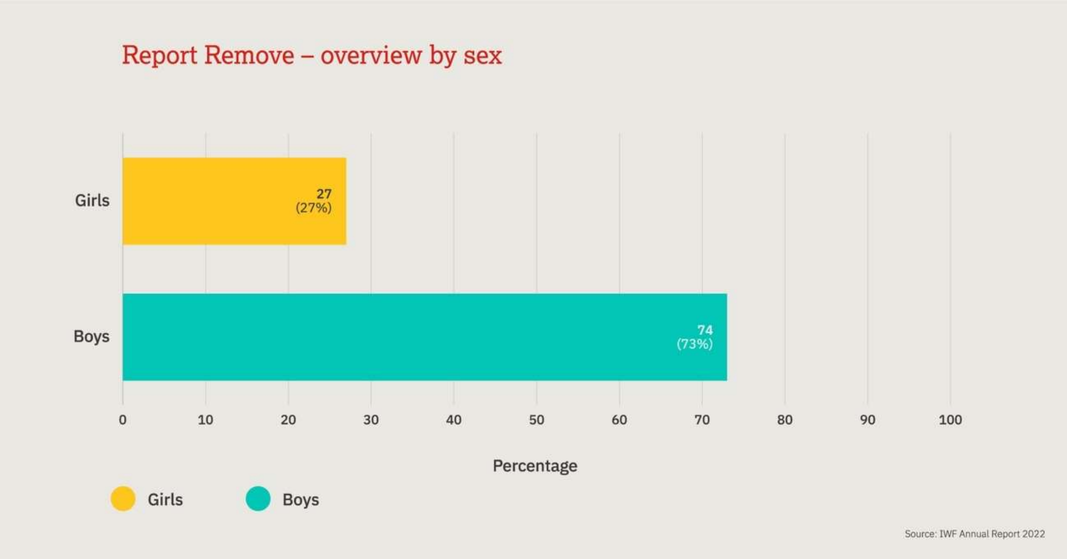
Young people create or sign into a Childline account which then allows them to receive Childline email updates about their report. Young people can use this email service for ongoing support, and they can contact a Childline counsellor via online chat and via their freephone number. They can also access relevant information and advice, self-help tools and peer support on the Childline website.

- In 2022, we received 187 reports through the Report Remove tool.
- We were able to take action on 101 reports.

Analysis of 'actionable' reports

These are reports which were assessed as containing images and/or videos or were URLs containing such images and videos of child sexual abuse according to UK legislation.

Of the 101 reports which we assessed as criminal images, most contained Category C images (69%), and more boys reported to us than girls, with boys making up 73% of the total.



Report Remove – overview by sex

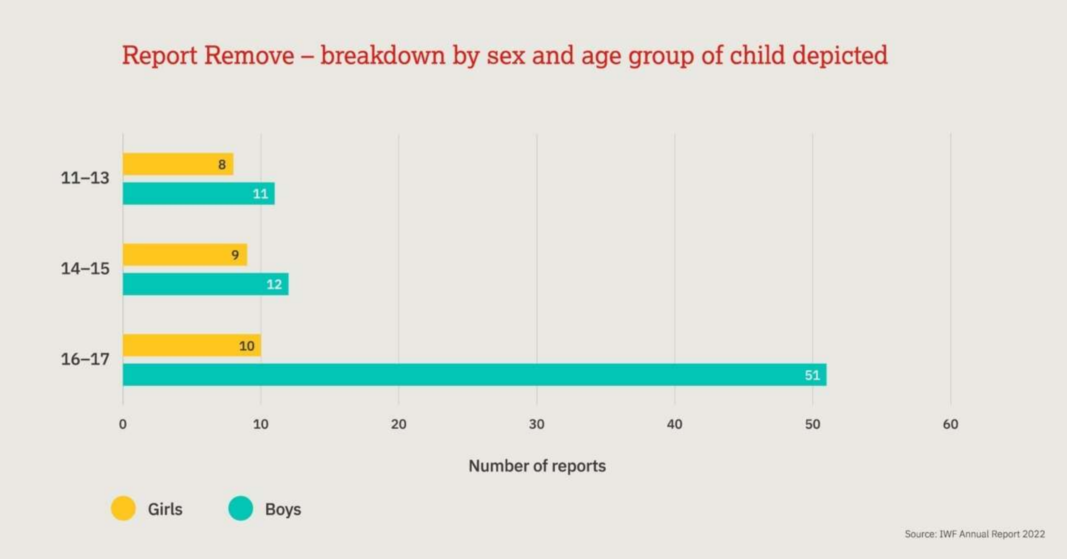
Source: IWF Annual Report 2022

This chart provides an overview of the sex of the child depicted in the images or videos sent through the Report Remove tool. Most – almost three quarters – came from boys.

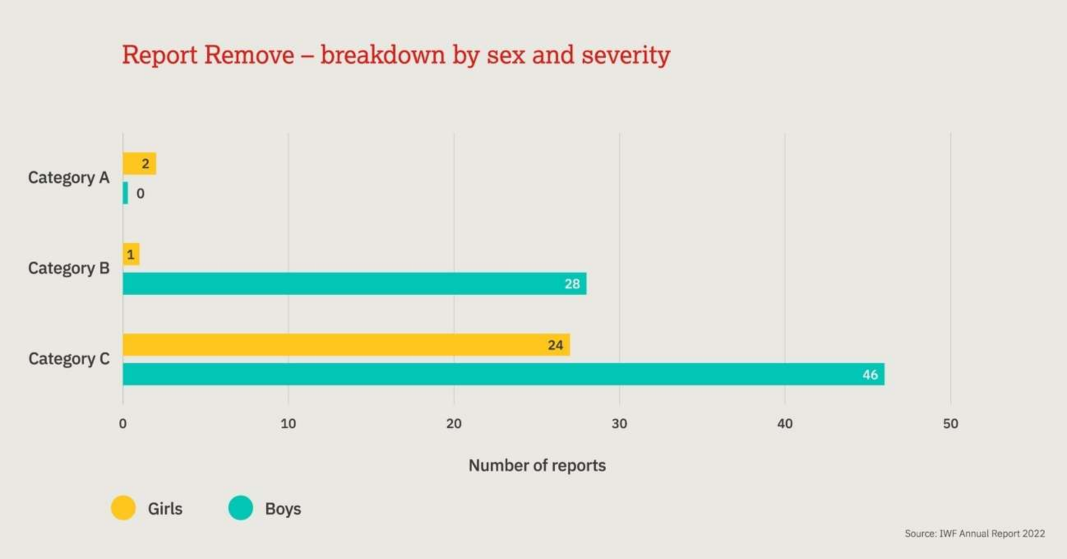
Sexually coerced extortion

A quarter (24% or 18 reports) of the 74 actionable reports from boys were because of **sexually coerced extortion**. We've seen how boys are typically lured into what they believe are mutual exchanges of sexual images where they mistakenly believe they are sharing images with a peer or older person.

We know that sexually coerced extortion is behind these specific reports from boys as they have included evidence of this within their report. This could be a chat log where the young person has demonstrated that they are being coerced or where a collage of images has been created by the offender, overlaid with threatening text. No such evidence was present against any of the images of girls.



This chart shows how boys aged 16 and 17 represent the biggest user group of the Report Remove service.



Most images and videos reported by young people through Report Remove (which are assessed as child sexual abuse material) fall into Category C, with a notable amount of imagery of boys assessed as Category B.

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.

'Self-generated' child sex abuse

Overview

In 2022, we continued to see a high proportion of ‘self-generated’ imagery. These are child sexual abuse images and videos created using smartphones or webcams and then shared online. In some cases, children are groomed, deceived or extorted into producing and sharing a sexual image or video of themselves by someone who is not physically present in the room with the child. These images are most often taken in a home setting – a child’s bedroom, or a bathroom.

A note on terminology:

We regard the term ‘self-generated’ child sexual abuse 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, we will continue to use the term ‘self-generated’ as, within the online safety and law enforcement sectors, this is well recognised.

In our charts, and explanations in this section, we have also used the term ‘abuser present’ to describe images and videos which are ‘not “self-generated”’. **Please note that ‘abuser present’ means that we assessed this content as being created when the abuser was physically present in the room with the victim/s or their likeness, but this does not necessarily mean that the abuser was depicted in the imagery itself.**

Trends

Children aged 11-13 continue to appear most frequently in ‘self-generated’ imagery, as in previous years. We observed a steep increase, however, in the proportion of this type of imagery including children aged 7-10 in 2022, up 129% from 2021.

- Of the 255,571 webpages actioned during 2022, **over three quarters (199,363 or 78%)** were assessed as containing ‘self-generated’ imagery.

This is a 6 percentage point increase on 2021 when 72% of actioned reports (or 182,281) were remote-captured.

- This represents a 9% increase in 'self-generated' reports from 2021 to 2022 in terms of the number of actioned webpages.

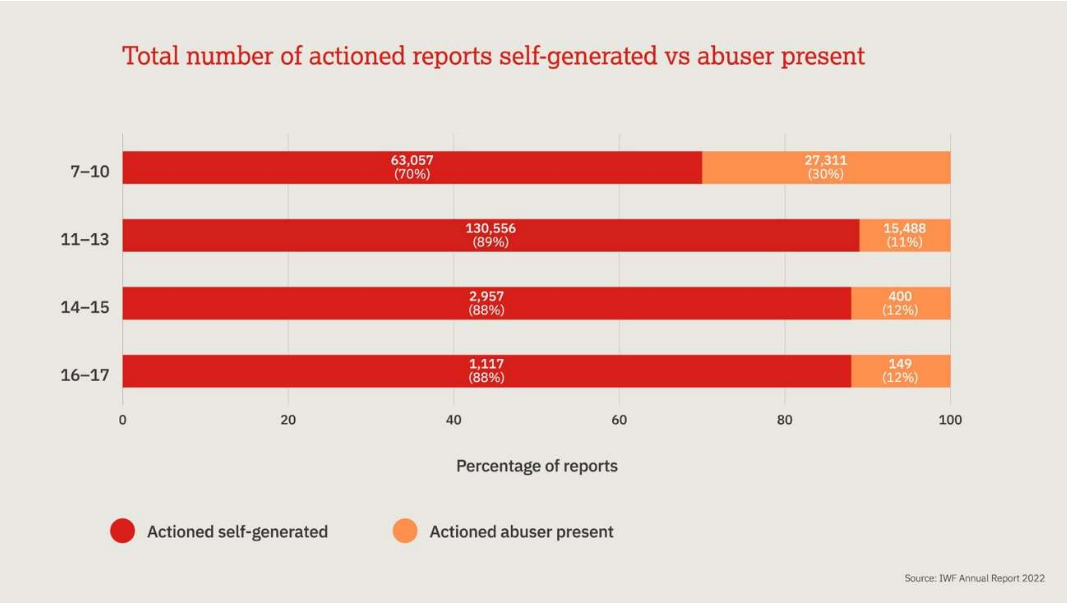
Key trends

More key trends of note:

- In 2022, 127,732 reports which included ‘self-generated’ imagery included an **11–13-year-old girl**.
    - This represents 50% of all actioned reports and 64% of ‘self-generated’ child sexual abuse reports.

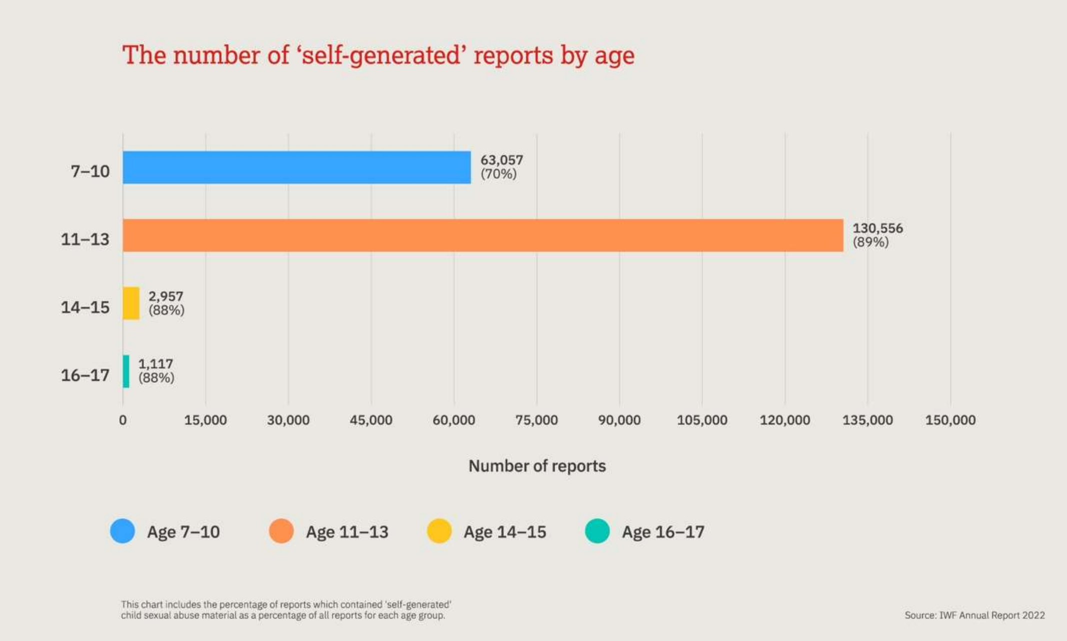
- We’ve been monitoring a steep increase in this imagery featuring 7–10-year-olds. In 2022, 63,057 ‘self-generated’ reports featured a 7–10-year-old, which is a 129% increase on 2021.
    - This is an increase of 1,058% since 2019 when 5,443 reports of ‘self-generated’ child sexual abuse of this age group were found. This exponential increase coincides with the global COVID-19 pandemic when children were spending more time online than usual and virtual socialising became the norm.

- In 2022, 61,754 reports which included ‘self-generated’ imagery included a **7–10-year-old girl**.
    - This represents 24% of all actioned reports and 31% of ‘self-generated’ child sexual abuse reports.


Total number of actioned reports self-generated vs abuser present

Source: IWF Annual Report 2022

*Please note that ‘abuser present’ means that we assessed this content as being created when the abuser was physically present in the room with the victim/s or their likeness, but this does not necessarily mean that the abuser was depicted in the imagery itself.

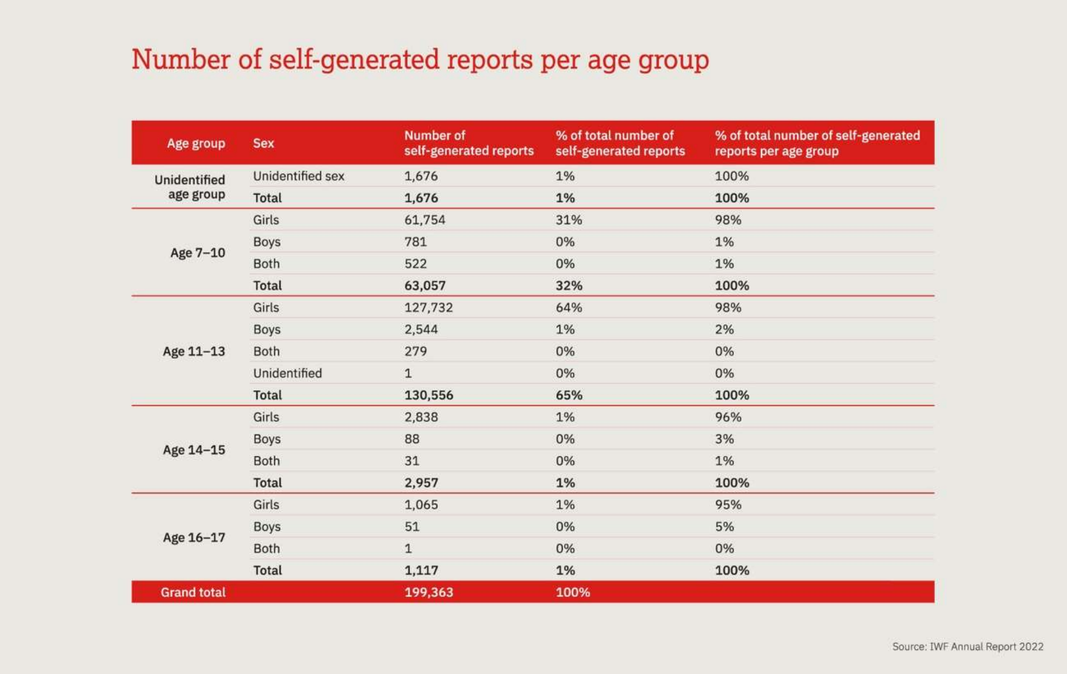


The number of ‘self-generated’ reports by age

This chart includes the percentage of reports which contained 'self-generated' child sexual abuse material as a percentage of all reports for each age group.

Source: IWF Annual Report 2022

This chart shows the total number of reports which included ‘self-generated’ content split by age of the child depicted.



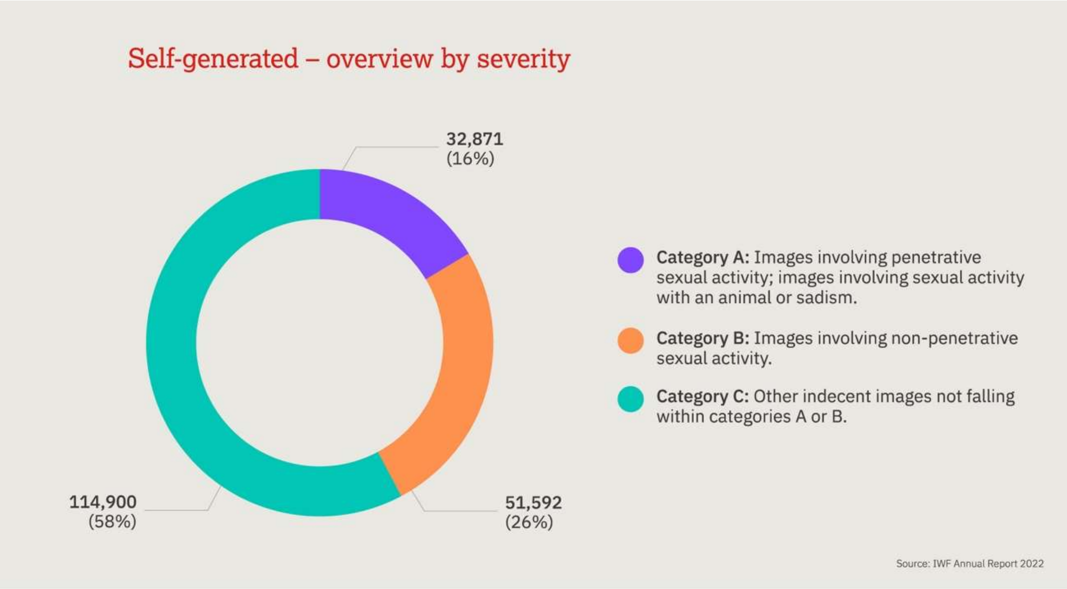
Number of self-generated reports per age group

Age group	Sex	Number of self-generated reports	% of total number of self-generated reports	% of total number of self-generated reports per age group
Unidentified age group	Unidentified sex	1,676	1%	100%
	Total	**1,676**	**1%**	**100%**
Age 7–10	Girls	61,754	31%	98%
	Boys	781	0%	1%
	Both	522	0%	1%
	Total	**63,057**	**32%**	**100%**
Age 11–13	Girls	127,732	64%	98%
	Boys	2,544	1%	2%
	Both	279	0%	0%
	Unidentified	1	0%	0%
	Total	**130,556**	**65%**	**100%**
Age 14–15	Girls	2,838	1%	96%
	Boys	88	0%	3%
	Both	31	0%	1%
	Total	**2,957**	**1%**	**100%**
Age 16–17	Girls	1,065	1%	95%
	Boys	51	0%	5%
	Both	1	0%	0%
	Total	**1,117**	**1%**	**100%**
Grand total		199,363	100%	

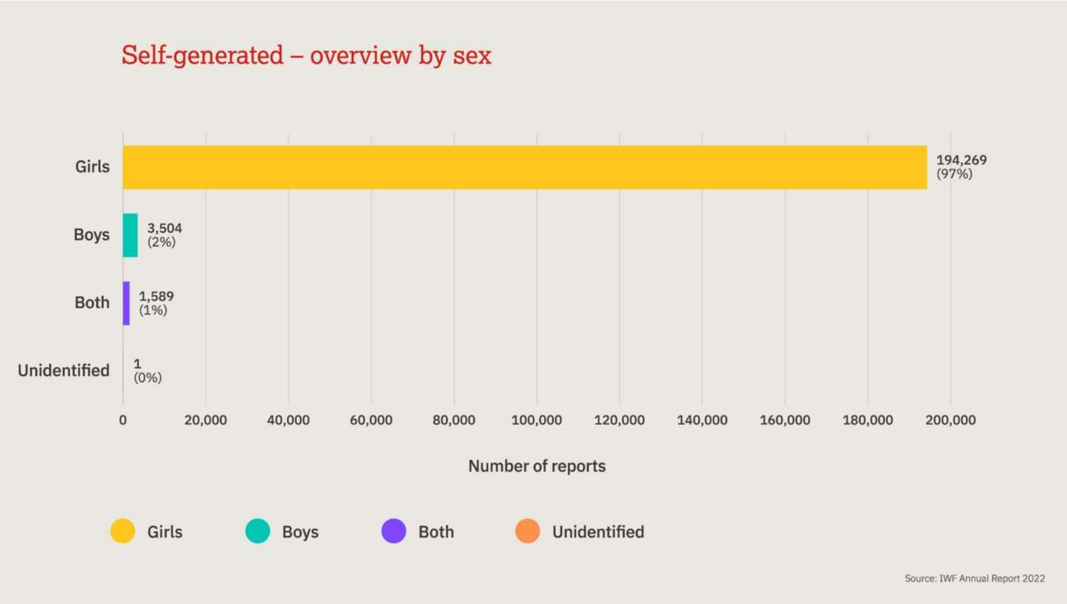
Source: IWF Annual Report 2022

This table provides a detailed breakdown of the reports which include ‘self-generated’ child sexual abuse material by sex and age.

Unidentified: This very small group relates to URLs displaying more than one image on the page (often many thousands) and where one or more of those images is self-generated. For these we are unable to attribute a specific age group to the multiple children seen. Some of these may also be younger children involved in self-generated images of sibling abuse.


Self-generated – overview by severity

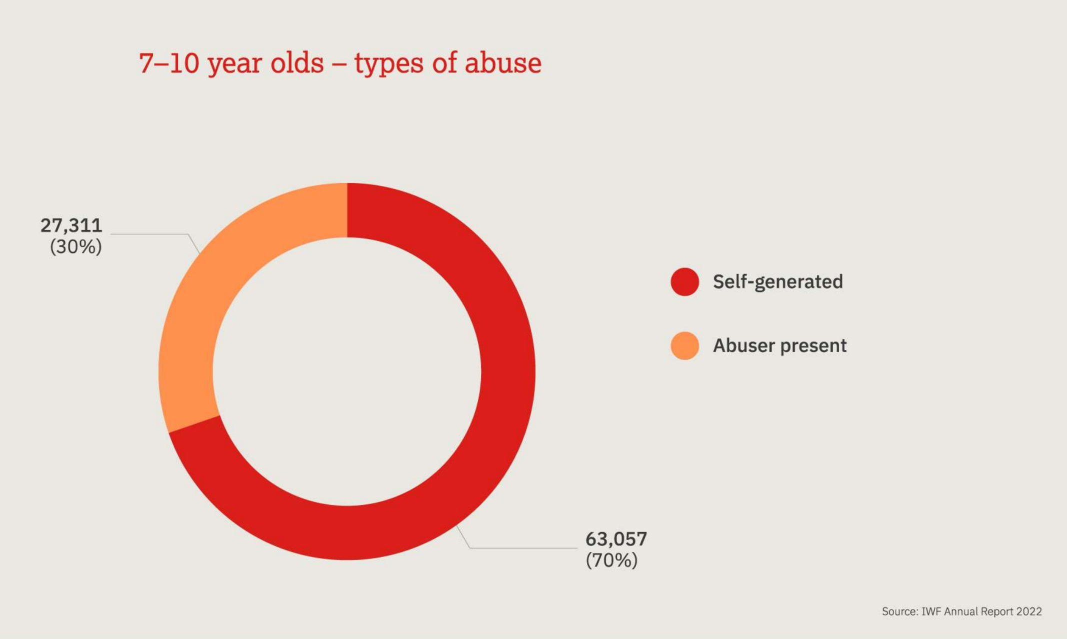
Source: IWF Annual Report 2022


Self-generated – overview by sex

Source: IWF Annual Report 2022

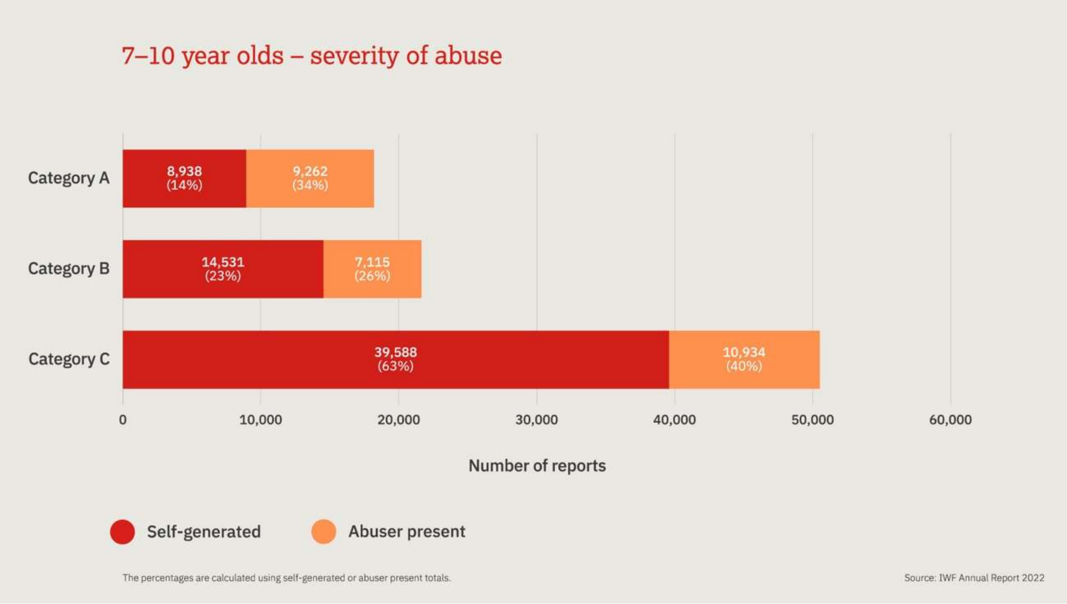
7-10 years: Pre-pubescent children

2022 was the first year that 'self-generated' child sexual abuse reports of 7-10-year-olds were more prevalent than content created when the abuser was physically present in the room.



7–10 year olds – types of abuse

Source: IWF Annual Report 2022

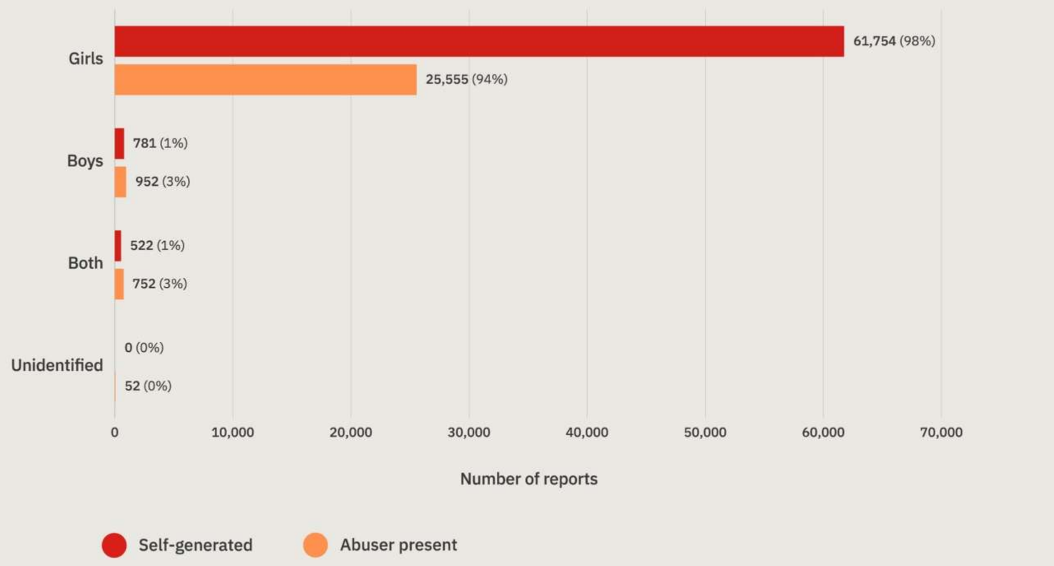


7–10 year olds – severity of abuse

The percentages are calculated using self-generated or abuser present totals.

Source: IWF Annual Report 2022

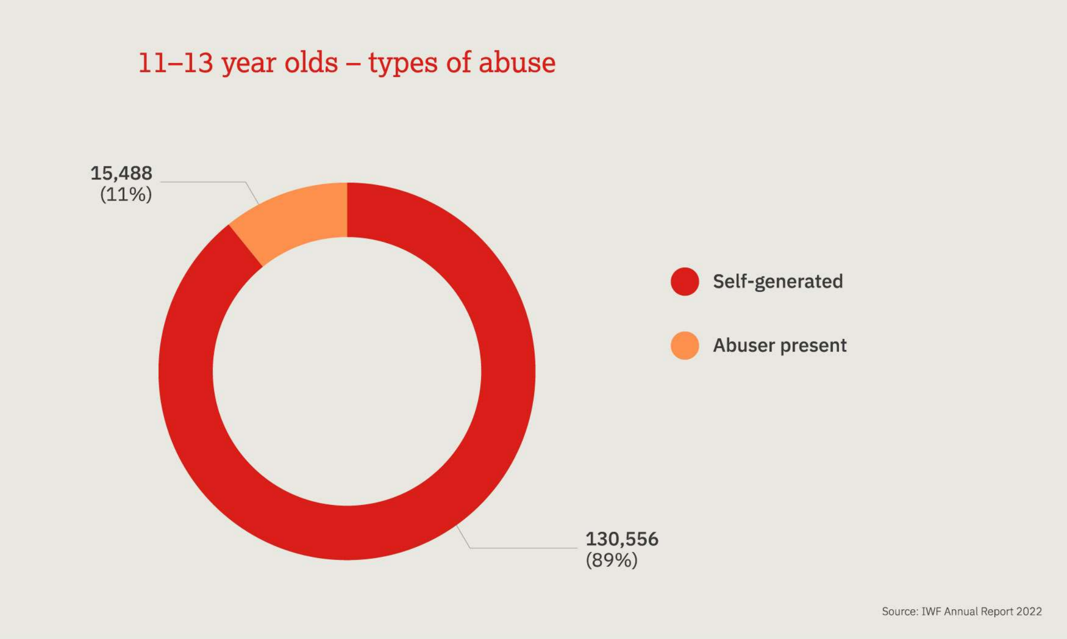
7–10 year olds – sex of victims

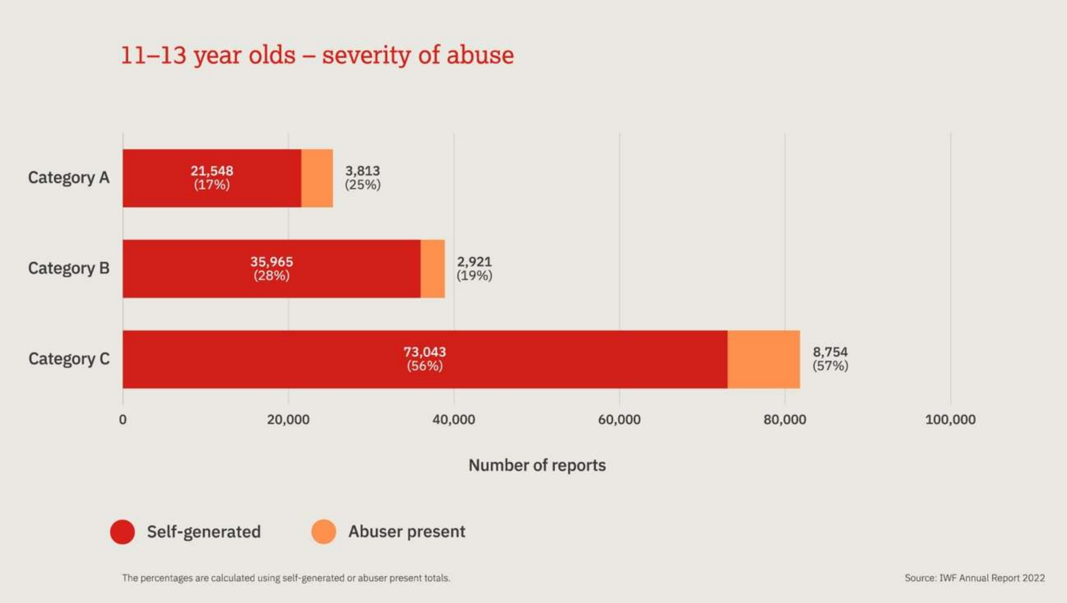


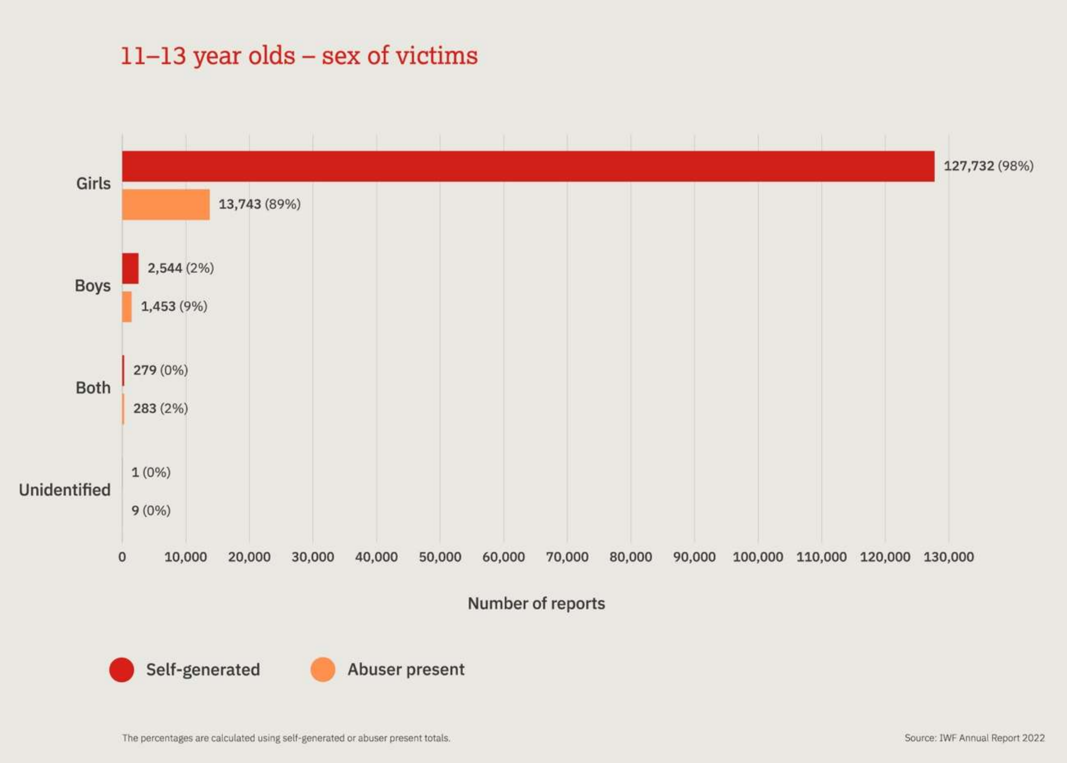
The percentages are calculated using self-generated or abuser present totals.

Source: IWF Annual Report 2022

11-13 years: Older children



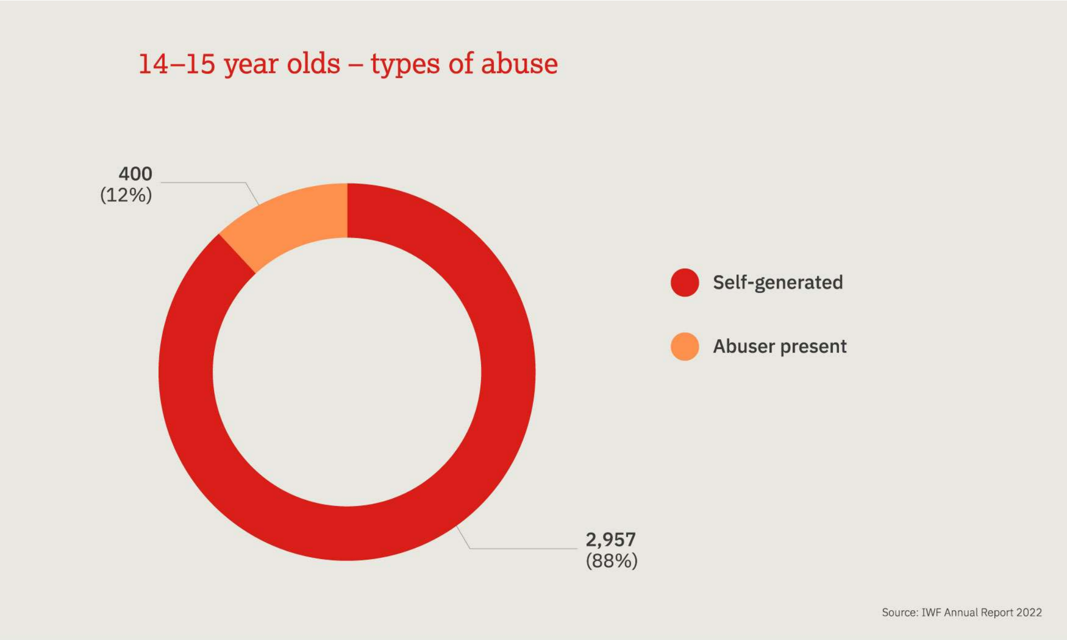




The percentages are calculated using self-generated or abuser present totals.

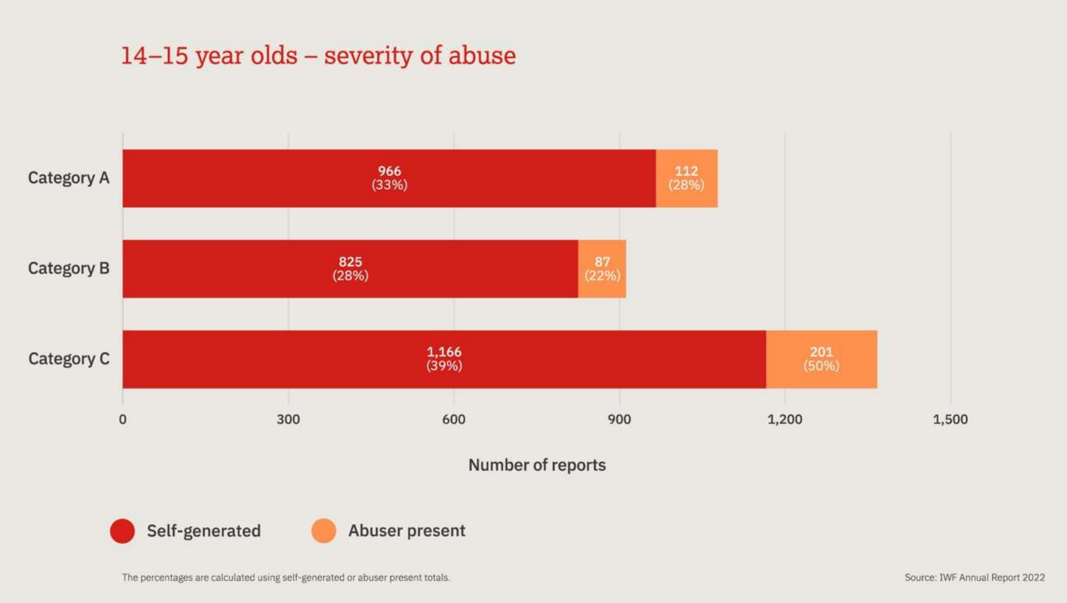
Source: IWF Annual Report 2022

14-15 years: Teenagers



14–15 year olds – types of abuse

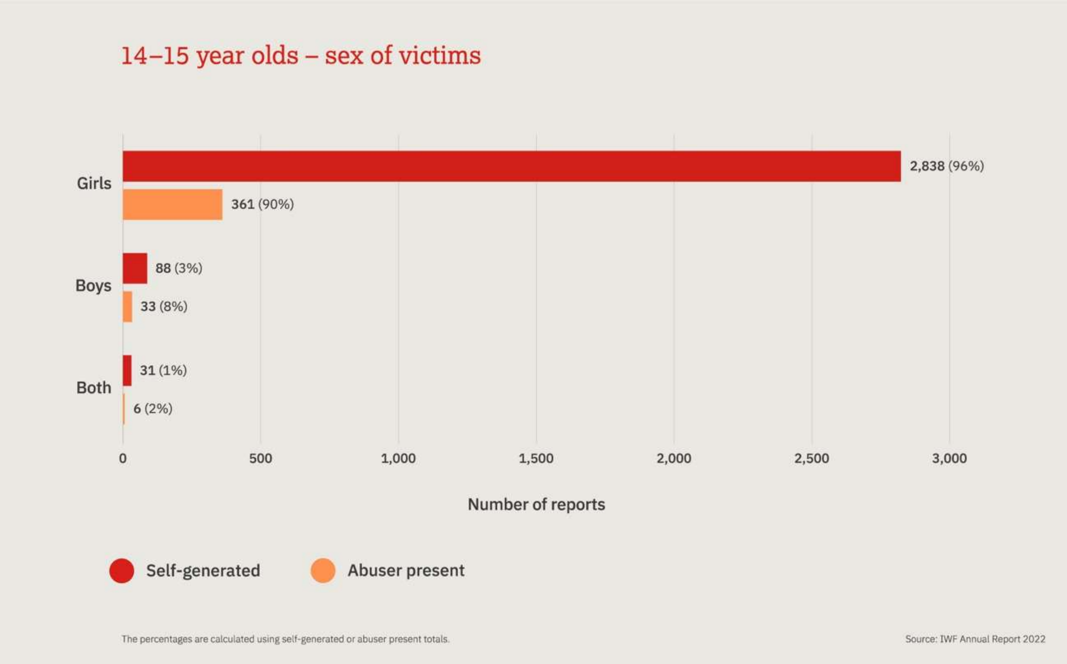
Source: IWF Annual Report 2022



14–15 year olds – severity of abuse

The percentages are calculated using self-generated or abuser present totals.

Source: IWF Annual Report 2022



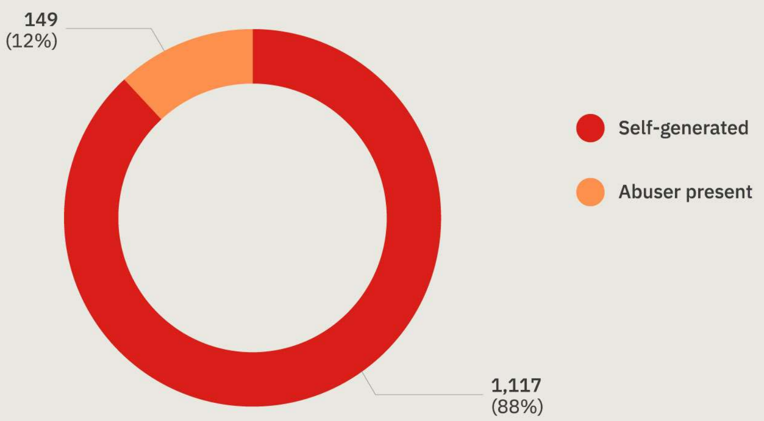
14–15 year olds – sex of victims

The percentages are calculated using self-generated or abuser present totals.

Source: IWF Annual Report 2022

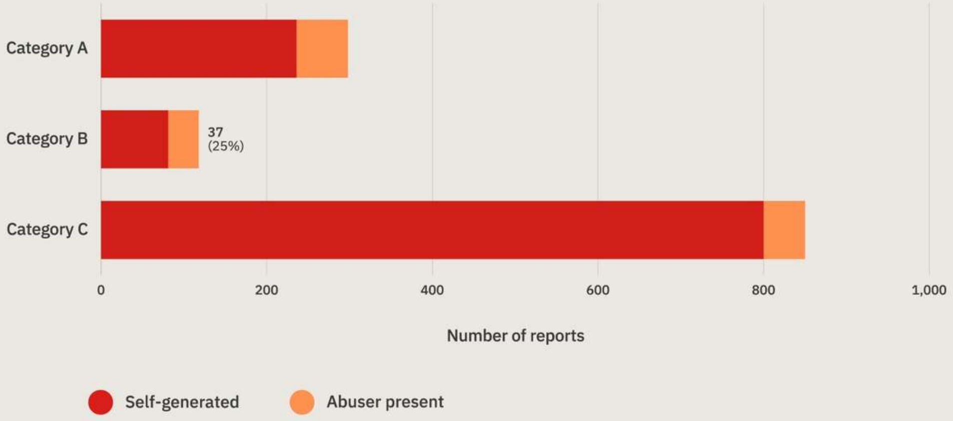
16-17 years: Teenagers

16–17 year olds – types of abuse



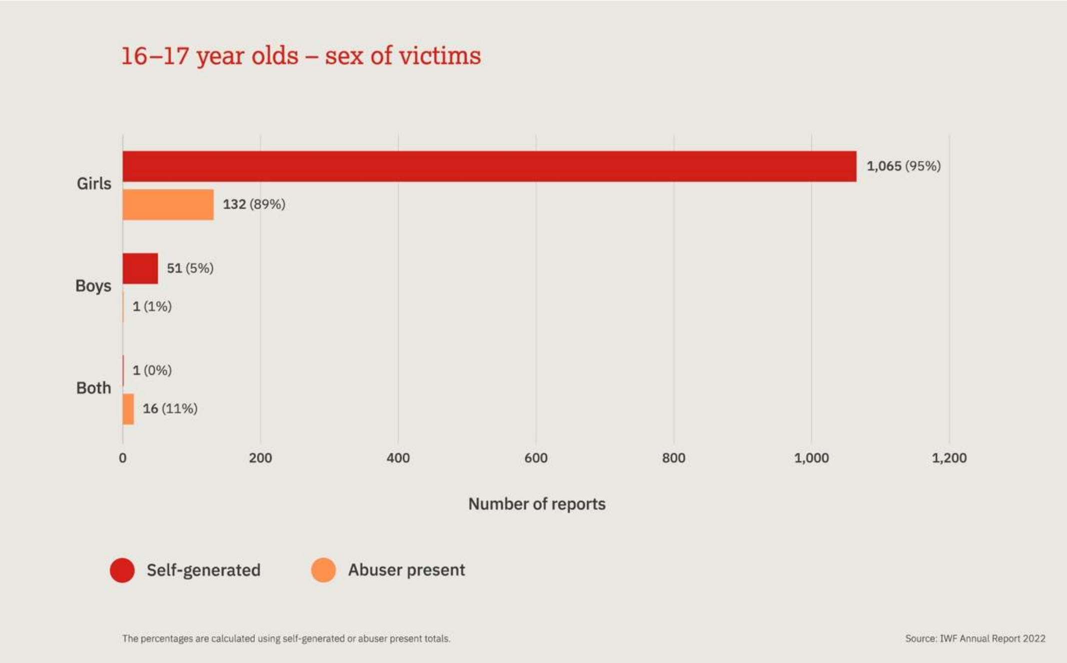
Source: IWF Annual Report 2022

16–17 year olds – severity of abuse



The percentages are calculated using self-generated or abuser present totals.

Source: IWF Annual Report 2022



The percentages are calculated using self-generated or abuser present totals.

Source: IWF Annual Report 2022

Geographical hosting: URLs

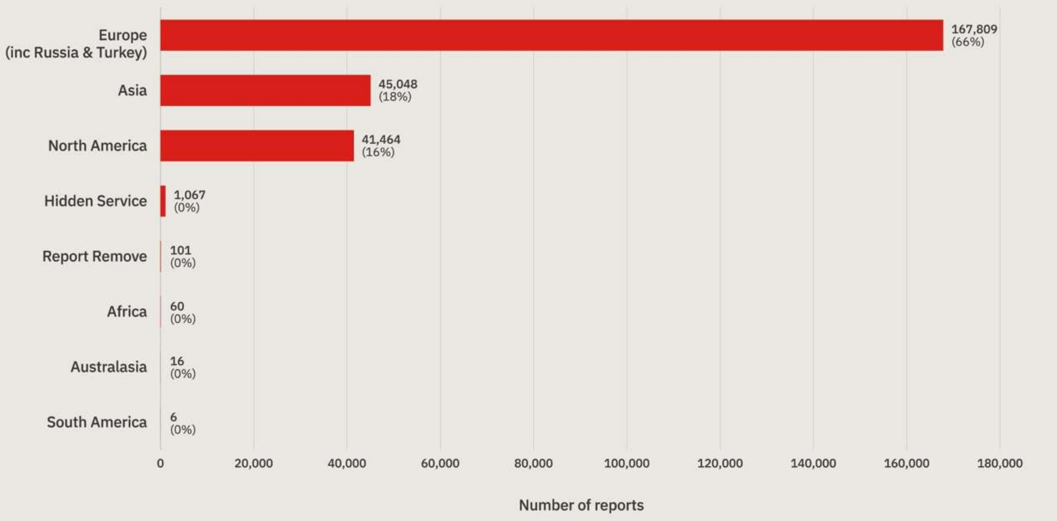
Where are webpages being hosted?

You can find out about the UK hosting situation here.

When we've assessed that an image or video fails UK law, our aim is to get it removed from the internet as fast as possible. To do this, we perform a trace on the URL to identify the location of the physical server that the content is hosted on. This tells us which partners in which country we need to work with. When the content is removed from the physical server – its source – then we can be sure that the image has been removed from any sites – like websites, forums, or image hosts – that could be linking to it.

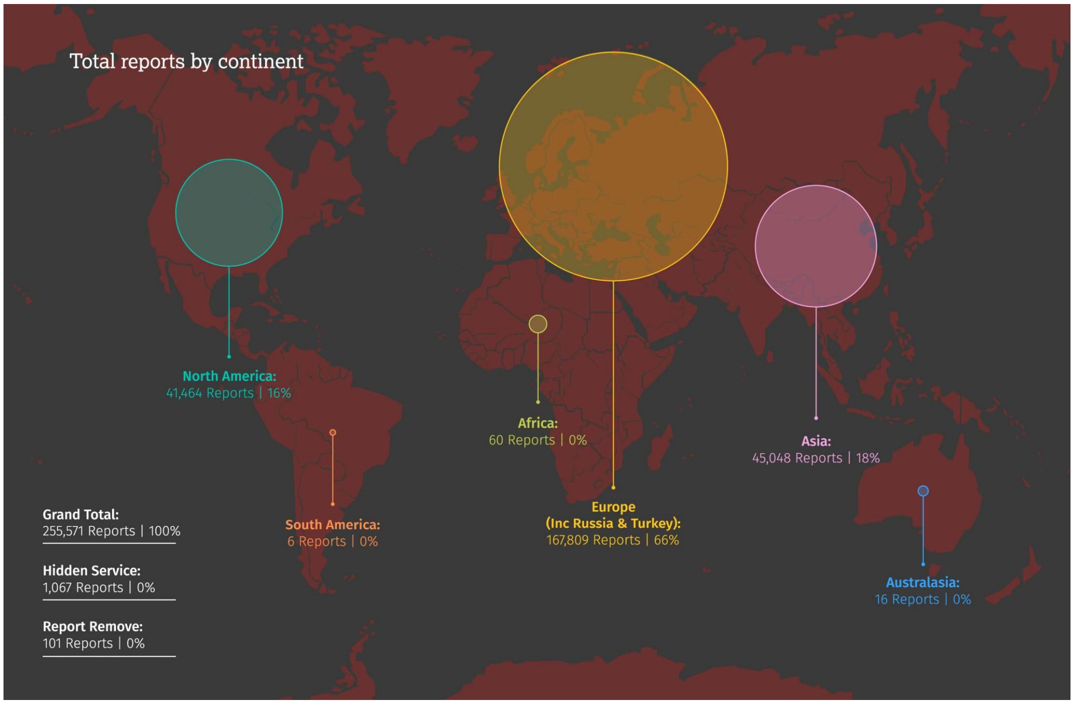
> "I would also like to share with you that pretty much all of the reports that you have contributed with so far has played vital roles in a number of investigations as well as a number of convictions relating to CSAM and CSE. It has played a key role in getting search warrants approved in many of the cases. A number of these search warrants and investigations has also led to the discovery of more aggravated crimes against children including hands on sexual offences. We are very thankful for your support in these cases." **Swedish Police Authority**

Total reports by continent

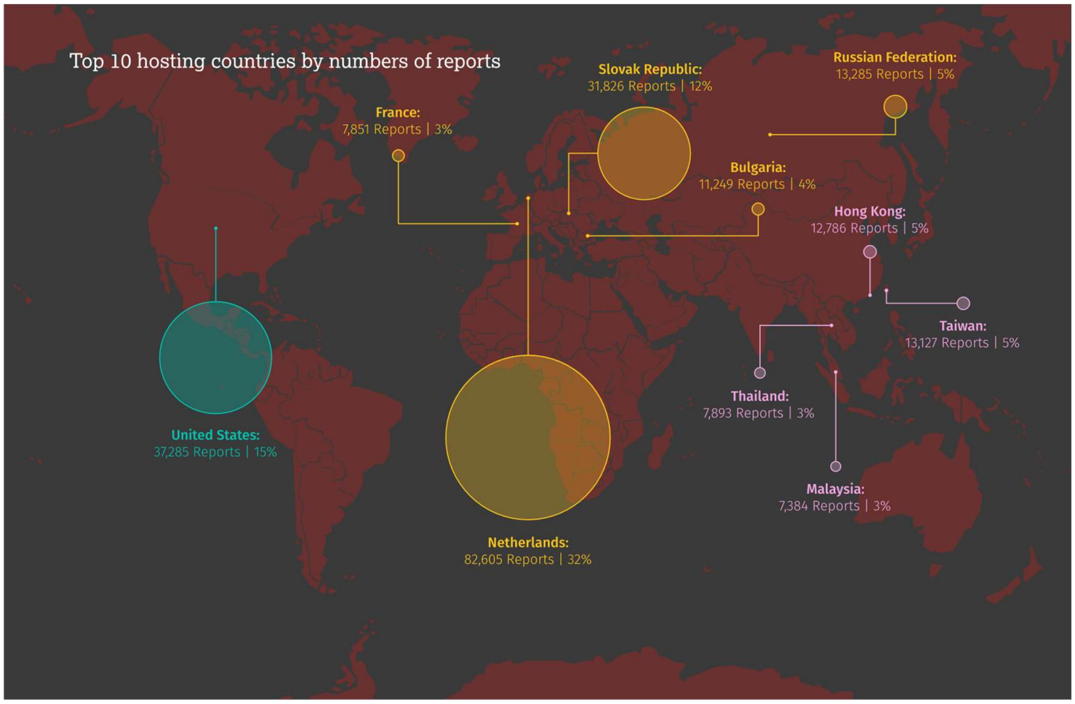


A number of reports including Tor domains, and images received through, for example, Report Remove, do not resolve to traceable locations.

Source: IWF Annual Report 2022

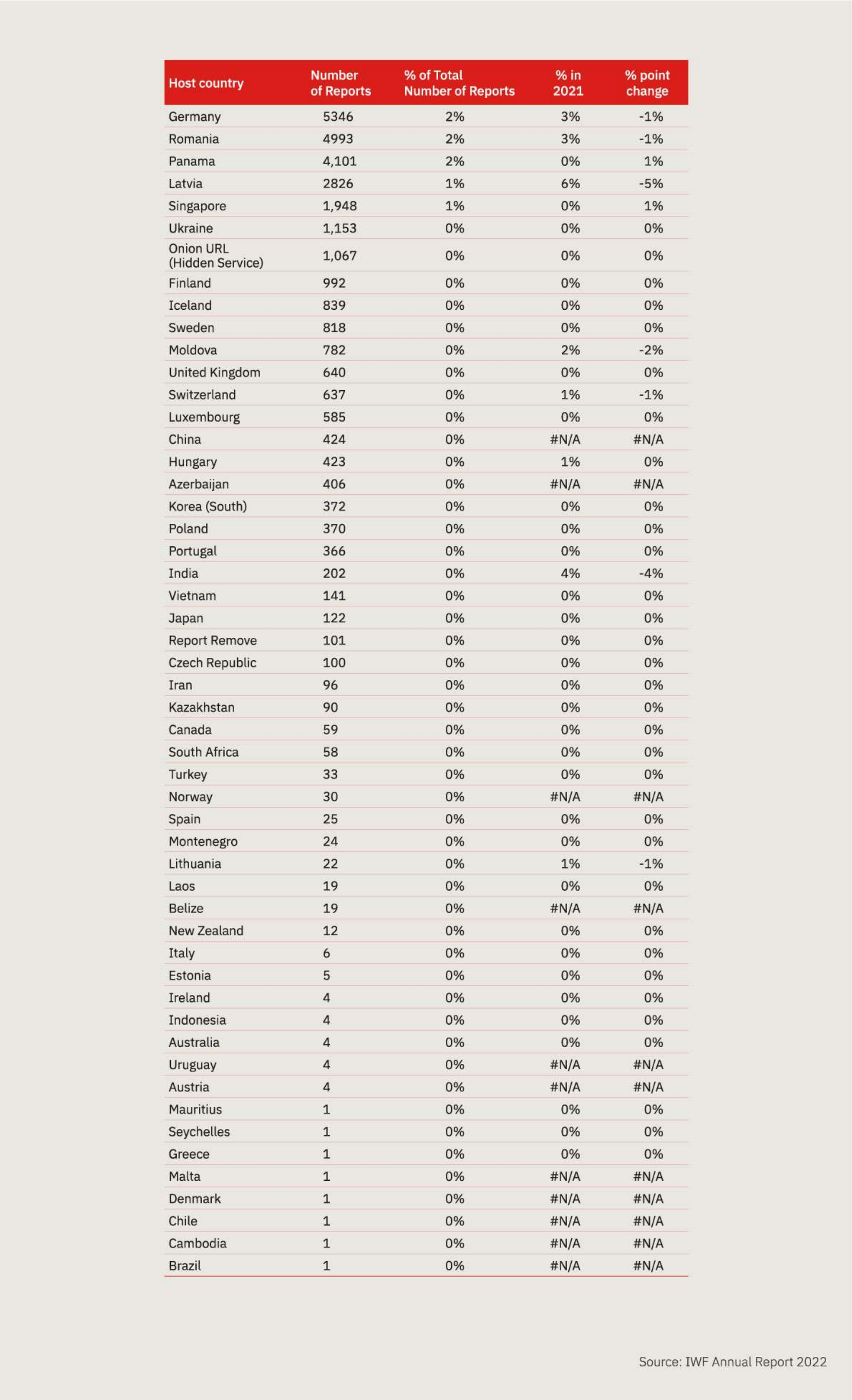


Total reports by continent



Top 10 hosting countries by numbers of reports

Number of reports (URLSs) by country (from number 11 onwards)



Host country	Number of Reports	% of Total Number of Reports	% in 2021	% point change
Germany	5346	2%	3%	-1%
Romania	4993	2%	3%	-1%
Panama	4,101	2%	0%	1%
Latvia	2826	1%	6%	-5%
Singapore	1,948	1%	0%	1%
Ukraine	1,153	0%	0%	0%
Onion URL (Hidden Service)	1,067	0%	0%	0%
Finland	992	0%	0%	0%
Iceland	839	0%	0%	0%
Sweden	818	0%	0%	0%
Moldova	782	0%	2%	-2%
United Kingdom	640	0%	0%	0%
Switzerland	637	0%	1%	-1%
Luxembourg	585	0%	0%	0%
China	424	0%	#N/A	#N/A
Hungary	423	0%	1%	0%
Azerbaijan	406	0%	#N/A	#N/A
Korea (South)	372	0%	0%	0%
Poland	370	0%	0%	0%
Portugal	366	0%	0%	0%
India	202	0%	4%	-4%
Vietnam	141	0%	0%	0%
Japan	122	0%	0%	0%
Report Remove	101	0%	0%	0%
Czech Republic	100	0%	0%	0%
Iran	96	0%	0%	0%
Kazakhstan	90	0%	0%	0%
Canada	59	0%	0%	0%
South Africa	58	0%	0%	0%
Turkey	33	0%	0%	0%
Norway	30	0%	#N/A	#N/A
Spain	25	0%	0%	0%
Montenegro	24	0%	0%	0%
Lithuania	22	0%	1%	-1%
Laos	19	0%	0%	0%
Belize	19	0%	#N/A	#N/A
New Zealand	12	0%	0%	0%
Italy	6	0%	0%	0%
Estonia	5	0%	0%	0%
Ireland	4	0%	0%	0%
Indonesia	4	0%	0%	0%
Australia	4	0%	0%	0%
Uruguay	4	0%	#N/A	#N/A
Austria	4	0%	#N/A	#N/A
Mauritius	1	0%	0%	0%
Seychelles	1	0%	0%	0%
Greece	1	0%	0%	0%
Malta	1	0%	#N/A	#N/A
Denmark	1	0%	#N/A	#N/A
Chile	1	0%	#N/A	#N/A
Cambodia	1	0%	#N/A	#N/A
Brazil	1	0%	#N/A	#N/A

Source: IWF Annual Report 2022

Note: 101 instances refer to Report Remove where images/videos have been directly reported to IWF and are therefore not online and cannot be traced to a location.

In 2022 we continued to see a decrease in the proportion of child sexual abuse URLs being hosted in the Netherlands, down to 32% from 41% in 2021. The proportion of child sexual abuse URLs hosted in the US also dropped in 2022, down to 15% from 21% in 2021.

URLs hosted in the Slovak Republic accounted for 12% of the child sexual abuse imagery we took action on in 2022; this is the result of targeted work focusing on one particular **image host** website. Hosting services in Hong Kong, Bulgaria, Malaysia and Thailand have also been abused in a similar way which is discussed in our Forum snapshot case study.

Almost three in every five (59%) child sexual abuse reports were traced to hosting services in EU Member states.

Some criminal child sexual abuse sites, especially those created specifically to share imagery for commercial gain, are dynamic and deliberately move their hosting from country to country to avoid removal. We continue to track these sites when they change location and seek to take them offline wherever they go. This trend has led to several new countries entering the top 10 hosts this year.

What can we do about removing this content?

We are committed to playing our part globally in the removal of content.

We constantly innovate to achieve this. We've set up 50 Reporting Portals around the world as part of our work in partnership with the Global Fund to End Violence Against Children. This has enabled us to develop vital links with other NGOs, governments and police services globally to remove this content.

In the EU we work closely with Europol and Interpol and the Lanzarote Committee of the Council of Europe. Europol have produced a number of threat assessments which have referenced many similar trends we have identified including a rise in self-generated content.

As a key organisation within the INHOPE network (International Association of Internet Hotlines) we work closely with all other INHOPE hotlines around the world to ensure that we alert our partners when we find child sexual abuse content hosted in their country. IWF Reporting Portals are included under the INHOPE umbrella.

Additionally, we “chase up” our partners if this criminal imagery is not removed quickly.

View trends and data for the UK.

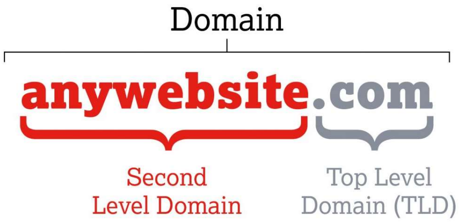
Geographical hosting: Domains

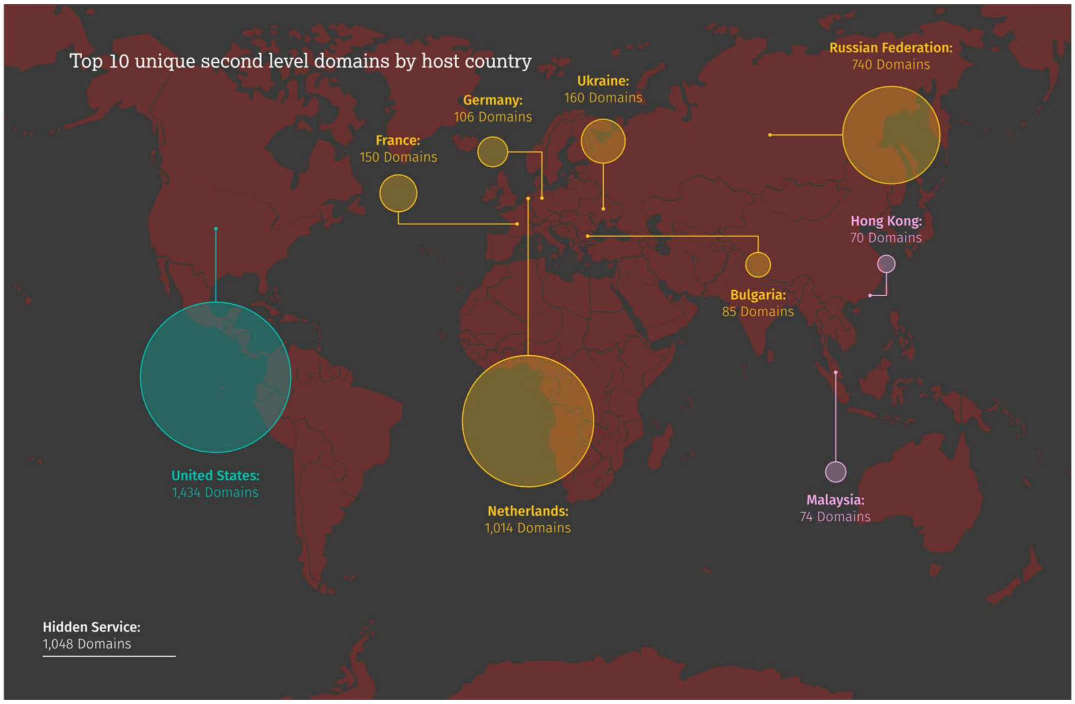
Unique domains

This is the second year that we have published two contrasting sets of domain analysis data, with a view to providing additional insights into the distribution and hosting hotspots of child sexual abuse images and videos across different countries and internet infrastructures.

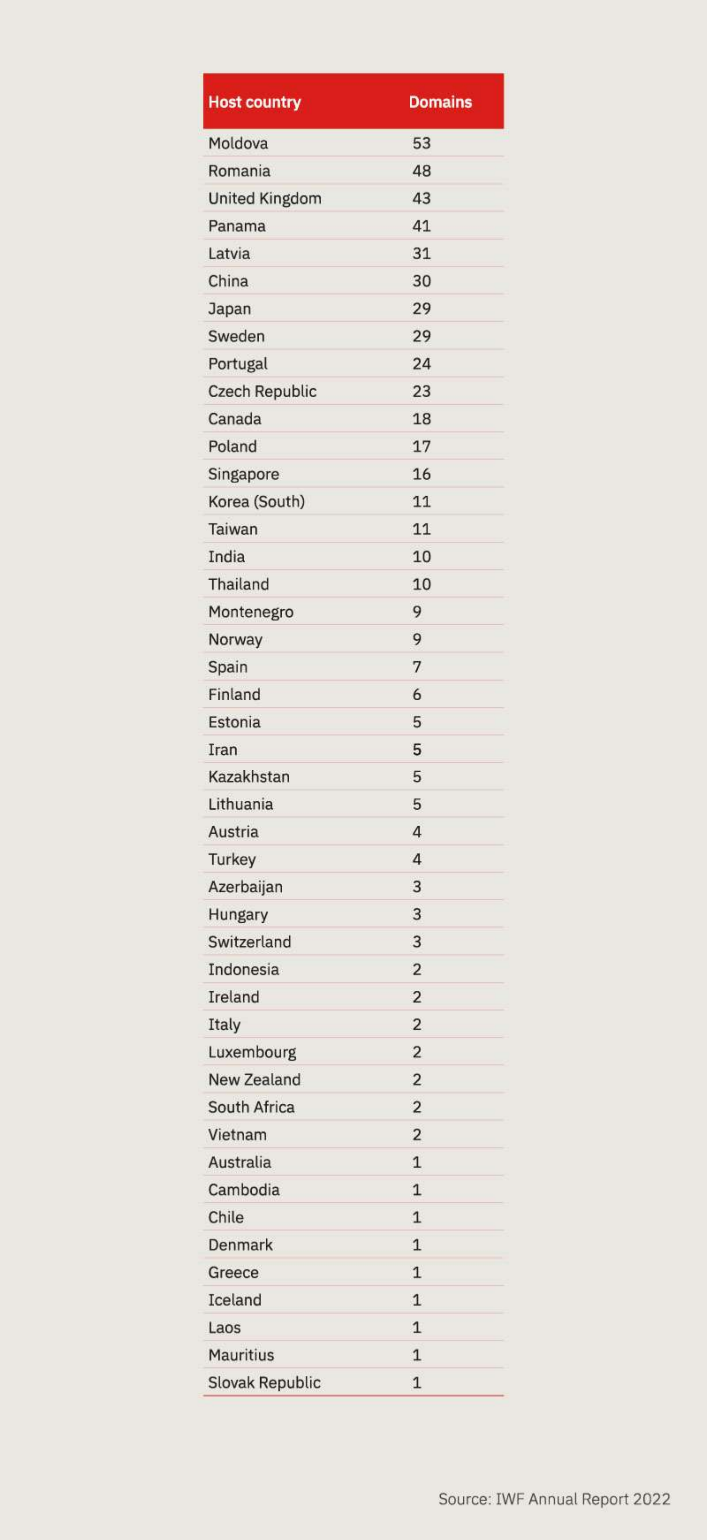
Specifically, while URL-level data indicates the number of reports and actions required to notify and remove this content, that granular detail may obfuscate the prevalence, or number, of unique domains identified to be hosting child sexual abuse material when analysed in different contexts.

For clarity, the diagram below sets out the domain naming conventions used throughout this report.




Top 10 unique second level domains by host country
Russian Federation: 740 Domains
Ukraine: 160 Domains
Germany: 106 Domains
France: 150 Domains
Hong Kong: 70 Domains
Bulgaria: 85 Domains
United States: 1,434 Domains
Netherlands: 1,014 Domains
Malaysia: 74 Domains
Hidden Service: 1,048 Domains

Number of unique second level domains by country (from number 11 onwards)



Host country	Domains
Moldova	53
Romania	48
United Kingdom	43
Panama	41
Latvia	31
China	30
Japan	29
Sweden	29
Portugal	24
Czech Republic	23
Canada	18
Poland	17
Singapore	16
Korea (South)	11
Taiwan	11
India	10
Thailand	10
Montenegro	9
Norway	9
Spain	7
Finland	6
Estonia	5
Iran	5
Kazakhstan	5
Lithuania	5
Austria	4
Turkey	4
Azerbaijan	3
Hungary	3
Switzerland	3
Indonesia	2
Ireland	2
Italy	2
Luxembourg	2
New Zealand	2
South Africa	2
Vietnam	2
Australia	1
Cambodia	1
Chile	1
Denmark	1
Greece	1
Iceland	1
Laos	1
Mauritius	1
Slovak Republic	1

Source: IWF Annual Report 2022

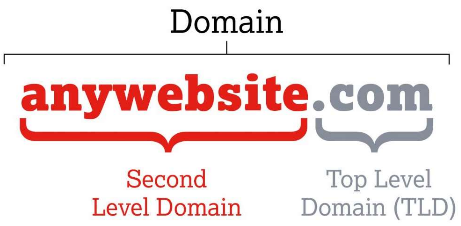
The data represented above shows the number of unique websites we identified to be hosted in each country. Each unique website was only counted once and attributed to its host country at the time of assessment. If a website changed its hosting country location at any point during the year, then the site was counted in each of the locations it was encountered. These numbers do not represent the individual number of URLs or reports that were actioned for each unique website.

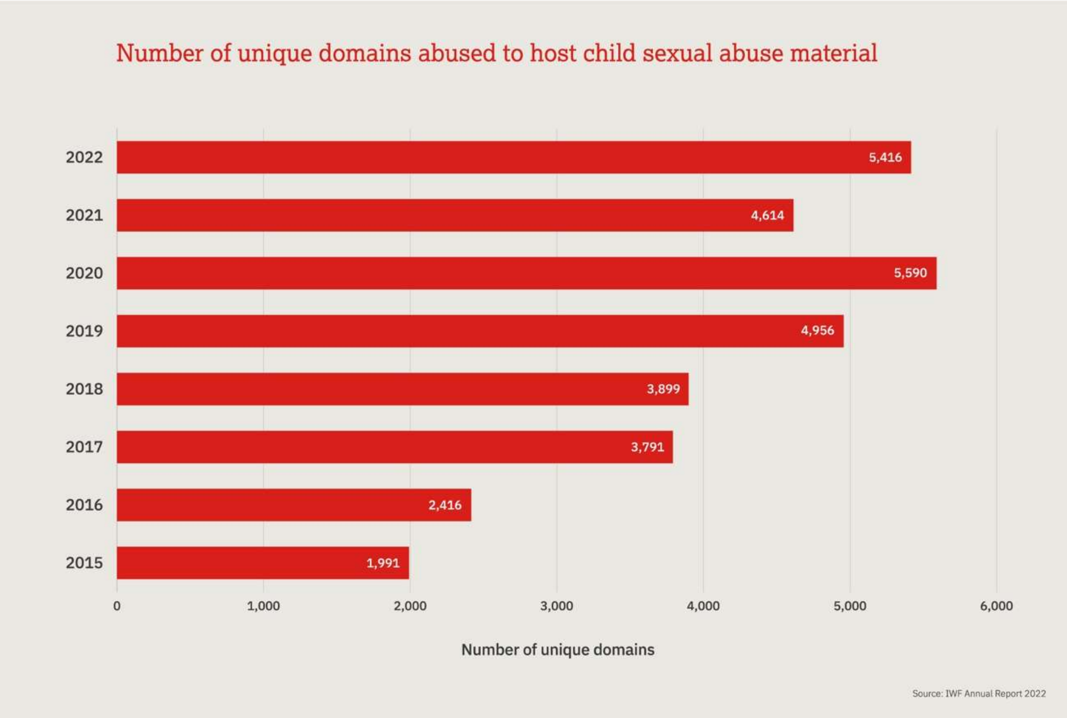
Domain analysis

Domain Distribution: In addition to the increased number of reports actioned in 2022, we also observed an increase in the number of unique second-level domains hosting child sexual abuse material.

- The number of unique second-level domains increased by 17% from 4,614 as identified in 2021 to 5,416 in 2022, representing an increase of 802 domains.
- Of the 5,416 unique second level domains identified as carrying child sexual abuse material, over half (3,057 or 56%) were classified as being dedicated to the sale and/or distribution of child abuse images for financial gain.

For clarity, the diagram below sets out the domain naming conventions used throughout this report.




Number of unique domains abused to host child sexual abuse material

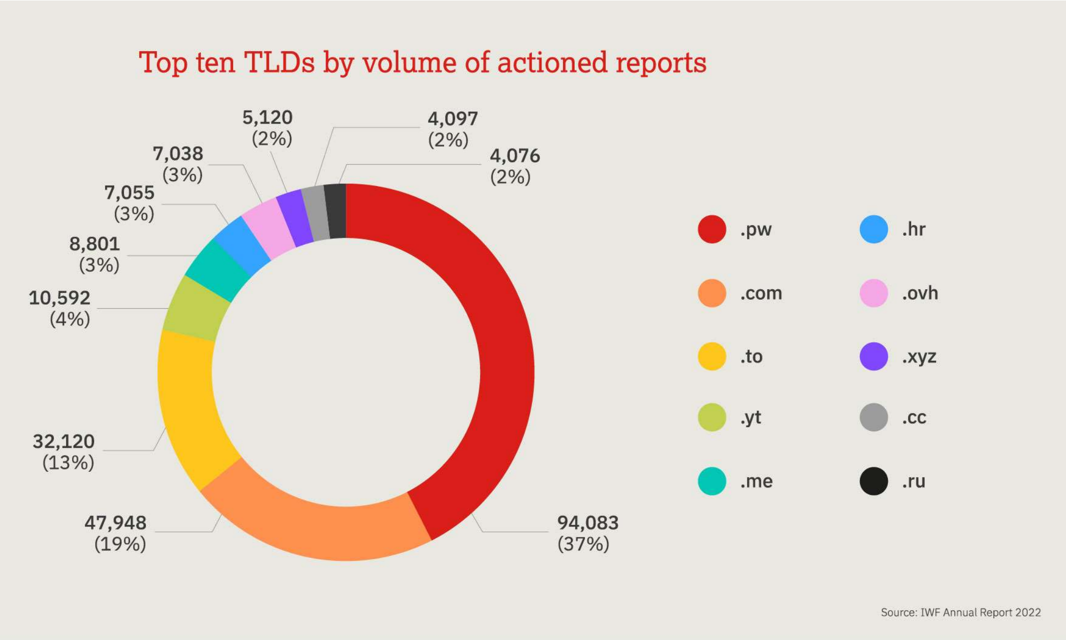
Source: IWF Annual Report 2022

Websites containing child sexual abuse content were registered across:

- 209 top level domains (an increase from the 162 TLDs identified in 2021)
- 97 generic Top-Level Domains (gTLDs), and
- 112 country code Top Level Domains.

Domains were traced to hosting in 55 countries.

For domain analysis purposes, the webpages of www.iwf.org.uk, www.iwf.org.uk/report, and www.iwf.org.uk/what-we-do are counted as one domain: iwf.org.uk


Top ten TLDs by volume of actioned reports

Source: IWF Annual Report 2022

New Generic Top-Level Domains, or gTLDs, continue to be released to meet the demand and consumer choice for new and exciting top level domain names, new TLDs will often spark interest and demand from specific sectors which seek to align their website or brand to a TLD e.g., .biz is an attractive alternative TLD choice for the business sector.

Our monitoring of TLDs shows that there have been some significant changes in the top 10 listings this year. Notable changes include the .com TLD that has historically always appeared at the top of our most abused domain rankings, in 2022, it dropped to second position, a reduction of 63% representing 83,241 fewer reports than in the previous year.

The .pw TLD was the most abused TLD in 2022 with 94,083 confirmed reports. It was previously listed 25th in 2021 when 294 child sexual abuse reports were identified. Its dramatic increase in abuse is directly related to several image host sites abusing the .pw TLD and accounted for 93% of all the child sexual abuse imagery identified on .pw.

The country code TLD .yt (French region Mayotte) was previously unlisted in 2021, and subsequently rose to fourth position as a direct result of nefarious activity involving two image host sites. Ironically neither of the image host sites were hosted in France, but were traced to be hosted in the Netherlands, Russian Federation and Taiwan at various points in the year.

What can we do about this abuse?

Our Domain Alerts help our Members in the domain registration sector prevent the abuse of their service by preventing criminals registering websites with a known CSAM abuse history being reregistered on additional TLDs.

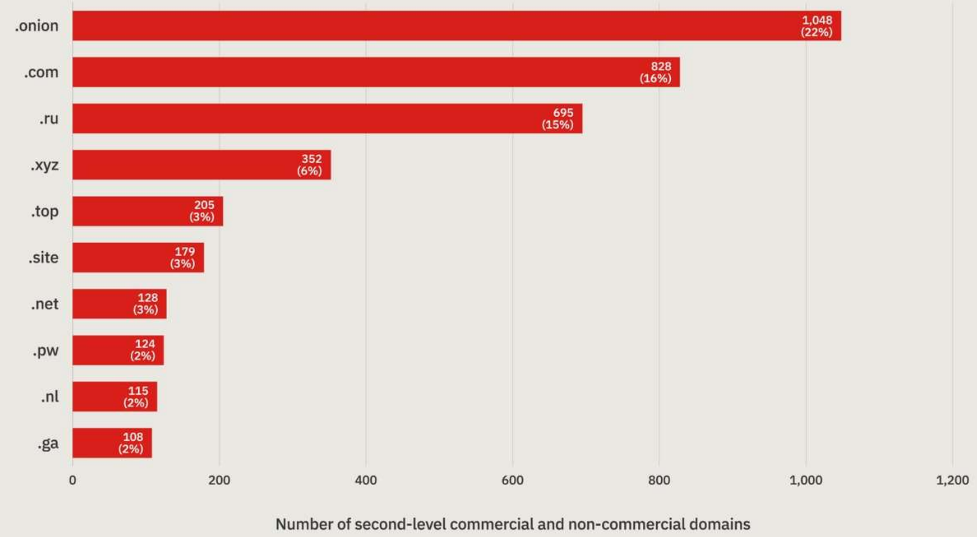
Domain analysis by second-level domain

“www.badsite.com” – in this URL, the ‘.badsite’ is the second level domain of the website address.

We have published data for the second consecutive year which gives additional insight into the scale and nature of domains abused to distribute child sexual abuse material across different TLDs.

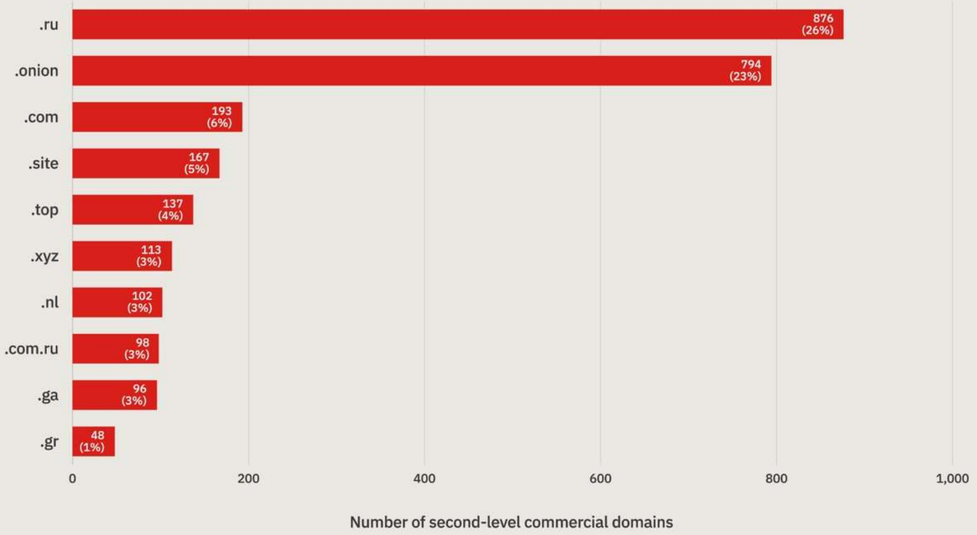
We are able to show the number of unique second-level domains found to be carrying child sexual abuse where they are grouped by the TLD on which they resided.

Top 10 TLDs used for commercial and non-commercial distribution of child sexual abuse material (instances of unique second-level domains)



Source: IWF Annual Report 2022

Top 10 TLDs used for commercial distribution of child sexual abuse material (instances of unique second-level commercial domains)



Source: IWF Annual Report 2022

Second-level TLDs specifically registered and used for the commercial distribution of child sexual abuse should rightly be a point of focus and we continue to research additional ways to locate and remove the sites and disrupt the registration of new sites.

What can we do about this?

By understanding more about how second-level TLDs are specifically registered and used for the commercial distribution of child sexual abuse material, we can make them a point of focus for our work. We continue to research new ways to locate and remove these sites and disrupt the registration of new sites for this purpose.

Top-level domain hopping

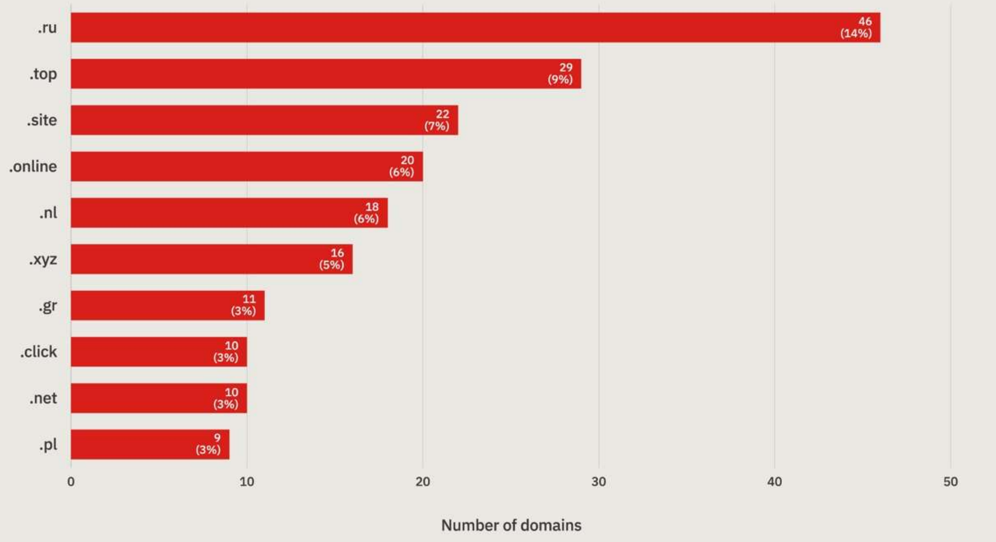
What is Top-level domain hopping?

“Top-level domain hopping” is when a site (e.g., ‘badsite.ru’) keeps its second-level domain name (‘badsite’) but changes its top-level domain (‘.ru’), in essence, creating a new website typically with different hosting details but retaining the sites identifiable ‘name brand’. From ‘badsite.ru’, multiple additional sites ‘badsite.ga’, ‘badsite.ml’ or ‘badsite.tk’ could be created. This allows instances of a website to persist online after the original has been taken down while keeping the website recognisable and easy to find by followers of the site.

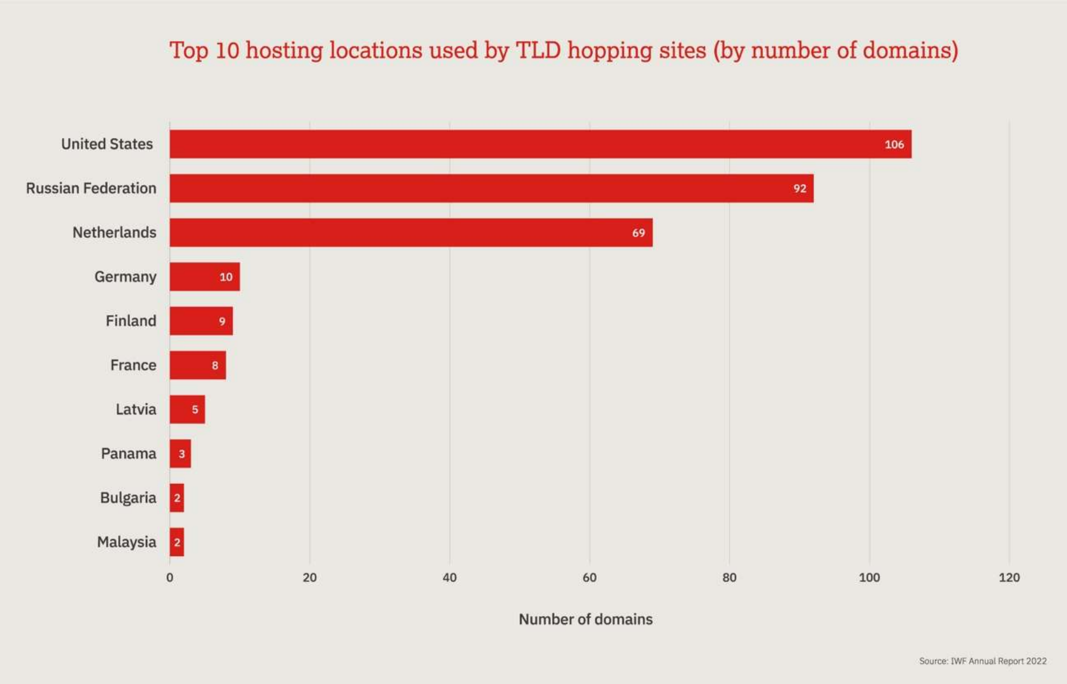
- 319 dedicated commercial second-level domains were identified to have hopped domain at least once in 2022.

Please note that no TLD instances from previous years were counted in this analysis, meaning that to be included in the statistics, the sites had to exist on a minimum of two different TLDs in 2022.

Top 10 TLDs abused in domain hopping (by number of domains)



Source: IWF Annual Report 2022



Source: IWF Annual Report 2022

- 125 second-level domains were found to have hopped once;
- 14 hopped twice;
- four hopped three times;
- one hopped five times in a bid to remain online and active in the 12-month monitoring period.
- **19 countries were identified as hosting domain hopping sites.**

We first work with partners to ensure that the site is removed from the internet. Every subsequent hop, however, then requires a new action by our analysts to re-enforce the previous take down(s) by actioning the site again on the new TLD.

When tracking the hosting country, we noted that some sites often changed TLD but remained hosted in the original host country; other sites showed a preference to change hosting country after each TLD domain change, sometimes returning to the originally identified hosting country after a period of hosting elsewhere under a different TLD.

What can we do about this?

Domains are allocated and managed by internet registries and registrars. Our ongoing work in this area will enable us to identify domains exploiting the legitimate TLD marketplace. We continue to work with Members to not only identify and remove criminal sites but offer new preventative measures to guard against domains hopping to unsuspecting TLDs.

We hope to involve more registrars and registries in the fight against this exploitative practice in 2023, and to this end we have started a service for Members which provides **an active ‘Watch list’ of second level domain strings** which can be used to pre-warn registries and registrars of domains that have a proven history of domain hopping exclusively in the sale and or distribution of child sexual abuse material. The new list service is live and available to Members wishing to access this new important data set.

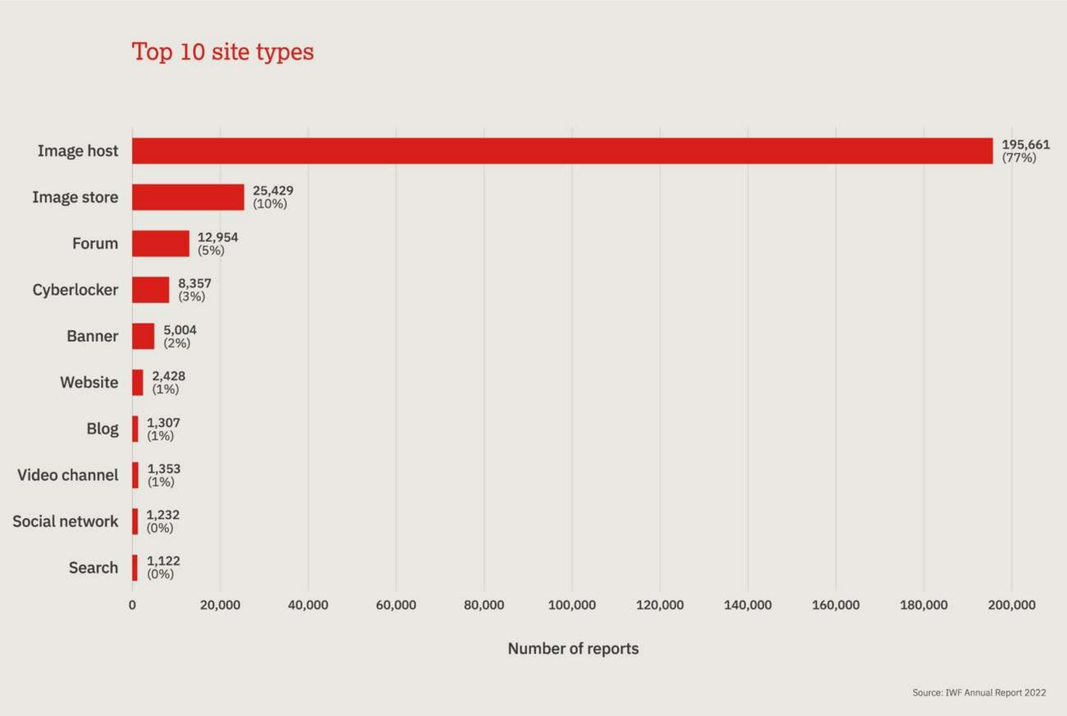
Site types

In 2022, as in previous years, image hosts were the website type most frequently abused by offenders distributing child sexual abuse imagery. These sites provide “storage” for images which either appear on dedicated websites or are shared within forums – another heavily abused site type.

When our analysts see this technique, they ensure the website is taken down and each of the embedded images is removed from the image hosting service. By taking this two-step action, the image is removed at its source and from all other websites into which it was embedded, even if those websites have not yet been found by our analysts.

Cyberlockers continue to be exploited by criminals sharing child sexual abuse imagery. These high-storage sites can be used to share one image or video at a time, or one or more folders that could potentially contain hundreds of images or videos under a single URL.

Image hosts also allow vast quantities of images to be indexed and saved, however these are not as easily accessible to the public as an image host or cyberlocker site.


Top 10 site types

Source: IWF Annual Report 2022

What can we do about this?

Our award-winning IWF Hash List, launched in 2016, can help image hosts to tackle this abuse by preventing the upload, sharing and storage of known child sexual abuse images and videos.

As well as removing images and videos from forums, chat sites and other platforms where child sexual abuse imagery is shared, our analysts ensure that these files are taken down at source by locating the image host sites where they are often stored. This prevents further distribution.

Paid for vs free hosting services

- 228,927 URLs (90%) were hosted on a free-to-use service where no payment was required to create an account or upload the content.

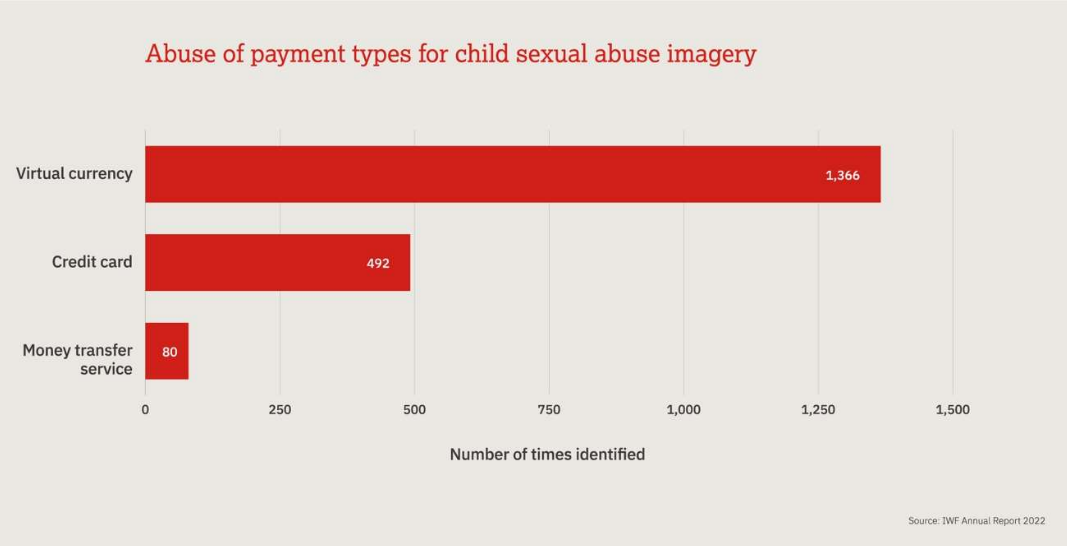
In the remaining 10% of cases, the content was hosted on a paid-for service, or it was not possible to tell whether the hosting was free or paid for.

Commercial content

We define commercial child sexual abuse imagery as images or videos that were seemingly produced or being used for the purposes of financial gain by the distributor.

Of the 255,571 webpages we confirmed as containing child sexual abuse imagery in 2022, 28,933 (11%) were commercial in nature. This is the same as last year, when we took action against 28,390 (11%) commercial webpages.

Of the commercial sites we actioned, we identified a number of different payment methods being offered.



Source: IWF Annual Report 2022

In 2022 we actioned 1,025 reports where commercial sites were offering a payment option.

Across all 1,025 reports we found 1,366 instances where crypto currencies were offered as a type of payment. These were attributed to 495 unique URLs.

Unfortunately, due to restrictions on some sites, not all payment methods were visible. 40% of those with no payment type visible were ICAP sites.

Find out more about our ICAP sites here.

What can we do about it?

We monitor and research any new trends we have observed. Sharing this intelligence with our sister hotlines and law enforcement agencies means that websites can be removed and distributors can be investigated.

Any payment information displayed on these commercial websites – including cryptocurrency details – is captured and shared with our partners in the financial industry. This helps to prevent misuse of their services and disrupt further distribution of the criminal imagery.

ICAP sites

We’ve identified a new way in which child sexual abuse material is being distributed which increases the risk of internet users stumbling across this criminal material.

These “invite child abuse pyramid” sites, or ICAP sites for short, incentivise users to share links to child sexual abuse sites far and wide in a “scattergun” approach with spams links on a variety of platforms such as social media and chatrooms among others.

The criminals running the sites benefit from increased web traffic and additional income with offenders potentially buying further videos of child sexual abuse and creating their own links to spam to others.

We first identified these sites in July. Thousands of reports have now been received by our hotline which are linked to this method of distribution.

What can we do about this?

We’ve been briefing law enforcement, our sister hotlines and technology companies to alert them to this new way of distributing child sexual abuse material which puts internet users at greater risk. We will continue to monitor this closely through 2023.

Dark web reports

What are hidden services?

Hidden services are websites hosted within proxy networks – sometimes also called the dark web. These websites are challenging as the location of the hosting server cannot be traced using normal methods.

- In 2022 we identified 1,067 new hidden services, up from 931 in This is an increase of 15%.

What can we do about this?

We work with the UK's National Crime Agency to share intelligence on any new hidden services which are displaying child sexual abuse imagery. With this intelligence, NCA can work with national and international law enforcement agencies to investigate the criminals using these websites.

Commercial dark web reports

Since 2016, we have seen a rising trend in 'commercial' hidden services – dedicated websites offering child sexual abuse imagery for sale.

Of the 1,067 newly-identified hidden services distributing child sexual abuse imagery in 2022, 848 (79%) were assessed as being commercial. Due to the anonymous nature of hidden services, these commercial websites increasingly accept payment in virtual currencies as well as credit cards.

What can we do about this?

We work with the wider payments services industry and our Virtual Currency Alerts help our Members in the virtual payments sector to identify payments which are associated with child sexual abuse imagery. We continue to monitor trends in these payments and share this intelligence with our partners.

Commercial disguised websites

What are commercial disguised websites?

Since 2011, we have been monitoring commercial child sexual abuse websites which display child sexual abuse imagery only when accessed by a 'digital pathway' of links from other websites. When the pathway is not followed, or the website is accessed directly through a browser, legal (usually pornographic) content is displayed. This means it is more difficult to locate and investigate the criminal imagery.

- In 2022, we uncovered 5,525 websites using a "digital pathway" to hide child sexual abuse imagery.
- Of the 28,933 commercial websites overall, 3,074 (11%) were also using a digital pathway.
- It represents a decrease of 42% on the 5,258 commercial disguised websites identified in 2021.

We saw a steep increase in image host sites using this 'digital pathway' in 2021. In 2022, we found that this trend has decreased. Most of the disguised sites we took action on were commercial in nature and dedicated to displaying child sexual abuse imagery.

Disguised websites have also continued to exploit 'top-level domain hopping' to avoid detection and remain online.

What can we do about this?

We actively monitor the techniques used by these websites in order to uncover the criminal material in order to get it removed. We also share intelligence with our partners to enable them to do the same.

UK hosted child sexual abuse imagery

UK hosting volume

The UK hosts a small volume of online child sexual abuse content.

- In 2022, 640 URLs displaying child sexual abuse imagery were hosted in the UK, an increase of 68% from 381 URLs in 2021.
- The UK hosted 0.25% of all child sexual abuse URLs which IWF identified in 2022.
- 433 reports related to multiple URLs identified on the same day and attributed to one host.

In 465 cases, the criminal content had already been removed by the time we received authorisation from the police to instigate its removal or it had moved hosting country already, leaving us with 175 URLs to take action on.

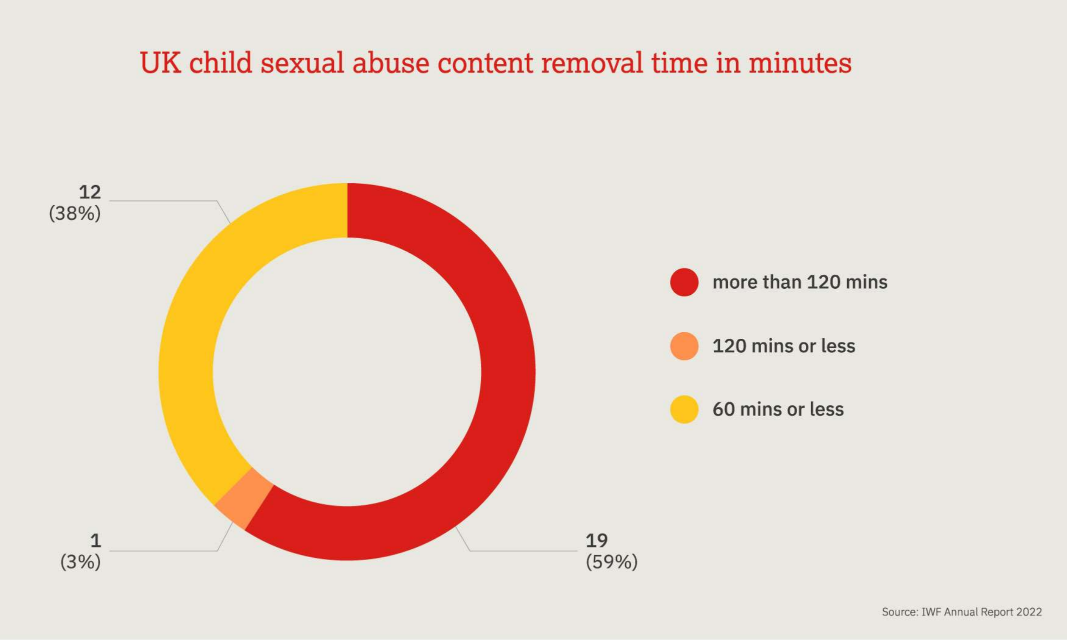
32 takedown notices relating to the 175 URLs were sent to UK hosting companies (we might send one notice for several webpages).

UK Child sexual abuse content removal in minutes

We have to act quickly. The longer an image stays live, the more opportunity there is for offenders to view and share it, and more harm is caused to the victims.

In partnership with the online industry, we push to secure the rapid removal of this content. The 'takedown' clock ticks from the moment we issue a takedown notice to the hosting company, to the time the content is removed.

Fastest removal: 3 minutes



Source: IWF Annual Report 2022

- 16 companies’ services in the UK were abused to host child sexual abuse images or videos during 2022.

We issue takedown notices to UK companies, whether they’re in IWF membership or not.

- **All companies who were abused were not IWF Members**.

What can we do about this?

We use a minimum of three pieces of technology to trace the hosting location, then issue a takedown notice to the company which is hosting the material. Law enforcement are consulted during this process and evidence is retained for investigation.

Although the URL numbers are relatively small compared to the global problem, it’s important that the UK remains a hostile place for criminals to host this content.

Non-photographic child sexual abuse

IWF's remit includes the identification and removal of UK-hosted non-photographic (Prohibited Images) child sexual abuse images and videos.

In 2022, we took action on 285 reports of non-photographic child sexual abuse imagery (a 22% increase from 2021). However, after our assessment, none of these were confirmed as UK-hosted content.

At the end of 2022, 324 unique URLs of non-photographic child sexual abuse imagery were listed on the NPI URL List. 18 IWF Members subscribe to this service.

What can we do about this?

The UK is one of the few countries in the world where non-photographic child sexual abuse imagery is criminal.

If we find this content hosted in the UK, we issue a notice to the hosting provider who removes it. This hasn't happened in the UK since 2016. However, this type of content does exist online and if UK-hosted, would fail UK laws.

Technology companies want the flexibility of being able to block and filter it to prevent their customers from stumbling across it.

Therefore, we created the NPI List, which contains, drawings, computer-generated imagery (CGI) and other non-photographic representations of child sexual abuse which is hosted outside of the UK.

The URLs provided in the NPI List are those deemed at the time of assessment to breach UK legislation, specifically Sections 62 to 69 of the Coroners and Justice Act 2009. Several international technology companies use this list to protect their services for their customers.

IWF URL List

We provide a list of webpages containing child sexual abuse images and videos hosted outside of the UK to companies who want to block or filter them for their users' protection, and to prevent the repeated victimisation of the children in the images. We update the list twice a day, removing and adding URLs.

During 2022:

- The list was sent across all seven continents.
- A total of 230,922 unique URLs were included on the list (a 14% increase on 203,234 in 2021).
- On average, 1,029 new URLs were added each day (1,001 in 2021).
- The list contained an average of 11,488 URLs per day (a 108% increase from 5,526 in 2021).

Case Studies

What it is like to lead the IWF Hotline

As IWF Hotline Manager, Tamsin McNally guides and supports a busy team who have the very difficult but important job of viewing and assessing child sexual abuse imagery every day.

In a recent blog, she provides insight into a typical working day, where she manages both our 14-strong team of Hotline Analysts who assess public reports and ensure criminal content is removed, as well as the Taskforce team of 14 who view and grade hundreds of images a day for the UK Government's Child Abuse Image Database.

Her days are varied and involve her being able to switch from presenting meetings for external partners, such as law enforcement with whom we work closely, to providing advice to a distressed member of the public who has stumbled across child sexual abuse content online.

In the blog, Tamsin, who has been with the IWF for more than eight years, stresses how important it is that she looks after the welfare of her team, whom she regards as some of the best people she has ever worked with.

Tamsin says: "People say that this is one of the hardest jobs out there. It's not right for everyone, but the people working here make me so ridiculously proud. They are fantastic people doing an incredibly difficult, but important, job."

Read Tamsin's blog in full.

Forums

Forums are online discussion websites where individuals can post messages, images, and replies. The posts are generally organised by a thread or topic.

Forums generate a vast amount of work for IWF analysts but this is not often apparent with the data we present in our annual report.

In 2022, our data shows that just 5% of child sexual abuse imagery that the IWF finds are on forums. But forums pull in a vast number of images and videos from other types of websites known as image hosting sites and cyberlockers. **This often disguises the fact that forums are a main culprit for spreading child sexual abuse material on the internet.**

Forums are also complex: Their removal is difficult as they often host legal content as well as illegal, hence we cannot simply get a forum removed at domain level, meaning the entire forum would be removed. In addition, they move host regularly, making permanent removal very difficult to secure. Therefore, we decided to carry out this snapshot study.

The purpose of the study was to record information about forums while the forums were still "live" and to provide an insight into the complexity of getting child sexual abuse material on forums removed. We hope that the information here is useful to others working in this space.

Forums are commonly reported to the IWF by the public

In addition, analysts often visit forums to proactively search for child sexual abuse material.

Arguably forums provide the biggest source of all proactive work given the volume of images found on each page. Forums are massive; there will be **multiple topics** within a forum and each topic contains **many threads** and each thread can contain **many pages all full of images** and links to potential child sexual abuse material (CSAM). **Unless both sexes are involved in sexual activity in an image, content of boys and girls tend to remain in separate places within a forum.** Often a proportion of the forum will contain legal content, which makes it difficult to remove the whole forum seeing as the whole forum is not actually illegal. Therefore, analysts tend to “action” (perform a set of tasks which lead to the removal of the images/videos) at thread level opposed to the domain level.

Forums that are dedicated to hosting child sexual abuse material predominately contain self-generated content. This is where the abuser is not physically present with their victim but is often directing or coercing the child into performing sexual acts via webcam. Occasionally chats can be seen between the child and person at the other end of the camera.

How forums are abused

Very often, a person abusing a forum for child sexual abuse material will upload images that are hosted elsewhere on a different domain, such as an image hosting site. In addition, beneath each image, a link is posted which appears to contain the whole video to the image that the viewer has been presented with. This link is hosted on a different domain too and it often requires payment to download the video.

When IWF analysts take steps to remove the illegal images and videos hosted within a forum, they need to trace where in the world the content is hosted. If the country where the content is hosted has a hotline, the information is sent to that hotline in the first instance. If the country does not have a hotline, the analyst passes this information onto law enforcement. In both instances if the content remains live, and the IWF has not been informed of an ongoing police investigation, the analyst will send a notice to the company that is hosting the content on its servers requesting for the content to be removed.

Methodology

Forum choice:
Three forums that are known to host child sexual abuse material were examined during the study:

- Forum 1 is predominantly known for hosting images of boys. The sexual abuse imagery on this forum was removed on day two of the study (this could have been as a result of IWF action – this is explained further down in the study) and before enough data had been collected.
- Forum 2 is predominantly known for hosting images of girls. This sexual

abuse imagery on this forum was also removed on day two of the study, but a large quantity of data had already been captured.

In both instances the forums remained live, however all the images were taken down/removed from the page. The links to the videos posted under each image remained on the page. However, access to these videos requires payment and the IWF does not go beyond payment barriers, therefore the links were not accessible to download. This did not pose a problem in the data collection given that there are so many forums dedicated to hosting child sexual abuse material. Hence, one more forum was chosen to continue with the data collection as enough data had already been collected of girls.

- Forum 3 was added on day three of the study, which housed sexual abuse imagery of boys and this was substituted for forum 1 to enable enough data to be captured.

Time spent on forum examination:
One hour per day, at roughly the same time each day, was spent examining the pages of the chosen forums. This took place over a four-day period. However, please note that this was just three days for the boy forums due to the content becoming unavailable and there being less content to find. We recorded a variety of information to highlight what goes on in forums and show how they operate. This information includes:

- Date and time checked;
- Thread date and time;
- Forum URL;
- Sex of child;
- Age categories;
- Self-generated or not;
- Website of the images being pulled into the forum;
- Website that the video link comes from;
- If a premium is required to download the video;
- Payment mechanisms to download videos;
- How many children seen in the images;
- If the offender is present in the image;
- The room in the house where the abuse took place;

- Hosting country of the forum;
- Username of the user posting content;
- If the images have been seen before by the Quality Assurance (QA) Officer;
- Anything of note that stood out in the images.

About the Quality Assurance Officer at IWF who collected the data

The IWF staff member who led the study has worked at the IWF for 14 years. She was an Internet Content Analyst for 13 years before becoming a Quality Assurance Officer. Both roles require the assessment and checking of large volumes of child sexual abuse material on a daily basis. During that time, she has seen many victims of child sexual abuse.

Top level findings

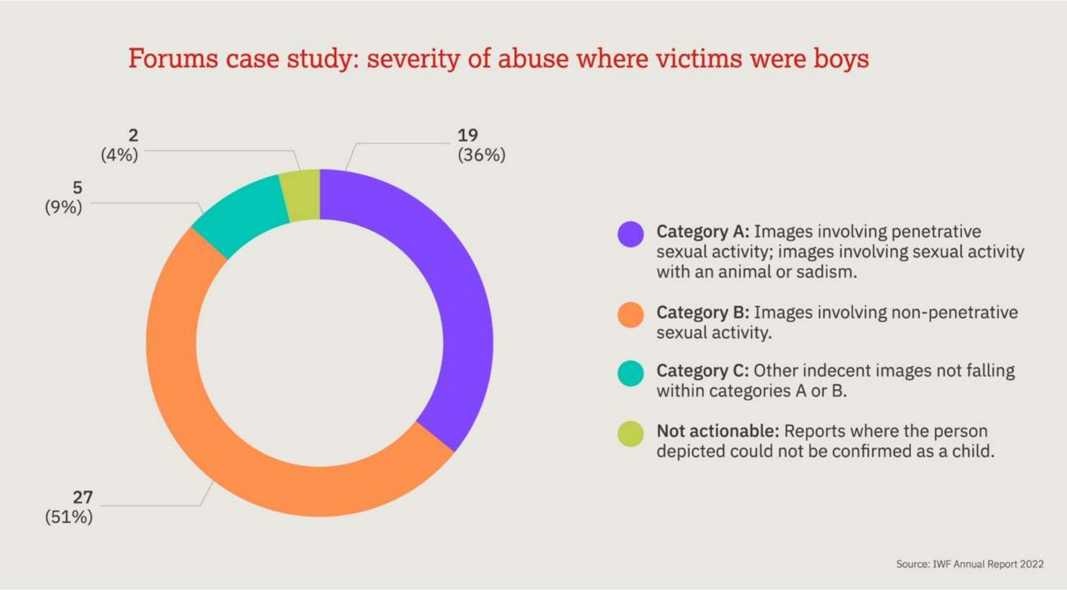
Analysis of content showing boys:

- 53 images of boys were recorded, 58% of the images of boys were of a self-generated nature.
- More boys were seen engaging in sexual activity, in a self-generated setting, while other children were present.
- In boys, the most frequent age seen was 11-13 years.
- Boys often appear to be under-represented in the data in terms of volume, however they are more likely to be assessed as Category A and Category B (more severe categories).
- 42% of boys had not been seen before by the Quality Assurance Officer who collected the data.

Analysis of content showing girls:

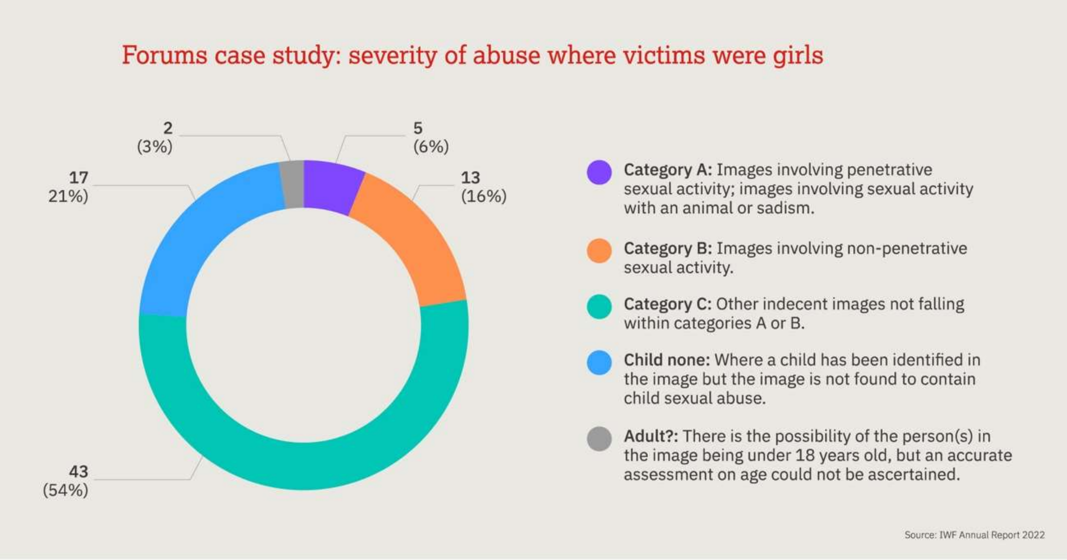
- 80 images of girls were recorded, 100% of the images of girls were of a self-generated nature.
- Girls are more likely to engage in self-generated content with no other children present.
- Girls aged 7-10 were the most frequently seen.
- 84% of the girls had not been seen before by the Quality Assurance Officer who collected the data.

Categories of child sexual abuse imagery found:


Forums case study: severity of abuse where victims were boys

Source: IWF Annual Report 2022

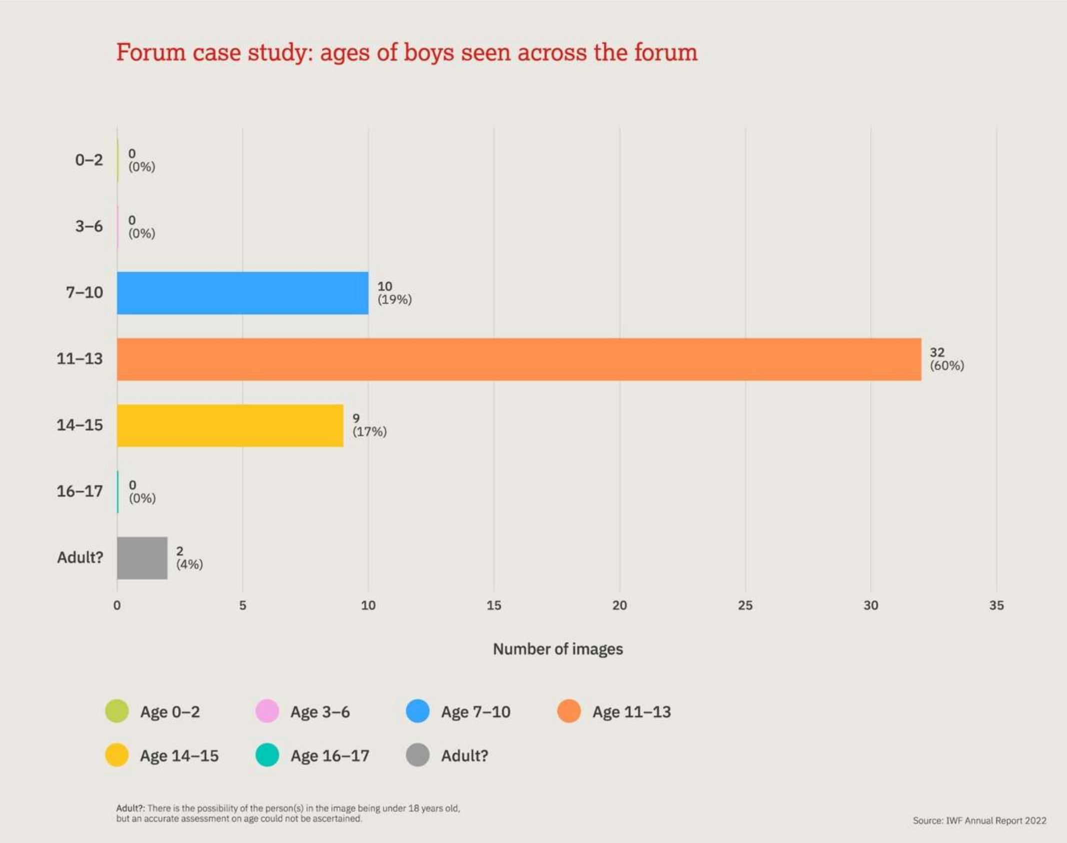
Four percent of the images were borderline on age. For the purposes of this study, this was categorised as "Adult?". Please note that Adult? has been represented in the age chart below. Adult? means that there is the possibility of the person(s) in the image being under 18 years old, but an accurate assessment on age could not be ascertained. We see vastly fewer boys in forums; however, the categories of boys are generally more severe which is also reflected in the data collection.


Forums case study: severity of abuse where victims were girls

Source: IWF Annual Report 2022

Child none is not an actionable category, but it has been represented in the data here as 21% of the girls were seen appearing to be in the early stages of revealing themselves to the camera, for example the girl may have been in her underwear or starting to undress which does not meet the threshold for further action.

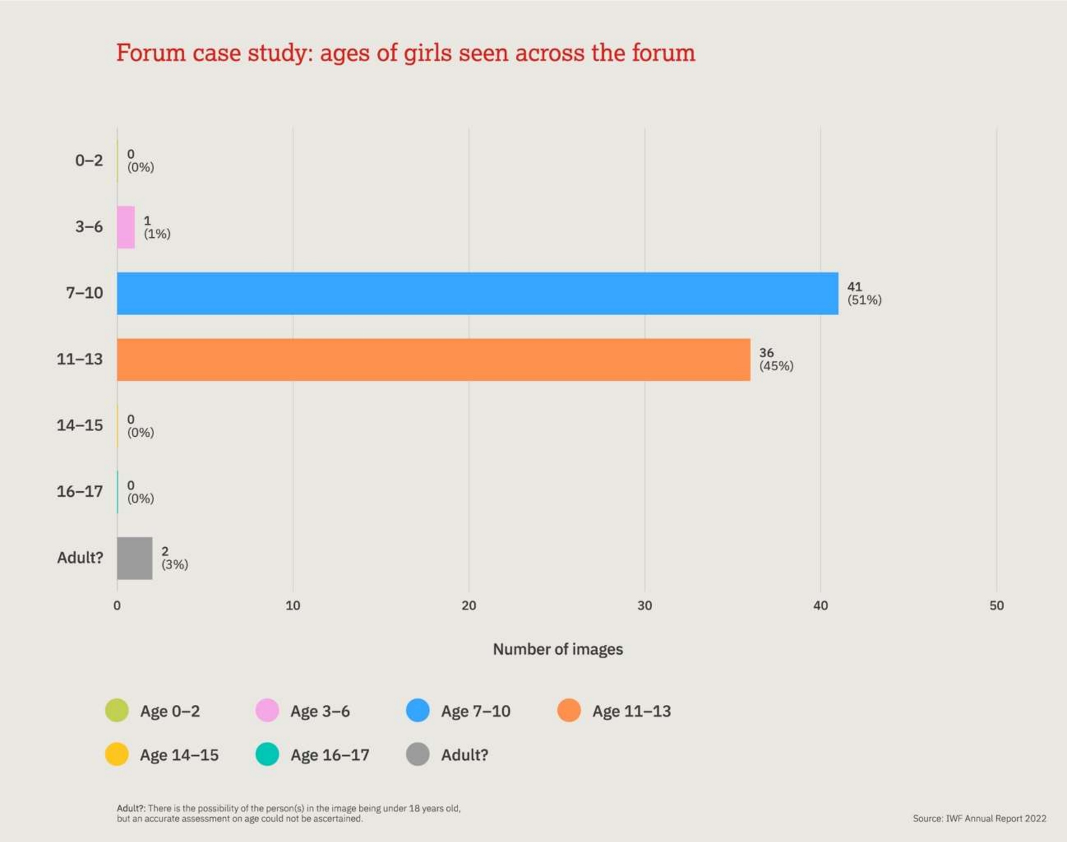
We were confident that 97% of the images seen contained children.



Forum case study: ages of boys seen across the forum

Adult?: There is the possibility of the person(s) in the image being under 18 years old, but an accurate assessment on age could not be ascertained.

Source: IWF Annual Report 2022



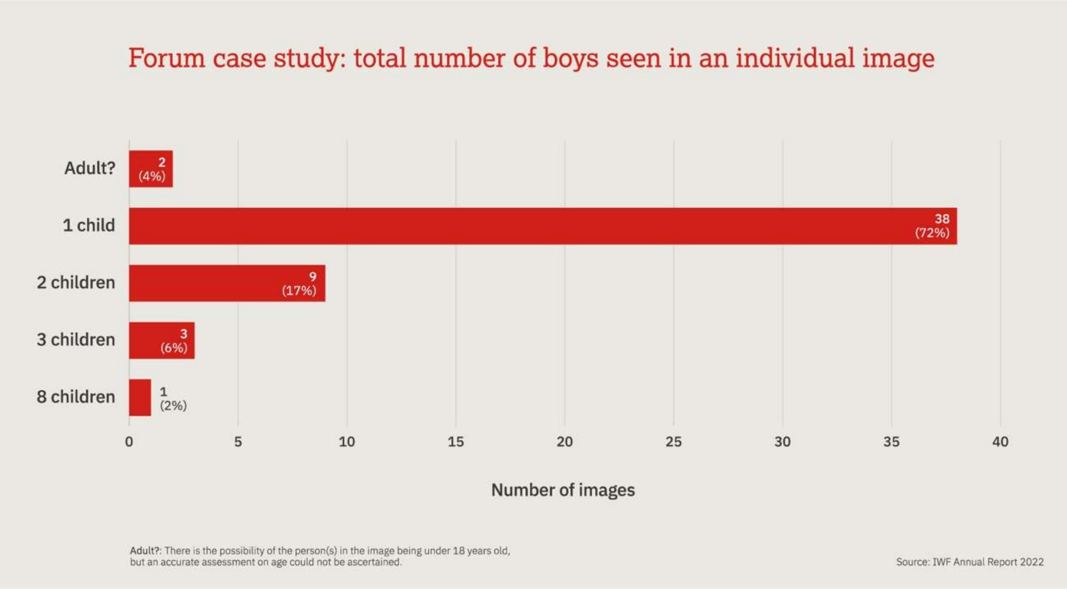
Forum case study: ages of girls seen across the forum

Adult?: There is the possibility of the person(s) in the image being under 18 years old, but an accurate assessment on age could not be ascertained.

Source: IWF Annual Report 2022

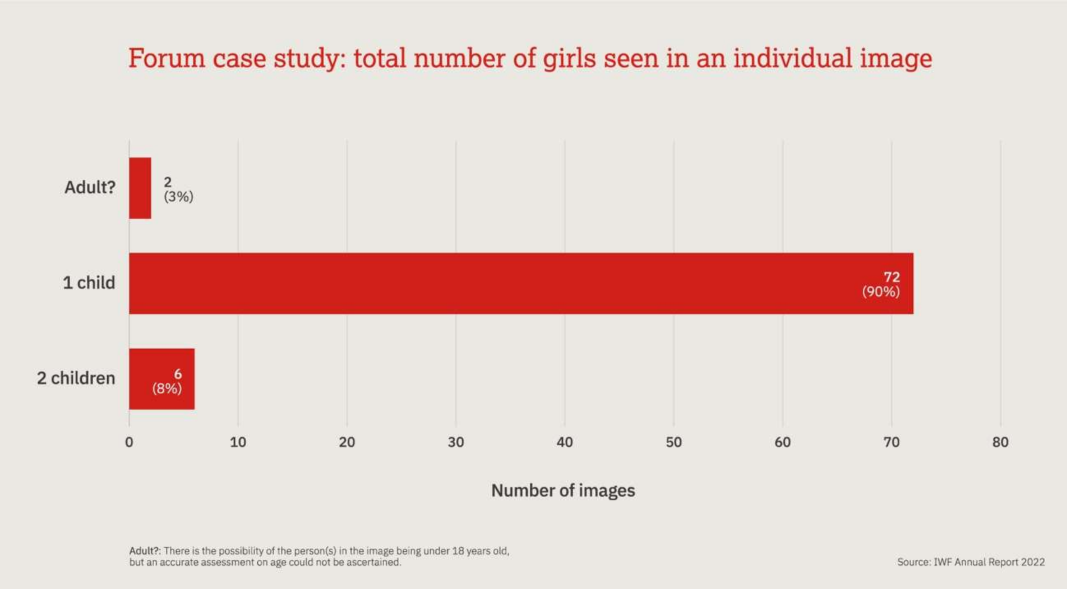
Number of children seen in individual images:

- 72% of the images showed 1 **boy** present in the image.
- 17% of the images showed 2 **boys** present in the same image.
- 6% of the images showed 3 **boys** being present in the same image.
- One image showed 8 children present (**7 boys and 1 girl**) however this was a grid image where multiple images had been merged into one large image.
- 4% accounted for *Adult*? images (**male**)
- 90% of the images showed **girls** on their own in an image
- 8% of the images showed 2 **girls** being present in the same image
- 3% accounted for *Adult*? images **(female)**


Forum case study: total number of boys seen in an individual image

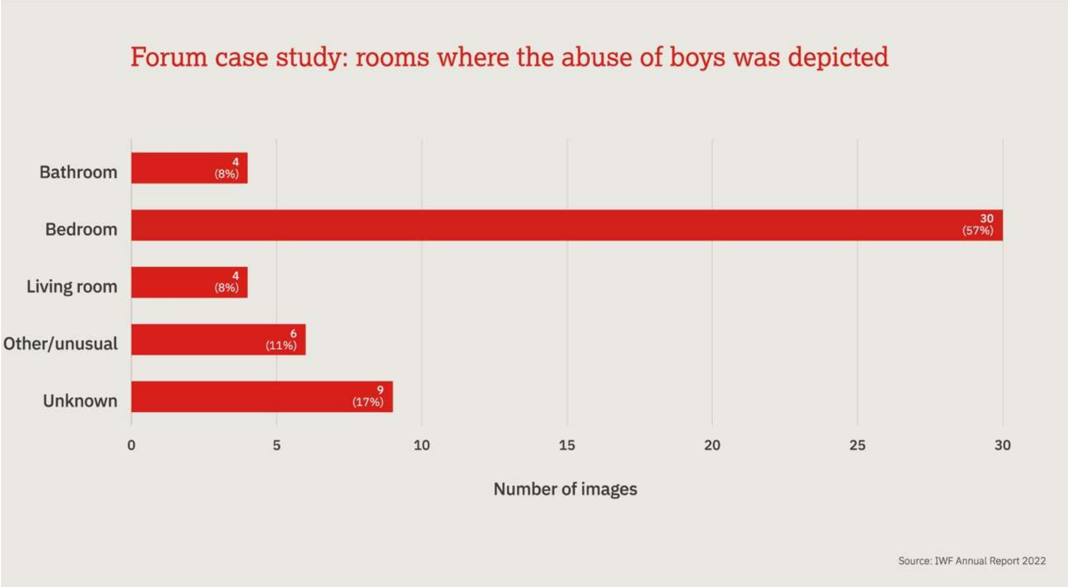
Adult?: There is the possibility of the person(s) in the image being under 18 years old, but an accurate assessment on age could not be ascertained.

Source: IWF Annual Report 2022


Forum case study: total number of girls seen in an individual image

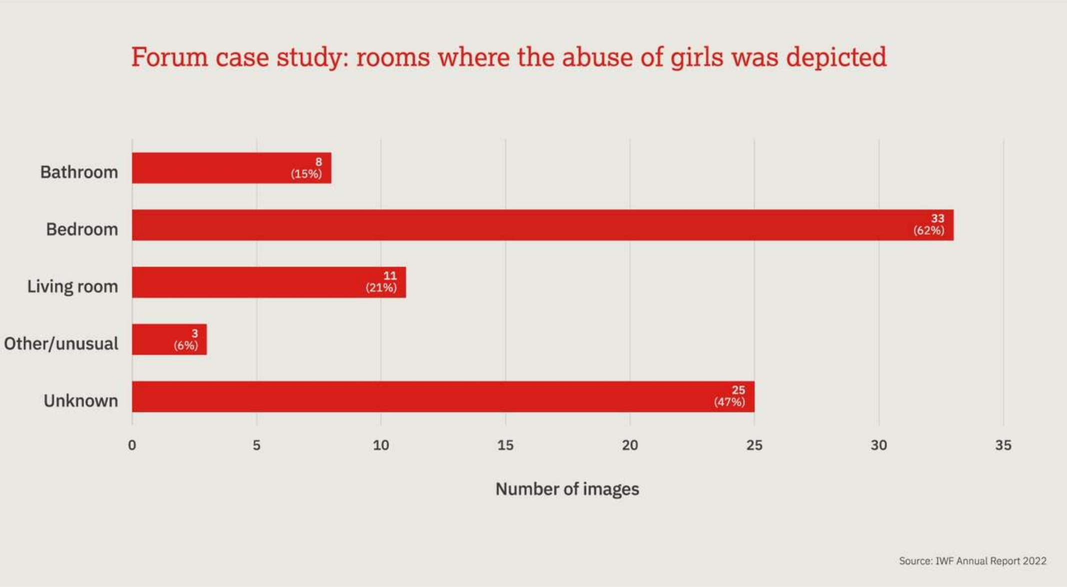
Adult?: There is the possibility of the person(s) in the image being under 18 years old, but an accurate assessment on age could not be ascertained.

Source: IWF Annual Report 2022



Forum case study: rooms where the abuse of boys was depicted

Source: IWF Annual Report 2022



Forum case study: rooms where the abuse of girls was depicted

Source: IWF Annual Report 2022

With the exception of the ‘unknown’ category, there was not a great difference between girls and boys in rooms where the child sexual abuse imagery had been captured.

As expected, the ‘bedroom’ was the most recorded room, accounting for 57% for the boys and 41% for the girls. This is not surprising given that most of the images were self-generated and the bedroom is the most likely place that a child will be alone with a device. Of course, some siblings may share a room and in one instance a child was seen on their device sitting on a bunk bed.

‘Unknown’ was the next highest recorded room. In these instances, the room could not be identified as these images tended to be closeup shots of the child’s genitals and not much else can be seen in the image. This accounted for 17% for the boys and 31% of the girls.

During the examination of the imagery, we were also able to identify other types of rooms which are less common to see. Examples of ‘unusual rooms’ found include a public changing room, outside in a field, a shed, a hallway and a playroom where lots of toys and a baby changing unit were identified.

Self-generated content vs not self-generated content

The term self-generated indicates that the abuser is not physically present with the child and the child has been groomed, coerced or encouraged into creating the content themselves. It is vital to remember that children are being groomed online and instructed to engage in this behaviour.

53 images of **boys** were recorded (51 images were confirmed as criminal).

- 58% of the images appeared to be self-generated content.
- 25% of the images contained the abuser.
- 13% of the images did not contain the abuser, however, did not appear to be self-generated content either (abuser presumed present however, outside of the image).
- 4% of the images were *Adult*?

Out of 80 images of girls recorded (62 images were confirmed as criminal) none of the images contained an abuser and all of the images appeared to be self-generated content.

- 100% of the images of girls were self-generated.

This is not surprising as most self-generated content that we see is of girls.

How forums operate

Three forums were used for data collection (two for imagery of boys and one for imagery of girls). Generally, the posts were uploaded by the same user on each of the forums checked.

Forums, threads, pages checked:
Forum 1 (boys): One thread checked over 4 pages. 40 images were found in total before the forum went offline.

Forum two (girls): Three threads checked over 10 pages. 73 images were found on one thread, 4 images on the second thread and 3 images on the third thread before the forum went offline.

Forum 3 (boys): One thread checked over two pages. 13 images were found in total.

The above demonstrates how many images can be found within a thread and how pages within a thread can vary in volume. Across the three forums, five threads were checked and returned 133 images.

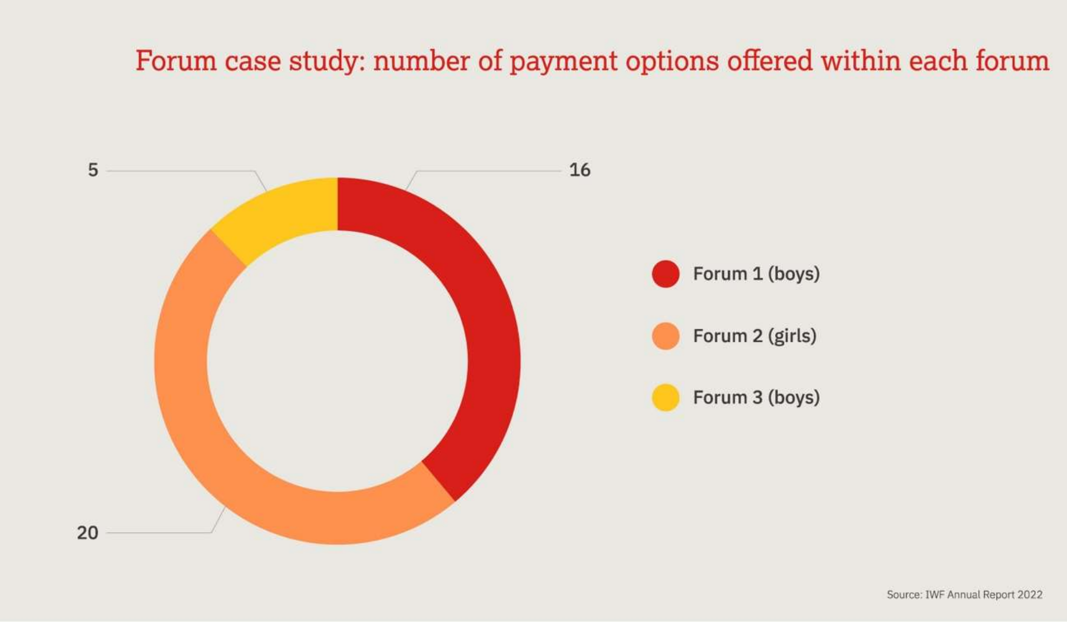
Third Party Hosts:
Forum 1 (boys): Two third party hosts were identified. 100% of the images found on the page were hosted on an external site known as an image hosting site. This means the images were being pulled in from a different website. A link underneath each image was found. These types of sites are known as cyberlocker sites. Every single image had a link to a cyberlocker site, which undoubtedly contained the full video of the content, however payment was required and therefore this could not be accessed or verified. The cyberlocker site was the same one throughout the threads checked.

Forum 2 (girls): Two third party hosts were identified. Once again 100% of the images were hosted on an external site known as an image hosting site and therefore were being pulled in from elsewhere. A link underneath every image was found going to a cyberlocker site. Once again, gaining access to the videos required payment and as the IWF does not breach payment barriers we therefore could not access them. The cyberlocker site was the same one throughout the threads checked.

Forum 3 (boys): Forum 3 was different in that none of the images were being pulled in from an external site. On this occasion 100% of the images on the pages were hosted on the same domain as the forum itself, which generally speaking, is not common. However, two third party hosts were identified. Like the other two forums, every image had a link underneath it going to a cyberlocker site appearing to contain the full video of the content. This time 2 different cyberlocker sites were identified.

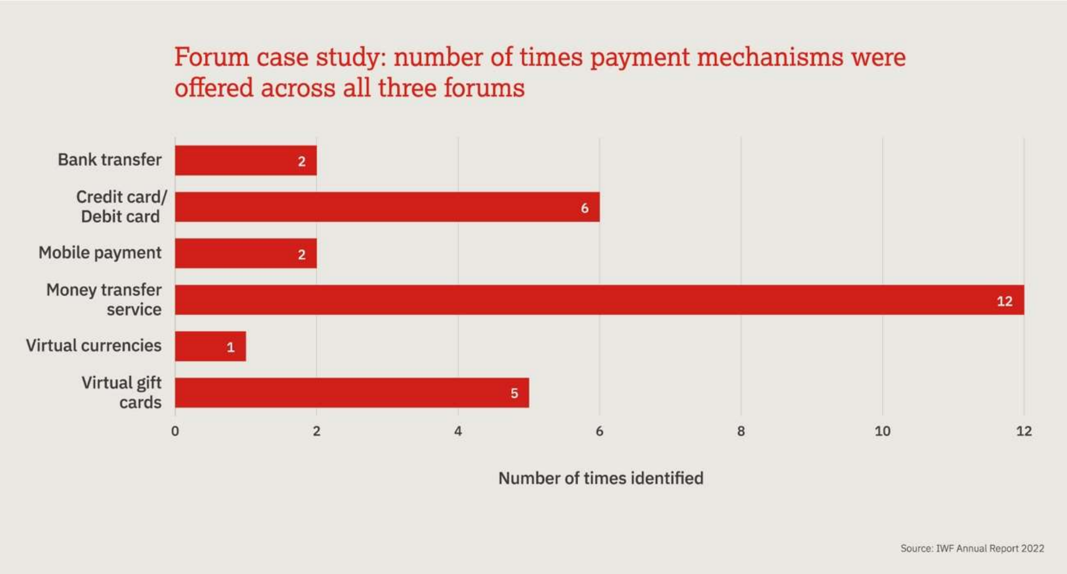
(Please note the image hosting sites and cyberlocker sites were different in all three forums).

Apart from a few video links which were offline, all videos required payment to download. Each forum offered multiple payment methods. The payment options remained the same for every video link within that forum, however, varied across the three forums. The below chart shows how many payment methods were offered for each forum.


Forum case study: number of payment options offered within each forum

Source: IWF Annual Report 2022

The above highlights the overall payment options being offered to make a payment to download the videos and covers the following payment mechanisms: bank transfer, credit card/debit card, mobile payment, money transfer services, virtual currencies, and virtual gift cards. The graph below illustrates this further. Please note this is across all three forums:



Forum case study: number of times payment mechanisms were offered across all three forums

Source: IWF Annual Report 2022

The graph shows that money transfer services were the most common payment mechanism to be offered as a means of payment.

We create a hash (digital fingerprint) of the images that are displayed on forums. These hashes are then made available to Members of the IWF under a strict licence to enable them to stop the upload, sharing and storage of images matching these hashes within their platforms and services.

The complexity of forum hosting

All the forums examined were hosted in either Hong Kong or Malaysia. Content does not usually come down easily or quickly in either of these countries, given that neither country has a hotline. In these instances, the IWF analyst who identifies child sexual abuse material which is hosted in these countries notifies the UK's National Crime Agency (NCA).

Analysts in our hotline are allocated countries to look after and if the content continues to stay available for a period of time after notifying the NCA, the analyst then informs the host company directly with the intention that the host will take the content down. With all of these forums, we had informed the host. Therefore, it is possible that the images on Forum 1 which had been removed during this study was as a result of our analyst's work in notifying the host.

Forums hosting child sexual abuse material will often appear to be removed from the internet but analysts know that these are not truly taken down, often just from the message that is received when loading the URL. We see time and time again how, after just a few days, the forum will be live again but this time with a new host and perhaps a new hosting country. Every country has its own set of laws and regulations, and some hotlines have a better rapport with law enforcement than others. All of these factors influence how quickly a site hosting child sexual abuse material goes offline.

Forum 1 (boys' imagery): This was hosted in Hong Kong. An IWF analyst notified the host and requested that the content be removed in early September 2022 and the images were no longer available on the page a week later. The links were still live on the page, however a premium account was required to access the content, meaning the content was being sold.

Forum 2 (girls' imagery): This was hosted in Hong Kong. An IWF analyst notified the host to request that the content be removed in early September 2022 and the images were no longer available two weeks' later.

Forum 3 (boys' imagery): This was hosted in Hong Kong. An IWF analyst notified the host in mid-September 2022. On the same day the hosting moved to Malaysia and our analyst created a new report, it was then passed on to law enforcement, however before the new host could be notified, the forum moved hosting back to Hong Kong the very next day. This highlights how wily operators of forums can be and how difficult it can be to get the forum offline. This particular forum has been around for some time and first actioned by the IWF in December 2019. It has changed hosting many times and has been actioned by the IWF in many different locations all around the world, most recently in the UK. The site became offline quickly due to the analysts' persistence in chasing up our law enforcement partners.

Age of the posts on the forums

Forum 1 (imagery of boys): This forum had posts dating back a month (at the time of data collection).

Forum 2 (imagery of girls): All posts containing child sexual abuse material were posted in April/May of 2022 and therefore were a few months old at the time of data collection. There are many more images of girls and it appears that newer content is readily available.

Forum 3 (imagery of boys): The second forum featuring boys was different. Half of the posts recorded were two months old and the other half were two years old. Generally speaking across IWF's work, we see fewer images of boys that we are confident in determining are under the age of 18 years, which means that the same images of boys are more likely to be re-posted time and time again. Indeed, in Forum 3 a couple of images had dates stamped on them; one dated back almost 30 years to 1994 and the other one to 1998.

Imagery of new victims

Often images are reposted, duplicated and edited leading to multiple copies of images being posted online. Consequently, we often see images of the same children over and over again.

The Quality Assurance officer who collected the data for this study was interested to record whether she had seen the child victims before (see the section above about the experience of this person). Based on this member of staff's knowledge, she recognised just 16% of the girls that were recorded compared with 58% of the boys seen.

This difference is not surprising, given that there are many more images of girls seen in this type of abuse (self-generated). As mentioned before, fewer images of boys means that the same imagery is more likely to be re-posted time and time.

In summary

This case study was carried out to capture the complexity of removing child sexual abuse imagery on forums. It has also provided an insight into the nature of child sexual abuse material found within just three forums.

Forums generate a large amount of work for IWF analysts. The removal of forums is difficult as they often host legal content as well as illegal, hence it is often the thread/page which is actioned rather than the whole forum at domain level.

In addition, they move host regularly, making permanent removal very difficult.

As forums pull in a vast number of images/videos from other types of websites it means that forums are a main culprit for the wide and global distribution of child sexual abuse images and videos and play a key role in the content’s monetisation.

Operation Makedom

IWF is playing a key role in finding, removing and hashing (creating digital fingerprints) child sexual abuse imagery created by jailed online sexual predator, Abdul Elahi.

In December 2021, Elahi was jailed for 34 years following a police operation called Operation Makedom. He prolifically abused adults and children online. He groomed his victims to abuse themselves, their siblings and other children, selling "box sets" of the abuse online, according to the National Crime Agency (NCA).

Elahi admitted 158 charges against 72 complainants, although the true number of victims is estimated to be nearer 2,000, with ages ranging from adult to children as young as eight months old.

In 2021 we found and effected the removal of 1,600 webpages featuring images of Elahi's victims. Throughout 2022 we continued searching and found a further **1,312** webpages containing images of the same eight victims known to us. This significant amount of child sexual abuse material relates to just a small proportion of the estimated number of victims in this case. We estimate there are likely thousands more images still to find.

Of those webpages we discovered in 2022:

- **Almost a third (31%) were graded Category A**, the most serious kind of child sexual abuse, depicting penetration, sadism or degradation. This illustrates the horrific nature of Elahi's crimes.
- **90% were images of girls**, and
- In seven out of 10 instances (70%) they were **images of children aged 16-17 years old**.

Challenges with verifying imagery of older teenagers:

The ages of older teens we see being abused online are often particularly difficult to determine without formal identification and age verification. Thanks to our partnership work with the National Crime Agency, we have the information we need to identify – with certainty – that the images we are finding are of child victims. It therefore enables us to take action on those images of young people that otherwise may not be identified as children.

Due to how we see child sexual abuse imagery being repeatedly shared online, we believe that we'll keep finding images of Elahi's victims for years to come.

While the successful conviction of Abdul Elahi is good news, sadly his arrest in 2018 wasn't the end of the abuse for his victims. Those he targeted still suffer as their images continue to be circulated online and this repeated trauma can be devastating and long lasting.

This case highlights the importance and the positive impact of our work in helping to end this revictimisation cycle by removing this imagery from the internet and providing hashes (digital fingerprints) to our Members to prevent it from circulating further.

Category A child sexual abuse material of a ‘self-generated’ nature

an IWF snapshot study

Preface

In her final report in the Independent Inquiry into Child Sexual Abuse (IICSA), Professor Alexis Jay OBE, the inquiry’s chair, calls for plain and clear language to be used when talking about child sexual abuse. She said in her opening statement to the final report:

“We also need to use the correct words to describe the actions of abusers – masturbation, anal and oral rape, penetration by objects – these words are still not considered acceptable terms by many in public and private discourse. Every incident of abuse is a crime and should not be minimised or dismissed as anything less, or downplayed because descriptions of the abuse might cause offence.”

She is right. And it is thanks to her remarks that IWF has decided to make this data publicly available, and to describe what we’re seeing as accurately as we can.

If we cannot be brave enough to use the right words to describe the true horror of what children are coerced to do, how can we expect children to be brave enough to use the right words and to talk to trusted adults about what is happening to them online?

Background

The IWF has been tracking an increase in ‘self-generated’ data of 7- to 10-year-old children. We’ve also published data over many years relating to an increase in the amount of ‘self-generated’ child sexual abuse material in the form of studies, and the 2021 IWF annual report.

We assess child sexual abuse material according to the levels detailed in the **Sentencing Council’s Sexual Offences Definitive Guideline**. The

Indecent Photographs of Children section (Page 34) outlines the different categories of child sexual abuse material.

- **Category A** is defined as: 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.

In the spring of 2022, an IWF analyst assessed a video of a young girl who was around seven or eight years old. She had been recorded while playing with her doll and lying on her bed. An online abuser appeared to instruct her to do a multitude of inappropriate acts, including penetrating herself and masturbating with the handle of a large sharp knife. Even to our analysts, whose resilience to this material is high, it was viewed as a truly horrific crime. This, coupled with questions to IWF about how a child, on their own (in most cases), could be seen in 'penetrative sexual activity', led to this study.

When a child is engaged in any type of sexual activity either alone or with a perceived peer on webcam, it could be understood that this is due to sexual exploration, however this is not reflective of what our analysts see in their work.

Methodology

Data were collected between 16 and 22 June 2022 – five working days.

We collated all the Category A child sexual abuse images and videos which fitted the 'self-generated' definition. This is child sexual abuse content created using webcams or smartphones and then shared online via a growing number of platforms. In some cases, children are groomed, deceived or extorted into producing and sharing a sexual image or video of themselves by someone who is not physically present in the room with the child.

Category A images involve one or more of the following aspects:

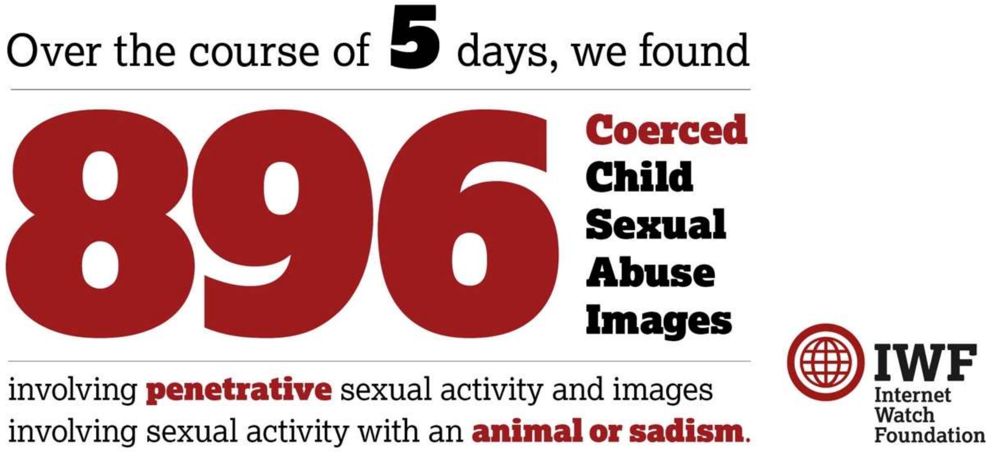
1. Penetrative sexual activity;
2. Images involving sexual activity with an animal, or
3. Sadism.

Anything which fitted this definition, within the timeframe allocated, was included in the study.

While the term ‘self-generated’ indicates that the child is creating the content themselves, it is vital to remember that children are being groomed online and instructed to engage in this behaviour. No blame should be placed on the child.

Results

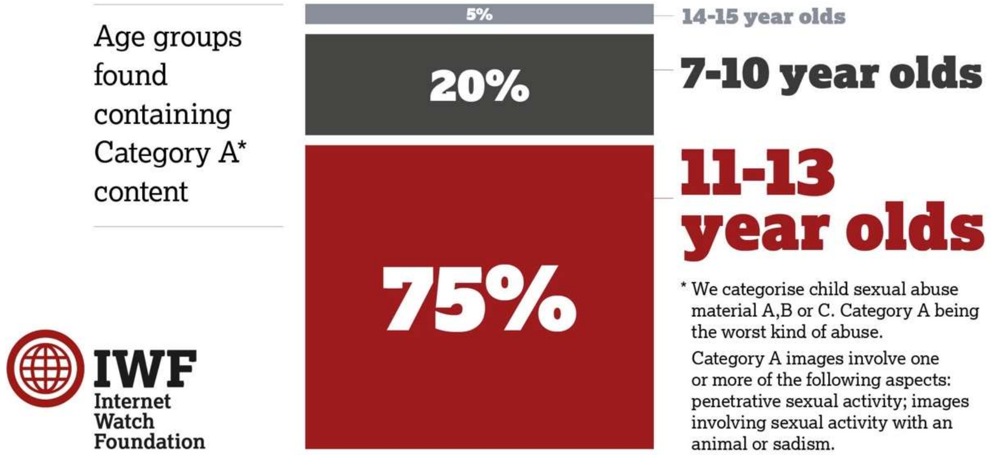
896 instances of online child sexual abuse images or videos were found containing Category A content of a ‘self-generated’ nature.



Over the course of **5** days, we found **896** **Coerced Child Sexual Abuse Images** involving **penetrative** sexual activity and images involving sexual activity with an **animal or sadism**.

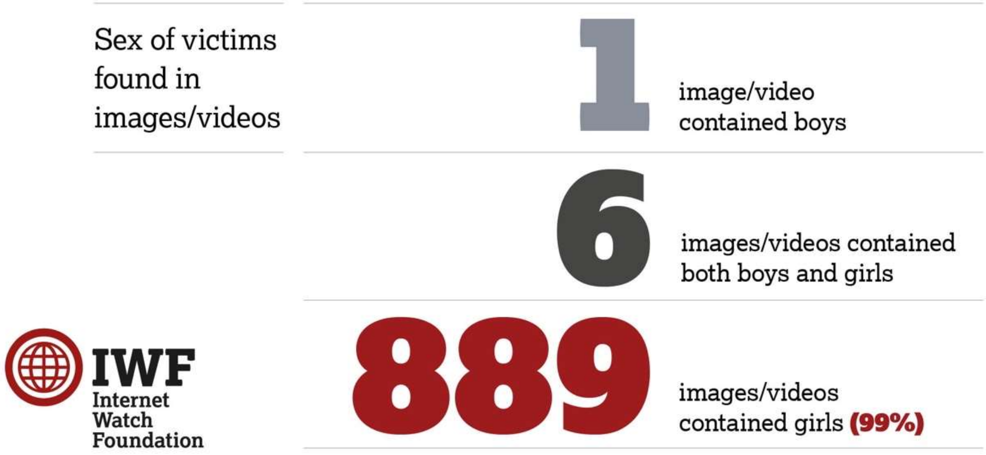
IWF
Internet
Watch
Foundation

- This averages as 179 Category A images a day.
- This equates to 25 Category A images every hour (over an analyst’s seven-hour working day).
- **668** of these images contained children aged 11 to 13 years old **(75%).**
- **184** of these images contained 7- to 10-year-olds **(20%).**
- **44** of these images contained 14- to 15-year-olds **(5%).**



* We categorise child sexual abuse material A,B or C. Category A being the worst kind of abuse.
Category A images involve one or more of the following aspects: penetrative sexual activity; images involving sexual activity with an animal or sadism.

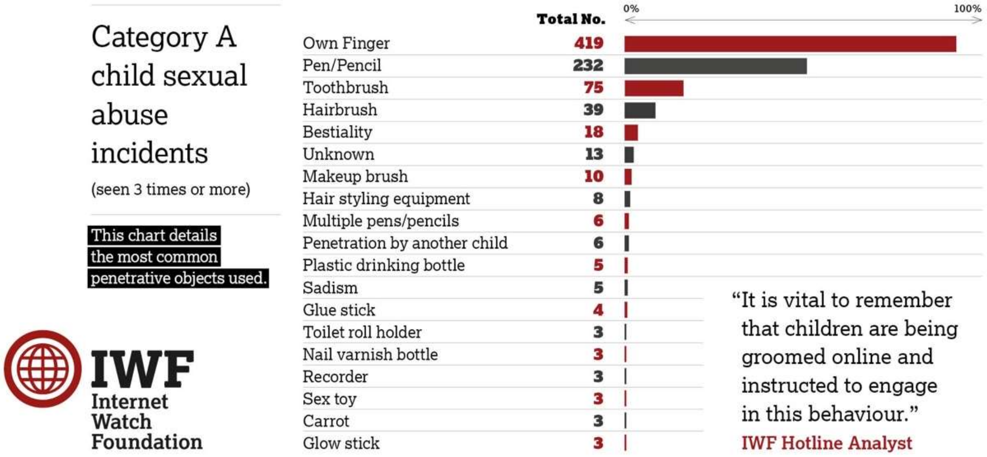
- **889** images/videos contained girls **(99%)**;
- **6** images/videos contained both boys and girls;
- **1** image/video contained boys.



Analysis of penetrative objects

Below is a breakdown of all the objects used for the act of penetration that were seen in the images and videos. The most common object was the child's own finger **(419)**, followed by a pen or pencil **(232)**, a toothbrush **(75)**, and a hairbrush **(39)**.

Below is a graph showing the most frequent objects/types of abuse that were seen three times or more.


Category A child sexual abuse incidents

(seen 3 times or more)

This chart details the most common penetrative objects used.

"It is vital to remember that children are being groomed online and instructed to engage in this behaviour."
IWF Hotline Analyst

The aim of gathering the data was to record the objects being used for penetration purposes by searching for Category A content. There are, however, more elements to Category A than just penetration, hence images involving bestiality and sadism were found.

Eighteen images accounted for bestiality (the child was involved in sexual activity with what appears to be the family pet). To be clear, in the images showing bestiality, there was no penetration seen. Animals were most often seen licking a child's genitals.

There were five images which contained sadistic content;

- Three images included pegs being used on the child's genitals and
- Two images showed the child drinking their own urine.

Other obscure objects found in the images included an egg whisk, a lint roller, and a USB cable. Additionally, penetration by another child was seen on six different occasions. There were unknown objects found in the images, which showed penetration taking place but were not clear enough to identify what the object was.

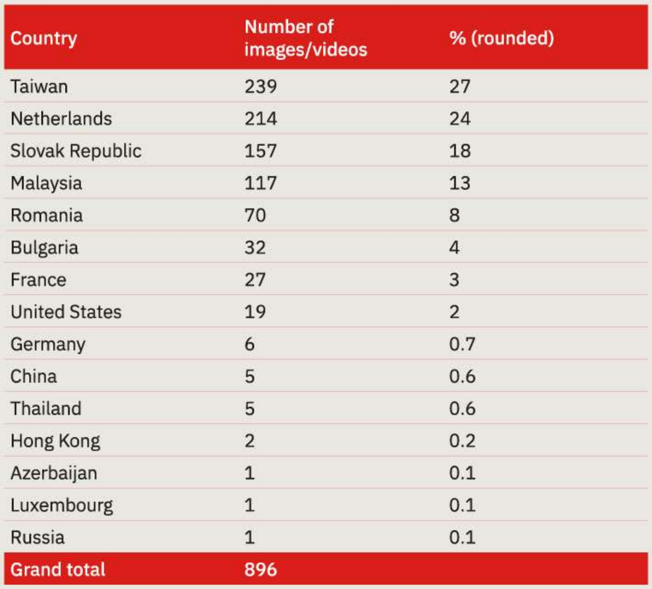
In total there were 69 different variables recorded. Please note there were not 69 different objects, but in some cases the child would use multiple objects within the same image set or video. Due to the way that child sexual abuse images are frequently uploaded and distributed to many locations online, some of the images in this data set will have been repeated. Images are frequently copied and re-posted again using a different URL.

Hosting analysis

When we’ve assessed that an image or video fails UK law, our aim is to get it removed from the internet as fast as possible.

To do this, we perform a trace on the content to identify the physical server that the content is hosted on. This tells us which partners in which country we need to work with. When the content is removed from the physical server – its source – then we can be sure that the image has been removed from any websites or forums, or image boards etc, that could be linking to it.

The table below shows the countries in which the imagery was hosted. To be clear, this does not tell us which country the victim(s) or offender(s) were in, nor from which country the content was uploaded online.



Country	Number of images/videos	% (rounded)
Taiwan	239	27
Netherlands	214	24
Slovak Republic	157	18
Malaysia	117	13
Romania	70	8
Bulgaria	32	4
France	27	3
United States	19	2
Germany	6	0.7
China	5	0.6
Thailand	5	0.6
Hong Kong	2	0.2
Azerbaijan	1	0.1
Luxembourg	1	0.1
Russia	1	0.1
Grand total	896	

Source: IWF Annual Report 2022

Real life example

This is a typed extract of a video found in the data. It involves a young girl being directed on webcam.

From her bedroom, a young British girl addresses her watchers and asks them to put any questions they might have in the chat below. She apologises for having to move to a different platform, but she was banned before. She tells the viewers she does not like to use Snapchat as her friends are on there. She is asked her age several times throughout the video and states that she is 14 years old, however looks around 12/13 years old.

Somebody asks her to show her feet and asks her if she can wear white socks, she says, **“You have a foot fetish?”** and giggles. Somebody tells her she is **“Really pretty and hot”** and she responds with **“Thank you”**.

She is asked to show her genitals on camera: **“Release your p***y”**.

They ask her to follow them back and she replies, **“I’ll follow you all back after the live stream. What do you want me to do?”** she asks then pauses to read their responses and tells them she needs to close the curtains. She is asked to show her naked body and she takes her shorts and underwear off.

“What else?” she asks, and then bends over and shows her genitals. She says, **“Is that better?”** and pulls the camera close to her genitals and masturbates and penetrates herself with her finger as instructed. She dances, exposes herself, masturbates and penetrates herself for several more minutes and then asks, “What would you like me to do?” and she penetrates her anus with her finger.

“Are you ready for the final piece?” she asks and shows her breasts while dancing and touching herself. After a while she says she must get changed but has a pair of dirty knickers and shows them to the camera. She says, **“Try and get this up to 5k”** and points to the bottom of the screen.

“I’m 14” she says again, **“Sorry I’ve got to go”** but says she would stay if she can get 5,000 viewers. She draws the livestream to a close by saying **“Don’t**

forget to send, but I won't be sending back as I do it on livestream." She ends the video by thanking her viewers for joining.

The above video is a common example of what the analysts find regularly. The primary concern for this girl is the number of viewers she has and wishes to have. We can only assume that the child has been groomed into behaving this way. Indeed, the text suggests this is not her first time, but rather a common occurrence. It was not revealed in the video how many viewers she had; her target was 5,000 people which is a large number of people to be viewing child sexual abuse material and furthermore be actively asking the child to carry out these acts on camera. Ultimately this girl is being instructed to behave this way and for one purpose – the viewers' sexual gratification.

Summary

This snapshot study was carried out to record the objects that we saw children use for penetration purposes when streaming online with an abuser. It is not uncommon for IWF analysts to encounter this type of child sexual abuse. It is the first time, however, that we have published this sort of detail about penetrative sexual activity. We hope that this helps to inform others' work: that of other hotlines, policy makers, technology companies, and law enforcement and our partners in the third sector who work tirelessly to protect children online.

Numerous objects were recorded, the most common being the child's own finger. It could be argued that this behaviour is part of the maturation process to explore sexuality.

However, this is certainly not always the case, especially given that 184 images included 7 to 10 year olds. Furthermore, the video transcript shows that the child was doing this for followers, perhaps likes or incentives. When only a child/children can be seen in the content, it can be easy to forget that there is always someone watching on the other end and often instructing children to carry out these acts.

Tech R&D

Harnessing innovative tech to advance our mission

2022 was a tumultuous year for the internet, one that showed how the IWF's mission to see an internet free of child sexual abuse is never more important.

Developments such as the metaverse, rapid growth in cryptocurrencies and decentralisation, greater levels of encryption, and ongoing efforts around the world to introduce regulations to combat online harms, have resulted in a constantly evolving and shifting landscape.

We have seen exciting new developments in online safety to detect and prevent abuse at scale, such as new machine learning tools and privacy preserving filtering tools, but also worrying trends and technologies which have the potential to create new harms and put more children at risk.

As the scale of the problem continues to grow, the IWF technology team has developed new tools to enable our expert human analysts to find and assess more content with greater accuracy than ever before, including leveraging GPU-accelerated (Graphics Processing Unit) computer vision techniques to cluster near duplicate images, web processing tools which can instantly highlight known child abuse images as soon as they appear on the page, and to detect and split the individual frames used to make collages or grid images.

In addition to supporting the core work of our Hotline, the tech team have also been working with IWF Members on bespoke projects to develop and test new innovative technology, leveraging the IWF's unique expertise with child sexual abuse content and rich tagged datasets.

The team has worked on and supported incredible developments such as the IWF reThink Chatbot, the SafetoWatch image classifier, and the privacy preserving Cyacomb safety tool, solutions which are pushing the boundaries of what technology can do to detect and disrupt the distribution and access of child sexual abuse material online.

IWF CAID Taskforce

Home Office THORN

We're collaborating with the UK Government's Child Abuse Image Database – CAID – to support law enforcement and help the tech sector find and remove copies of known child sexual abuse images online.

IWF is the only non-law enforcement body in the world with access to the Child Abuse Image Database (CAID) as part of a collaboration to support law enforcement, and stop the upload, sharing and storage of known child sexual abuse images online.

This work, in turn, benefits sexually abused children all over the world.
In 2022, our six highly trained graders were increased to 14, plus two quality assurance staff. They have assessed, graded and hashed nearly two million images from the database.

When we hash an image, we create a 'digital fingerprint'. As standard, we hash all images using multiple algorithms, and due to our ability to store the imagery, we can retroactively add new algorithms as they are developed, keeping pace with the technology as it advances.

We take pride in the quality of our work and the expertise of our staff. And we've gone over and above in the grading of these images so that we're enriching each image and hash with additional metadata.

This means we're tagging the image with extra descriptions such as the estimated age of the victim and the type of sexual abuse that was taking place. By tagging them with this extra information, it makes them compatible with other legal jurisdictions around the globe, which is additionally uploaded back into CAID. By doing this work, it also makes it easier for technology companies to deploy these hashes through their services in different territories. This work means we have more chance of copies of that image being found and removed, and that image getting stopped from being uploaded, downloaded, or shared in the first place.

As a result, we're supporting the efforts of law enforcement in the UK, and global industry can better protect their customers, and better protect children whose abuse images are shared online. This gives peace of mind to victims who often live with the knowledge that footage of their abuse could be shared by criminals around the world.

This work has been funded by Thorn and the UK Government's Home Office and started in 2020.

It was made technically possible by building IntelliGrade. The capabilities of IntelliGrade, alongside our training, allows us to make sure that the quality of our assessments is the focus of our work.

Using IntelliGrade means that we can create hashes of more victims' images than ever before; not only assessing images from CAID, but also wherever the IWF analysts find a criminal image, either through responding to public reports or our proactive work.

Nominet Fund for Countering Online Harm

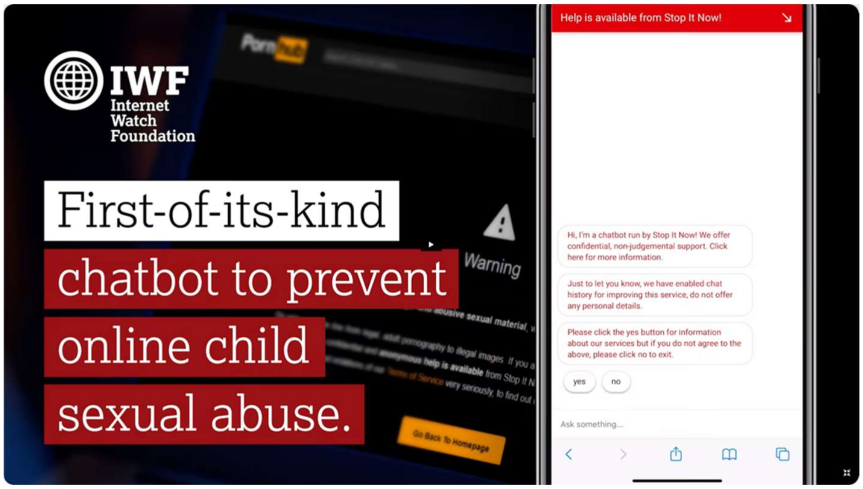
NOMINET

Nominet, the official registry for UK domain names, started the Countering Online Harm Fund in December 2019 to offer child protection networks additional resources to respond to ever-changing threats to children online. Nominet's partnership with the IWF has enabled our tech team to grow and take risks, going beyond day-to-day operations to be truly innovative in our mission to develop technology for good.

The fund has enabled us to create and expand a dedicated software engineering team and to invest in infrastructure to scale up bespoke tools developed in-house to find, assess, and remove child sexual abuse material online.

The team at Nominet share IWF's mission to see a safer internet for all, free of child sexual abuse material. The partnership has had a transformative effect on our ability to develop technology that enhances our work, increasing impact and helping to counter online harm through the removal of child sexual abuse material from the internet.

ReThink Chatbot



Hi, I'm a chatbot run by Stop It Now! We offer confidential, non-judgemental support. Click here for more information.

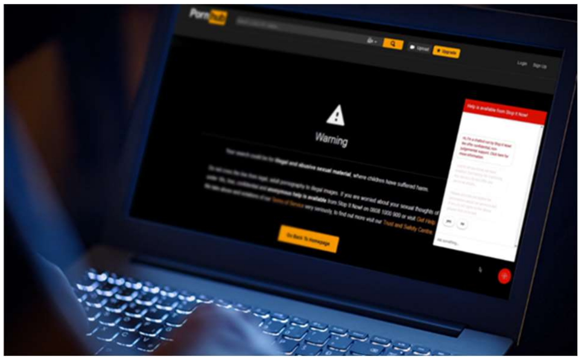
Just to let you know, we have enabled chat history for improving this service, do not offer any personal details.

Please click the yes button for information about our services but if you do not agree to the above, please click no to exit.

In partnership with Stop It Now! UK and Ireland, we developed a chatbot to help deter potential offenders from searching for child sexual abuse material and divert them to sources of support to change their behaviour. The project has been funded by the Safe Online Initiative at End Violence.

It targets internet users who show signs that they might be looking for images of child sexual abuse. Technology company MindGeek volunteered to pilot the chatbot on the Pornhub UK platform as part of its trust and safety protocol, which also includes content moderation programmes and non-profit partnerships.

The chatbot was launched in March and the project will be evaluated by Associate Professor Jeremy Pritchard and Dr Joel Scanlan from the University of Tasmania. The evaluation is funded by Childhood Foundation and the Safe Online Initiative at End Violence and is expected to finish late 2023.



This is the first project of its kind to use chatbot technology to intervene when people attempt to search for sexual images of children and try to help them stop, or not start, offending.

Getting to grips with grid images

By Chris Wilson, IWF Head of Software Development

We've deliberately scaled up our tech team to enhance the efforts of analysts in our Hotline.

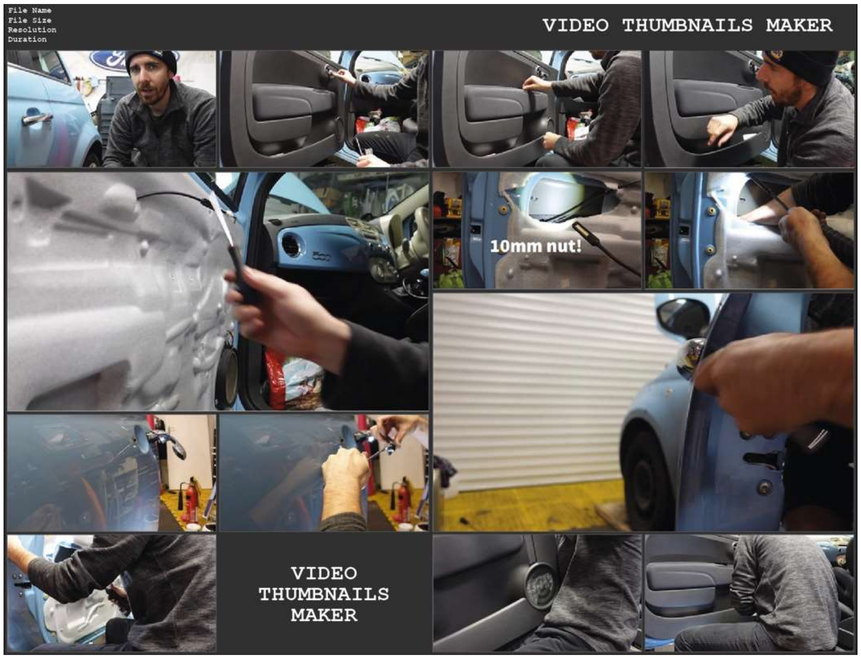
One of our challenges we're tackling is around the recurring issue of 'grid images' in the hashing process. This process creates hashes, or digital fingerprints, of child sexual abuse images and videos that can be used to identify and block the images online.

Grid images, however, are notorious for causing perceptual hash collisions, which means that the perceptual hashes from grids will sometimes match images of simple repeating patterns.

A grid is a particular type of preview image used by offenders to advertise and make money from selling child sexual abuse videos online. Offenders create the grid images from video frames of the criminal content and post them on the internet along with a link to entice buyers to a premium file sharing service. These services require a subscription for users to access and download the full video.

You can read more about commercial child sexual abuse imagery here.
Grids can constitute up to 40% of the images we process in reports at any given point in time. But most of the tech companies who use our data to block

child sexual abuse imagery exclude grid image hashes from searches because of the chance that they might clash with another image.



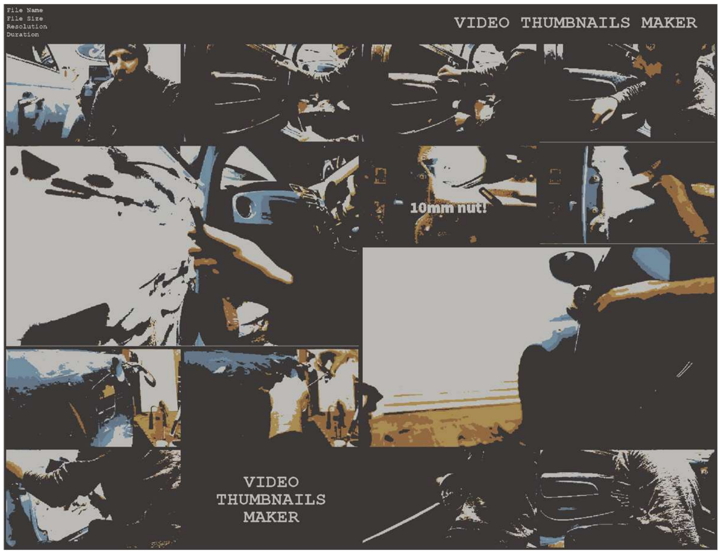
The work in progress

While there is no standard layout, background colour, sub-image size or software used to generate grids, we established that collisions are more likely to occur when a 7×7 grid or higher of sub-images is used.

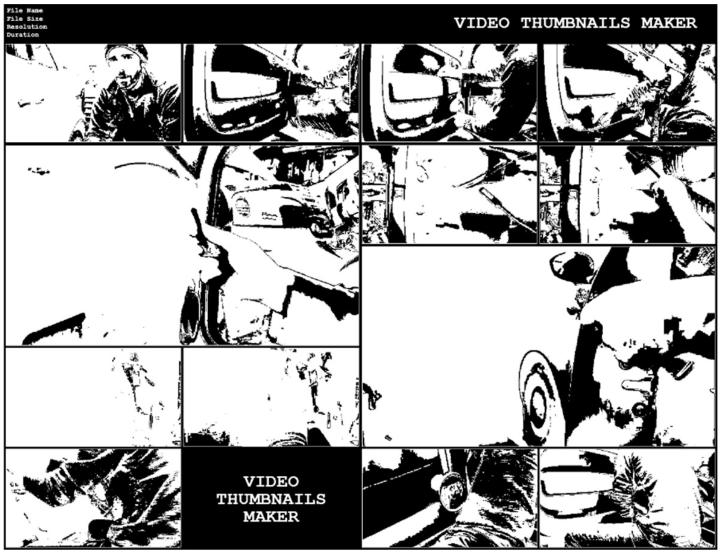
To handle grids in an automated fashion, we created a process that can detect the background and separate the images back into the constituent frames from the video for perceptual hash matching and clustering.

Our testing on synthetic grids and real-world child sexual abuse material has shown this approach to be 95% effective with a 0.2% false positive rate, which is when an image is flagged as matching a grid and extracted erroneously. The software we have developed so far is too slow to be useful in real-time detection for external tech organisations, but it is suitable for IWF purposes, and we are working with partners internationally to optimise the code.

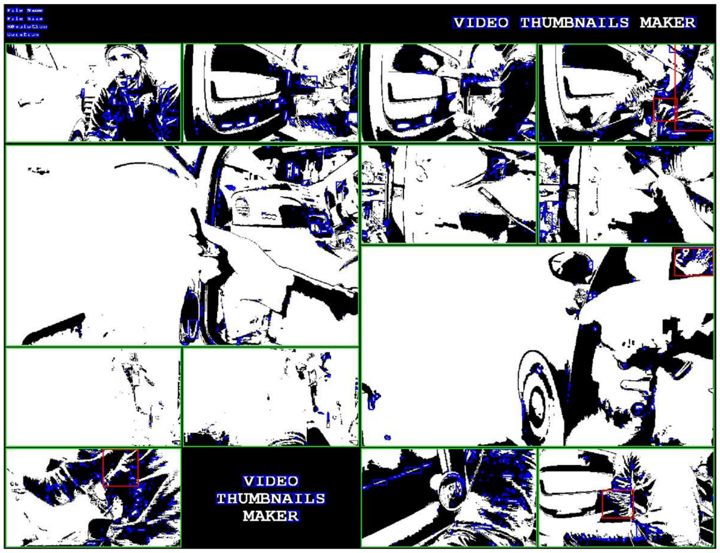
In brief we:



- Apply a quantization filter to restore a uniform background – removing JPEG compression artefacts – and simplify the image.
- Scan the image for any uninterrupted solid background colours that touch all four edges.



- Use the identified background colour to generate a binary image as a foreground mask.



- Apply blob detection to find the sub-images, subject to some edge case filtering

A potential game changer

This means we can now:

1. Associate grid images with the source child sexual abuse video if we've already assessed it, restoring context to some images which may not otherwise have evidently been criminal content from the grid preview alone.
2. Automatically detect and exclude grids in their raw form from perceptual hash matching and clustering to prevent collisions.
3. Add the sub-image perceptual hashes to our data sets which would match the frames of the source videos on platforms that implement scanning on videos and enable the detection of a known video of child sexual abuse even where we don't have the video itself.

Impact on clustering

For a similar area of our work, we use DBSCAN clustering with Photo DNA hashes to group very similar images together. This increases our ability to assess very visually similar images, such as simple resizes, and to improve consistency with our assessment process as we can compare assessments made by different analysts for slightly altered copies of the same images. We found assessments based on clusters to be 112% faster than assessing individual images.

Grid images come into play for clustering when it comes to videos. The standard Photo DNA process for videos is to first extract the frames. These can then be assessed as images. The video receives its overall assessment rating based upon the “highest category” assessment of any of the constituent frames. This way the video itself can be graded for the severity of the child sexual abuse it contains. We also account for any frames extracted and circulated individually.

The frames from any given video would form into a Photo DNA cluster much in the same way as copies of the same image would because each frame will be very similar to the next and previous frames. In the case of grids, this means that the extracted sub-images from a grid would merge into the cluster for the source video (if we have it to match against), which can provide vital context for us when assessing images.

For example, the sub-images of a grid may not be obvious child sexual material because the image does not contain enough of the victim to be sure, but when it merges into the existing cluster, the analysts can then see where the grid came from, and the images before and after it in the video, which can often confirm one way or another whether the image is of a child or not.

Why is this important?

This makes our work faster, more accurate, and closes the loopholes which criminals have tried to exploit in their making and sharing of child sexual abuse images and videos.

Machine learning with SafeToNet

SafeToNet
Incorporating Net Nanny

We’ve been working with safety tech company SafeToNet to develop a new online child safety solution which will use machine learning to recognise child sexual abuse material and stop it being sent to, or created by, mobile devices. The solution, called SafeToWatch, will detect threats in real time, block harmful content or switch off the camera on a child’s phone if they are viewing inappropriate material or tricked into taking sexual imagery of themselves by an online predator.

In 2022, 78% of the websites we removed contained images or videos where children had been groomed and coerced into sexual activities over an internet-enabled device with a camera by an abuser.

We hope this new technology will help prevent children from being targeted in this way by criminals.

Our tech team helped train SafeToWatch, using known child sexual abuse material assessed by our experienced IWF analysts, to teach it what child sexual abuse material is and how to detect it, and then rigorously tested it. SafeToWatch can sit on the device itself and will work, even in end-to-end encrypted platforms, to help keep children safe. It is also being developed to be integrated on platforms themselves and could be an important child safety solution as more platforms fully encrypt their services.

> “It is prevention at the point of creation or distribution. We are unique in that we are focusing on a preventative solution rather than a reporting tool. The reason we wanted to work with the IWF is because we believe they have the best and richest data worldwide. It is well labelled and lends itself to helping with this kind of work.”
>
> Tom Farrell, Chief Operating Officer at SafeToNet.

Our role in the Safety Tech Challenge

As more digital platforms look to fully encrypt their messaging services, efforts to disrupt and prevent the spread of child sexual abuse material online could be hampered, helping criminals evade detection.

This is why we partnered with digital forensics company Cyacomb for the Safety Tech Challenge, a UK Government-funded initiative to develop innovative tech solutions for detecting child sexual abuse content in end-to-end encrypted environments, while ensuring that users' privacy is respected.

Through our collaboration with Cyacomb, we've helped to create a tool that could block images and videos of children suffering sexual abuse from being uploaded into end-to-end encrypted platforms, where it would be impossible to trace them.

This has shown that a technical solution to the challenge posed by end-to-end encryption is possible and would help in preventing the spread of known criminal content.

We tested the solution in an enclosed environment to simulate how the tool would detect real child sexual abuse content in a private messaging platform.

While it is not possible to scan inside an end-to-end encrypted environment, it is possible to stop known child sexual abuse content from being uploaded into an end-to-end environment before it is transmitted, distributed, and shared.

This tool has potential; however, it needs to be used in conjunction with other measures to make sure children are fully protected.

Ian Stevenson, Cyacomb CEO said: "We were privileged to collaborate with IWF on the UK Government Safety Tech Challenge Fund exploring potential solutions for detecting and blocking child sexual abuse material in end-to-end encrypted messaging environments.

"The IWF provided deep understanding of the problem to be solved, the challenges in doing so, and was able to provide practical testing in appropriately secure and controlled environments. We learned a huge amount from this collaboration, and IWF testing contributed to confidence that the technologies under development were effective.

"We hope this work will continue to develop to the point where it can deliver real impact in the fight against child sexual abuse imagery in messaging for IWF Members and more widely."

Our work with the adult sector

MindGeek

We're working on a two-year pilot project in partnership with MindGeek to develop a model of good practice to support the adult industry in combatting child sexual abuse material online.

MindGeek, a technology company, operates a number of brands which offer legal, adult-themed content to a global audience. They have implemented a number of trust and safety measures to keep their platforms and users safe and prevent the upload/re-upload of illegal material. These include mandatory identification for content creators, hash-list scanning, AI tools, human moderation, deterrence messaging, a trusted flagger programme and user reporting options.

During the two-year project, MindGeek will supplement its existing trust and safety programme by taking and deploying all relevant IWF services across its platforms including the URL List, Hash List, Non-photographic Imagery List and Keywords List.

The partnership began in November and is being overseen by an external advisory board of experts who will guide the outputs of the partnership.

The partnership aims to:

- Develop a model of good practice to guide the adult industry in combatting child sexual abuse imagery online;
- Evaluate the effectiveness of IWF services when deployed across MindGeek's brands;
- Combine technical and engineering expertise to scope and develop solutions which will assist with the detection, disruption and removal of child sexual abuse material online.

The project's progress will be reviewed at set intervals and reported into the IWF Board. Key learnings from the project will be shared publicly to support others' work in this area.

Welfare

Welfare at IWF

By Heidi Kempster, Deputy CEO and Chief Operating Officer

The IWF has grown more in 2022 than at any time in our 26-year history. At the beginning of the year, we embarked on our biggest recruitment drive yet, with appointments to new roles across our organisation. We have grown, from January 2022, to 70 by the end of December.

Given the sensitive nature of the work we do at IWF, that kind of expansion was no mean feat. We need to ensure that we recruit carefully, with people who have both a high emotional resilience and a passion for our mission. And following our response to Covid, where we split our workforce between those who work in the office and those who can work remotely, we had additional challenges to maintain that sense of unity. We've needed to re-think how we create that feeling and culture of one "IWF family".

When we speak publicly about our work, we often get asked about the welfare provisions for our staff, how we recruit the right people, and how we manage to maintain such high staff retention. We've taken a deeper dive into these issues in this annual report, by featuring the views of our new Head of HR, one of our Senior Analysts who supports staff wellbeing, and our professional mental health support team.

We work hard as a team to ensure that those who dedicate their working lives to our mission are, in turn, looked after. At the end of 2022 we welcomed four independent experts who carried out our Hotline Audit, which had been delayed by a year due to the Covid pandemic.

As part of this audit, Dr Georgina Clifford, Specialist Clinical and Research Psychologist and Director of London Trauma Specialists, inspected our welfare provision. The independent auditors found our Gold-standard welfare programme to be an: *"excellent, carefully considered and ever-evolving welfare package...[with] a trauma-informed approach to assessing the suitability of new staff for the role, with a comprehensive and rigorous interview and induction process."*

What welfare means to me

Lillian is a Quality Assurance Officer at the IWF, having worked in our Hotline for 13 years, finding and assessing child sexual abuse images. She takes a lead in helping to support the welfare of others. Here's Lillian's view of what welfare means to her.

"People often assume that something bad must happen to you for your mental health to be compromised, but it can also be the small things that grind away at you over time, like a busy lifestyle, a dark dingy day, a hideous commute to the office, working conditions that are not fit for purpose and many people suffer with loneliness when working from home.

This is why the IWF prides itself on providing an excellent welfare system to support staff wherever possible. Good mental health is of utmost importance when working for an organisation which deals with the subject matter of child sexual abuse material.

There are many roles at the IWF, some people assess images and videos of children's sexual abuse as part of their job and some work in other areas of the organisation, which means they are working from home or hybrid working; all roles present their own challenges and stresses.

I joined the IWF Mental Health Working Group in the peak of Covid.
We focus on promoting mental wellbeing and improving staff happiness.

We take a sensitive approach, factoring in the different needs of all IWF employees.

Every month I send out a welfare email to the whole organisation. I search for tips on managing mental health. Every email has a theme dependent on what's going on at that time. It might be work-related, for example a hectic time when we are working towards meeting a target, or it could be down to external factors, like the winter blues.

I spend a lot of time listening to Ted Talks looking for the right one which coincides with the mental health tips I want to give. Ted Talks are motivational and can be very thought-provoking.

I also believe the benefits of meditation are boundless. There are so many different forms of meditation/mindfulness. While some are uplifting and active, others are centred around winding down and relaxing. Everybody is different and mood is transient, so one type of therapy does not suit all. I include links to a variety of wellness approaches from our wellness employee benefit platform, so staff can choose which method works for them.

My welfare email may be as simple as providing a break and a distraction from the everyday, but the overall purpose is to give my colleagues a range of psychological tools that they can draw from, as and when they need them. Like our physical health, mental health requires maintenance. The truth about mental health is that it varies from one day to the next, and I'm proud to play my part supporting others at IWF."

Professional mental health support

We give our staff the support they need to do their job well

Our analysts have one of the toughest jobs in the world. Every day, staff in our Hotline see distressing images and videos of children being sexually abused, raped and tortured.

Ongoing exposure to this type of imagery can take a toll on an analyst's wellbeing. However, staff at the IWF consistently point to the strong welfare system in place that helps them to cope with the nature of their work.

It starts with the recruitment process

The IWF's rigorous support system begins as soon as candidates are selected for interview and continues throughout their time at the charity. Recruitment and training are carefully managed to guide potential and new analysts through the process of viewing graphic and upsetting images.

This strong start reinforces a wider organisational strategy ensuring that there is a support network every step of the way to help them maintain good mental wellbeing.

Our analysts come from all walks of life, ages and experiences, yet they all speak of a sense of shared camaraderie and understanding in the Hotline. They know that they will always be able to speak to a colleague or line manager about their work and it is encouraged that staff recognise and voice that they might not be able to cope as well as they'd like with something they have viewed.

Regular breaks, and no overtime

It is vital to our analysts' wellbeing that they can 'close the door' on what they have seen during the day and leave work behind when they go home. For this reason, staff in the Hotline work a shortened day to keep the amount of time viewing images to a minimum. Regular breaks are mandatory and there is no overtime, ever.

During lunch and time away from their screens, analysts are encouraged to relax and eat in a bright and cheerful communal space or if they're feeling energetic, play a game of table tennis. There are also jigsaws, colouring books, building sets and juggling balls available for other mindful distractions. Further support is provided by an in-house welfare working group that meets regularly to discuss aspects of staff welfare across the organisation and provides team-building sessions to maintain morale.

Mandatory counselling, every month, without fail

On occasion however, viewing a particular image or video can have an emotional effect on an analyst and stay with them beyond their working day. This is why all employees who view criminal images have in-person, mandated monthly counselling sessions with a licensed therapist.

These sessions gently explore how the analyst is dealing with their exposure to child sexual abuse material and whether it may be affecting their home life. Sometimes an analyst will describe viewing an image that is 'triggering' and which they're finding difficult to stop thinking about. It could be something as innocuous as a recognisable toy or piece of clothing or something more upsetting that can be heard on the audio track of a sexual abuse video.

In these cases, the therapist can work with the analyst to try and dispel the impact that the image has; to take away its power to shock. These include techniques such as imagining the image painted on a wall and then manipulating it. The analyst is encouraged to paint over the image or break down the wall in their minds, mentally blocking or throwing it away.

An annual visit to "The Prof"

The monthly sessions are backed up by an annual assessment with a clinical psychologist, affectionately called 'The Prof'. His work with the IWF differs from his usual sessions in that instead of helping people to deal with the aftermath of a crisis or trauma, it is specifically designed to prevent crisis and trauma from occurring.

He says that to do their jobs effectively, analysts need to become desensitised to some degree. While the content they view remains shocking, because of the analyst’s training and experience the images no longer have the same sort of ability to shock that they might have had for someone who was ill prepared to see them.

Analysts are taught to try not to ‘fill in the gaps’ when viewing images of children being hurt and exploited, which means to avoid thinking about what might have happened to a child and whether they are still at risk. Though it is a natural thing to wonder about, our analysts learn to distance themselves from the emotional aspect so they can focus on the job at hand.

The IWF mission as motivation

Analysts know that the vital data collected through their assessment of child sexual abuse images is used by law enforcement and the tech industry around the world to track down child abusers and block further distribution of abuse material. This gives our Hotline staff great satisfaction knowing that they have made a difference to help children.

As one analyst says: “I’m glad we do see what we do if it protects children.”

Providing support across the organisation

By Samantha O’Byrne, IWF Head of Human Resources

> “Our welfare considerations have focused on creating a culture where everyone feels thought of, valued and united, whether working together in the office or remotely.”

Our staff team at the IWF has grown rapidly over the past two years and we now employ about 70 people who are based across the UK and Brussels. Half of the team work together every day as one unit in our Cambridge Hotline, where they assess child sexual abuse images. The other half work predominantly from home but come together regularly for individual team gatherings, meetings at the office or company-led events.

Our welfare considerations have focused on creating a culture where everyone feels thought of, valued and united, whether working together in the office or remotely. Ensuring that everyone has the right tools to be effective and feel connected has been vital in this process.

We have an exceptional welfare programme in place to support our Hotline, which is scrutinised and endorsed by external subject matter experts, including a high court judge, a clinical psychologist and law enforcement. Culturally, we work hard to ensure we bring people together often, making them feel connected and ensuring they have an equal voice. We hold routine, organisation-wide online meetings, run an employee-led staff forum, take regular surveys to seek employee opinion and give people responsible roles on the welfare group and environmental team.

Our groups and meetings combine office-based and home workers to give a rounded view across the organisation. This helps to foster collaboration and develop strong relationships among colleagues, wherever they are in the country.

However much we have grown, we strive for equity across the organisation wherever possible, for example offering welfare perks that suit both those at home and in the office. We know that needs differ across individual teams and we meet those differences when we can, yet we always prioritise a consistent and balanced approach to staff welfare.

Hotline audit

We welcomed four independent inspectors into IWF at the request of our Board. Led by retired High Court Judge Sir Mark Hedley, they were asked to:

- Comment on whether the Hotline and Administrators' Manuals are fit for purpose and whether the procedures are complied with by staff.
- Quality check active child sexual abuse URLs and hash images for consistency of decision-making and managerial oversight.
- Sample previous child sexual abuse content screen captures for consistency of decision-making and managerial control mechanisms.
- Review and comment on administration in discharging content assessment complaints.
- Consider Internet Content Analysts' training requirements to enable them to undertake their roles confidently and accurately.
- Sample work of the Quality Assurance team to ensure adequate, objective and representative testing and reporting mechanisms.
- Review Hotline security arrangements and conformance with ISO/IEC 27001.
- Review and comment on Hotline welfare arrangements including recruitment processes, counselling arrangements and general support mechanisms comparing with other models of good practice in law enforcement and other professions.

They concluded that:

> "The IWF is an extremely professional and well-managed organisation led by a strong but caring and compassionate leadership team. The mission is clearly understood by all staff members who are committed to protecting children from the serious harms that can be inflicted by the perpetrators of online child sexual abuse."
>
> Keith Niven QPM, National CAID IT Implementation Lead, Norfolk Constabulary.

The full report is published on the IWF website.

Policy

Policy in UK

Online Safety Bill

In March 2022, the UK Government presented its much-anticipated Online Safety Bill to be read in the House of Commons. This was the culmination of almost six years' worth of pre-legislative consultation in the preparation of the Bill. The IWF continued to influence and follow the Bill throughout its passage in Parliament.

Second reading, 19 April 2022

At a heavily curtailed debate on the Bill's Second Reading, the former Chair of the Digital, Culture, Media and Sport (DCMS) Select Committee, Julian Knight MP, called for the IWF to have a role in assisting Ofcom to identify companies who were failing in their duty of care.

Former Digital Minister Dame Caroline Dinenage MP also referenced the harm caused to children and how the IWF and partners blocked 8.8 million attempts in one month to access known child sexual abuse material. Read our briefing note.

Video clip of former Minister of State for Digital and Culture Dame Caroline Dinenage MP speaking at the Second Reading of the Online Safety Bill in Parliament on 19 April 2022

Video clip of the former Chair of DCMS Select Committee, Julian Knight MP, speaking at the Second Reading of the Online Safety Bill in Parliament on 19 April 2022

Public Bill Committee, 24 May 2022

The Bill entered its Public Bill Committee stage for the first time in May. The Committee, Chaired by Sir Roger Gale MP and Christina Rees MP, used its first session to hear from a wide range of stakeholders, including IWF CEO Susie Hargreaves OBE, on various aspects of the Bill before considering line by line scrutiny of the Bill.

Topics of discussion at the Public Bill Committee evidence session included categorisation of companies as part of the Bill, end-to-end encryption, grooming, co-designation of expert bodies and media literacy. Read our evidence to the Public Bill Committee.

Video clip of IWF CEO Susie Hargreaves OBE giving evidence to the Public Bill Committee on 24 May 2022

Video clip of IWF CEO Susie Hargreaves OBE giving evidence to the Public Bill Committee on 24 May 2022

Report Stage, 12 July and 5 December 2022

The Bill had two days of Report Stage. The first on 12 July and the second, following two changes of Prime Minister, on 5 December.

Many of the amendments relating to child sexual exploitation and abuse were considered on 5 December, when several MPs stood up to raise concerns about the need for more detail on how the implementation of the legislation would work in practice.

Former Safeguarding Minister, Rachel Maclean MP, called for the IWF's technical expertise to be reflected in the new regulatory framework. Former Home Secretary Priti Patel MP pushed the Parliamentary Under Secretary of State, Paul Scully MP, to ensure he was aware of the IWF's expertise and that it would be reflected in the new framework. Several other Parliamentary Champions, including Sarah Champion MP, Miriam Cates MP and Vicky Ford MP, backed these calls.
Read our briefing note.

Video clip of former Home Secretary Rt Hon Priti Patel MP and the former Safeguarding Minister Rachel Maclean MP during Online Safety Bill Report Stage discussions in Parliament on 5 December 2022

Video clip of IWF Parliamentary Champion Miriam Cates MP during Online Safety Bill Report Stage discussions in Parliament on 5 December 2022

Video clip of IWF Parliamentary Champion Rt Hon Vicky Ford MP during Report Stage discussions in Parliament on 5 December 2022

Video clip of IWF Parliamentary Champion Sarah Champion MP during Report Stage discussions in Parliament on 5 December 2022

Safer Internet Day

IWF Champion Laura Trott MP chaired a virtual session for Members of Parliament and Peers to hear from three of Childnet's Digital Leaders as part of a discussion about the theme for Safer Internet Day 2022: 'All fun and games? Exploring respect and relationships online'.

Speaking in a debate on mental health in Parliament on the same day Laura Trott said:

> "Today, at an event involving the Internet Watch Foundation, I heard four teenagers talk about the pressures that they felt online, and how difficult they found to talk to people about what was happening and where to refer it. We must fix this, and I think the Online Safety Bill will be the key to that."

A screenshot shows IWF Champion Laura Trott MP chairing a virtual Safer Internet Day event with teenagers discussing the pressures that they felt online

Video clip of IWF Champion Laura Trott MP in Parliament on 8 February 2022 referring to the Safer Internet Day event she chaired

Independent Inquiry into Child Sexual Abuse

The Independent Inquiry into Child Sexual Abuse published its final report in October after nearly seven years of work, hearing from 7,300 victims and survivors and considering nearly 2.5million pages of evidence.

We were proud to play our part in the Inquiry which concluded that: “too often institutions prioritised their personal and institutional reputations above the welfare of those they were duty bound to protect.” The final report stated: “Children must be given a greater priority in public life.”

A month after the Inquiry concluded, we were pleased to add our name to a letter to the Prime Minister and Home Secretary calling on them to implement the recommendations in the report.

APPG On Social Media

This year, as part of the UK Safer Internet Centre, we continued to run the Secretariat for the All-Party Parliamentary Group (APPG) on Social Media. The APPG elected two new Co-Chairs in 2022, Labour MP Luke Pollard and Conservative MP Aaron Bell who took over from outgoing Chair Chris Elmore MP.

The APPG held two meetings this year related to the Online Safety Bill. The first considered child protection measures in the Bill where MPs and Peers heard from SWGfL, Barnardo’s and the IWF on how the Bill could be improved, with a response from then Digital Minister Chris Philp MP.

The second session considered changes the Government made to the Bill concerning the "legal but harmful provisions." Speakers included Will Perrin of the Carnegie Trust, Parliamentary Under-Secretary of State for Tech and the Digital Economy at DCMS Paul Scully MP and Labour Shadow Minister for Tech, Gambling and the Digital Economy Alex Davies-Jones MP.

November's APPG on Social Media included speakers Will Perrin of the Carnegie Trust, DCMS Parliamentary Under-Secretary of State Paul Scully MP and Labour Shadow Minister Alex Davies-Jones MP

November's APPG on Social Media included speakers Will Perrin of the Carnegie Trust, DCMS Parliamentary Under-Secretary of State Paul Scully MP and Labour Shadow Minister Alex Davies-Jones MP

Written evidence to Scottish Parliament Justice Committee

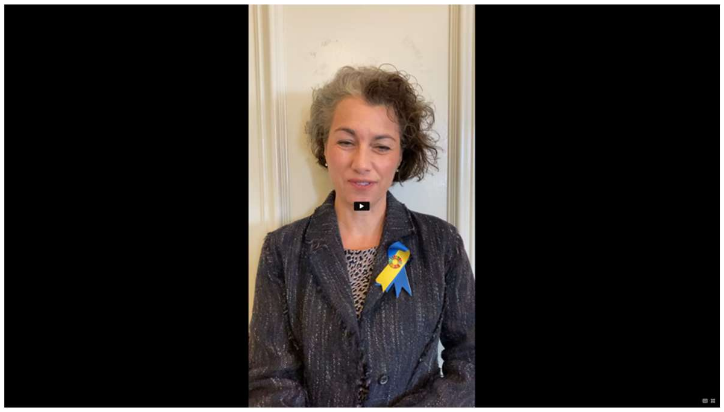
In May, the IWF was asked to give written evidence to the Scottish Parliament Justice Committee, for a one-off evidence session on online safety. We provided information on the scale and nature of the CSEA threat, CSEA definitions, education and awareness and the challenges we face. Read our written submission.

IWF's 25th anniversary

We celebrated our 25th anniversary at an event in the House of Lords, sponsored by Baroness Nicky Morgan of Cotes, with then Home Secretary Rt Hon Priti Patel MP speaking alongside Professor Hany Farid from the University of California, Berkeley, IWF Chair Andrew Puddephatt OBE and IWF CEO Susie Hargreaves OBE.

Other attendees at the event included Rt. Hon. Sir Jeremy Wright KC MP, Chair of the APPG on Digital Regulation; Damian Collins MP, Chair of the draft Online Safety Bill Joint Committee; Alex Davies-Jones MP, Shadow Minister for Tech, Gambling and the Digital Economy; Daniel Zeichner, Member of Parliament for Cambridge; Rt. Hon. Lord Tim Clement-Jones CBE FRSA, Lib Dem spokesperson in the House of Lords for the Digital Economy; Laura Trott MBE, Member of Parliament for Sevenoaks; Dame Melanie Dawes, Ofcom CEO; Rob Jones, Director of Threat Leadership, National Crime Agency; and Deputy Chief Constable Ian Critchley, National Police Chiefs' Council lead for child protection. Representatives from Meta, Apple, Google, Talk Talk, Tik Tok and Snap also attended, as well as BT who very kindly sponsored the event as one of our founding Members.

Speakers at the IWF's 25th anniversary event at the House of Lords included, from left, IWF CEO Susie Hargreaves OBE; University of California, Berkeley, Prof Hany Farid; then Home Secretary Rt Hon Priti Patel MP; Rt. Hon. Baroness Nicky Morgan; and IWF Chair Andrew Puddephatt OBE



Video of IWF Champion Sarah Champion MP speaking about the work of the IWF on our 25th anniversary

Video of IWF Champion Simon Fell MP discussing the work of the IWF on our 25th anniversary

Policy in Europe

EU proposals to tackle Child Sexual Abuse

In February, the IWF used Safer Internet Day to urge the European Commission to bring forward their plans to tackle child sexual abuse online following an increase in reports to our Hotline by 374% in just two years, with the majority of the content being hosted in Europe.

In May, the European Commission announced their proposed new regulation to prevent and combat online child sexual abuse. The proposal from the European Commission would create a new independent EU Centre on Child Sexual Abuse and would place clear obligations on service providers to detect, block, report and remove child sexual abuse material. The proposal also focusses on prevention and assistance to victims as well as a role for national authorities.

In the same month, IWF CEO Susie Hargreaves OBE met with the European Commissioner for Home Affairs, Ylva Johansson, in Brussels to discuss the European Commission's new proposal. Discussions centered around the end of the temporary e-Privacy derogation in 2024 and the need for the proposal to complement existing international structures tackling CSEA online.

IWF CEO Susie Hargreaves OBE met with the European Commissioner for Home Affairs, Ylva Johansson, in Brussels in May

Alongside the UK Home Office, the IWF presented in August to a delegation from the Czech Presidency which is responsible for progressing the proposal file in the European Council.

In December, the IWF hosted a delegation from the European Parliament, which included the LIBE Rapporteur, Javier Zarzalejos MEP, to discuss strategies to combat child sexual abuse content online.

A group photo of attendees at MEP visit to the IWF office, showing, from left, Deputy Director at the UK Home Office, Christian Papaleontiou; Parliamentary Assistant to Niyazi Kizilyürek MEP, Hakan Choban; IWF Policy and Public Affairs Executive, Jonah Thompson; Secretary General of the European Parliament's Child Rights Intergroup, Emilio Puccio; UK Home Office Tackling Child Sexual Abuse Unit, Rob Corr; Parliamentary Assistant to Lena Dupont MEP, Anastasija Ore; Parliamentary Assistant to Javier Zarzalejos MEP, Zoe Nubla; Member of the European Parliament, Javier Zarzalejos; and IWF Chief Executive, Susie Hargreaves OBE

Review of the Child Sexual Abuse Directive

The European Commission held a public consultation on its review of EU rules to combat child sexual abuse. The IWF responded to this consultation in July, supporting the European Commission's intention for both new legislative and non-legislative measures to tackle the spread of child sexual abuse online. You can read the IWF's response here.

Council of Europe, Italian Presidency of the Committee of Ministers

In April, IWF CEO, Susie Hargreaves OBE, attended a two-day meeting in Rome to celebrate the launch of the new Strategy for the Rights of the Child (2022-2027). She spoke on a panel about protecting children from child sexual abuse and exploitation online.

IWF's 25th anniversary

As well as our UK event, the IWF was in Brussels in April to celebrate our 25th anniversary and to discuss the forthcoming EU legislation to tackle child sexual exploitation and abuse. Attendees at the event included Hilde Vautmans MEP, Vice-Chair of the European Parliament Intergroup on Children's Rights, Cathrin Bauer-Bulst, Head of Unit for the fight against cybercrime and child sexual abuse in DG Migration and Home Affairs at the European Commission, Maria Castello-Branco, Vice-Chair of the Lanzarote Committee, Professor Hany Farid from the University of California, Berkeley, IWF Chair Andrew Puddephatt OBE and IWF CEO Susie Hargreaves OBE. Read our release.

From left, speakers at the IWF's 25th anniversary event in Brussels included Prof Hany Farid from the University of California, Berkeley; Maria Castello-Branco, Vice-Chair of the Lanzarote Committee; IWF Chair Andrew Puddephatt OBE; and Hilde Vautmans MEP, Vice-Chair of the European Parliament Intergroup on Children's Rights. Cathrin Bauer-Bulst, head of unit for the fight against cybercrime and child sexual abuse in DG Migration and Home Affairs shown on screen

MEP Hilde Vautmans speaks at the IWF's 25th anniversary event in Brussels in April

International Policy

In May, we presented to a delegation of Malaysian parliamentarians from the Parliament Special Select Committee on Women and Children Affairs and Social Development at the National Crime Agency in London, alongside the WePROTECT Global Alliance.

IWF CEO Susie Hargreaves OBE and IWF Head of Policy and Public Affairs Michael Tunks can be seen fourth from left and far right respectively with Malaysian parliamentary members at the NCA in London in May

Where next for a 'UK Internet'?
PARLIAMENT & INTERNET
Ben Lake MP (Chair)
Michael Tunks, Senior Policy and Public Affairs Manager, IWF
Katie O'Donovan, Director of Government Affairs and Public Policy, Google
Emily Taylor, CEO, Oxford Information Labs
Amy Jordan, Director for Technology Policy, Ofcom
Till Sommer, Head of Policy, ISPA UK

Forums

The IWF’s opinion is sought internationally. We were also represented on the following forums this year:

At the **Parliament and Internet Conference** in March, IWF Head of Policy and Public Affairs Michael Tunks spoke on a panel alongside Ben Lake MP, Katie O’Donovan (Google), Emily Taylor (Oxford Information Labs), former Head of Policy at IPSA Till Sommer, and Amy Jordan (Ofcom).

Where next for a 'UK Internet'?
PARLIAMENT & INTERNET
Ben Lake MP (Chair)
Michael Tunks, Senior Policy and Public Affairs Manager, IWF
Katie O'Donovan, Director of Government Affairs and Public Policy, Google
Emily Taylor, CEO, Oxford Information Labs
Amy Jordan, Director for Technology Policy, Ofcom
Till Sommer, Head of Policy, ISPA UK

IWF Head of Policy and Public Affairs Michael Tunks, third from left, spoke on a panel at the Parliament and Internet Conference in March, alongside former Head of Policy at IPSA Till Sommer; Public Policy Manager at Google UK Katie O’Donovan; Plaid Cymru MP for Ceredigion Ben Lake; Emily Taylor, Oxford Information Labs CEO; and Ofcom Director of Technology Policy Amy Jordan

In October, Michael Tunks spoke at the **Safer Internet Forum** in Brussels and Chief Technology Officer Dan Sexton presented at the **European Liberal Forum**.

In November, Dan Sexton joined the **UK Internet Governance Forum** discussion on encryption alongside the ICO and Alec Muffet. Michael Tunks also attended the **FOSI conference**, **World Economic Forum event** in Washington DC and the **UN Internet Governance Forum**.

Members & partners

Our Members & partners

By Neil Prowse, IWF Development Manager

In 2022, our membership base continued to grow across sectors and industries, and into more countries, widening the reach, impact and benefit of our cutting-edge services. With 181 Members by the end of the year, and about 60% of these registered outside the UK, our deployment of services now crosses all continents, making the IWF a global force in disrupting child sexual abuse material online.

See who funds our work and takes our services.

In parallel, and through our ever-growing collaborations with industry Members closer to home, we helped to keep the UK a highly hostile location for hosting images and videos of child sexual abuse.

As the world adapted to living with Covid, we aimed to regularly meet face to face with Members throughout 2022 and continue to do so. Our stewardship programme has provided a chance to discuss wider topics, trends and challenges, and in some cases, meet in person for the first time. This is an ongoing programme and we hope to meet more of our Members in 2023. We were also delighted that our 2022 AGM could be held in person for the first time in several years, as it brought a degree of normality back to business.

We entered several new sectors during the year, welcoming the likes of Niantic, who operate in the world of augmented reality; and Qintel, who provide data forensics for law enforcement.

As part of our membership drive we looked at ways to work with other sectors, particularly within the bounds of encryption and privacy, and ran a campaign targeted at the VPN sector with the support of the VPN Trust Initiative and the Internet Infrastructure Coalition. Since then, we have held productive talks with many VPN providers and are optimistic that 2023 will see this sector explore the use of IWF services and expertise to stop the criminal circulation of online child sexual abuse imagery.

We have also had an influx of interest from both Members and corporate partners in new ways to collaborate, particularly in the safety tech sector, pushing boundaries and testing tools and technical innovations to tackle child sexual abuse material and improve online safety for children.

We anticipate our membership base to expand further in future, especially in light of the UK Online Safety Bill and increased UK regulation, but also in many other countries around the globe, as governments tighten up regulations to protect children in the online environment and attempt to stamp out the distribution of child sexual abuse material on the internet for good.

Our Members

Members as of 31 December 2022

£80,000 +

amazon.com		ASPIEGEL
BT	cisco	Globe
Google		Meta
Microsoft	MTN	PLDT Smart
sky	TalkTalk For Everyone	Telefónica
	VERISIGN	Virgin media

£50,000 +

ATLASSIAN

BROADCOM SOFTWARE

coinbase

Danske Bank

FORTINET

McAfee

paloalto NETWORKS

PayPal

Safaricom

TREND MICRO

zoom

£25,000 +

3

Avast

BAE SYSTEMS INSPIRED WORK

BrightCloud Threat Intelligence

CLOUDFLARE

CONVERGE

Dropbox

Forcepoint

linx

NIANTIC

ROBLOX

SOPHOS Cybersecurity delivered.

The Walt Disney Company UK & Ireland

Yandex

£20,000 +

allot See. Control. Secure.

Barracuda

exoClick

F-Secure

Llywodraeth Cymru Welsh Government Hwb®

JAGEX

jamf

SANDVINE

SONICWALL

The FA FOR ALL

WatchGuard

zscaler

£15,000 +

Chainalysis

depop

GRAYSHIFT

iomart

ALSI Group NetSTAR

STACKPATH

£10,000 +

AdEPT Education

AT&T

BBC

bumble inc.

CRISP A KROLL BUSINESS

CYACOMB

CYREN

cyta

DNSFilter

EASTERN COMMUNICATIONS

element

exa

G2 A TransUnion® Company

Gamma

GoDaddy Registry

iboss

identity™ digital

Impero

Jisc

JT

KCOM

LGfL

Lightspeed Systems®

MAGNUM PHOTOS

medialab

NetClean.

NETCRAFT

NetSupport

netsweeper

NOMINET

NORTH DAKOTA UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

OMICRON

ENEA Openwave

PA

pir

Qintel TARGETED. TACTICAL. RELEVANT.

radius

REVERSINGLABS

RM™

SafeToNet Incorporating Net Nanny

schools broadband

securly

senso. Remote Monitoring and Management

smoothwall® Part of family zone

sure.

switchshop IT NETWORKING AND SECURITY

SYSTEM1

TESCO mobile

wgtwo

zen

zvelo We categorize the Web

£5,000 +

.auDA	a	domain name commission nz
HYPERSLICE	ISPA UK THE VOICE OF THE UK INTERNET INDUSTRY	last.fm
Manchester Metropolitan University	( ) names.co.uk	NTU Nottingham Trent University
Performance Networks	SAFEDNS	SCORECHAIN
Sheffield Hallam University Knowledge Applied	ShortDot THE VALUE IS IN YOUR NAME	XYZ

£2,500 +

breadcrumbs
INVESTIGATE THE BLOCKCHAIN

CleanDNS

dhiraagu

E²BN

fastvue

iQ

IT Systems.
For Schools
For Learning
For Support

plan.com

Securus
Safeguard Monitor Protect

STRAW BERRY SOCIAL

US
UNIVERSITY OF SUSSEX

USENEXT

verifymy

vigilai

wightfibre
because we care

wykop.pl

yubo

£1,000 +

3 SIDES

4D

ANTI-HUMAN TRAFFICKING INTELLIGENCE INITIATIVE

AVANTI

BRIGHTSTAR

bublup

CYDA

CleanBrowsing

Diladele B.V.

GIGANEWS

Jigidi

Jurassic Fibre

Krystal

.LONDON THE NEW DOMAIN FOR LONDON

MeWe

mojeek

natterhub preparing children to thrive online

OAKFORD

Opendium e-Safety

Precedence TECHNOLOGIES

QUICKLINE

The Social Element

UNIVERSITY OF WINCHESTER

wildanet From anywhere to everywhere

XS NEWS USENET ACCESS

Our Members' testimonials

TikTok

"Child sexual abuse and exploitation is abhorrent and this kind of behaviour has no place online or off. As we work together on our shared mission of ending child sexual exploitation, it's with thanks to the IWF's knowledge and expertise that we're able to further protect our community from some of the internet's most heinous criminal content."

Elizabeth Kanter, Director of Policy and Government Relations

Meta

"Combating CSAM requires a society wide and holistic approach, which is why Meta has partnered with IWF for more than a decade, working together on ground-breaking initiatives to combat child exploitation online. We are proud of this long-standing partnership and the work we have achieved, and we will continue to collaborate with IWF and other partners across the globe to prevent and respond to this horrible crime."

Antigone Davis, VP, Global Head of Safety

AdEPT Education

"At AdEPT we are incredibly proud to be a Member of the Internet Watch Foundation (IWF). As a provider of IT, communications and connectivity to over 12,000 organisations across the UK (including more than 4,000 schools) we appreciate and support the crucial role that the IWF play in making the internet a safer place."

Schools Broadband (Talk-Straight)

"Safeguarding is at the very heart of everything Schools Broadband does, which is why we continue to support the vital work of the Internet Watch Foundation in their fight to protect children and young people from the horrendous child sexual abuse that exists around the world."

David Tindall, Schools Broadband CEO

Cyacomb

"We were privileged to collaborate with the Internet Watch Foundation on the UK Government Safety Tech Challenge Fund exploring potential solutions for detecting and blocking child sexual abuse material in End-to-End Encrypted messaging environments. The IWF provided deep understanding of the problem to be solved, the challenges in doing so, and was able to provide practical testing in appropriately secure and controlled environments. We learned a huge amount from this collaboration, and IWF testing contributed to confidence that the technologies under development were effective. We hope this work will continue to develop to the point where it can deliver real impact in the fight against child sexual abuse material in messaging for IWF Members and more widely."

Securus

"Securus is proud to partner with the Internet Watch Foundation who provide such an invaluable global service in the battle to eliminate child sexual abuse imagery online. Working together and sharing knowledge allows us to improve the support we offer all schools and education establishments with our monitoring and safeguarding solutions, increasing the protection for pupils from online harms and incidents."

ExoClick SL

"ExoClick fully supports the Internet Watch Foundation (IWF) in their mission to stamp out child sexual abuse online. As an active Member, we donate funds towards the services that the IWF provide and the great work that the organisation does in the global fight against ever increasing levels of child sexual abuse material. We have zero tolerance towards any form of the exploitation and online harm of children. As an online business, whenever we encounter such content, we immediately notify the IWF using their reporting tool. We are proud to help the service and the swift actions that the IWF take to rid the internet of this content. We will continue to support the IWF in the years to come."

CleanDNS

"The internet has a scourge of materials and behaviours to which the Internet Watch Foundation (IWF) has stepped up to address and mitigate. As CleanDNS's mission statement is "Cleaning up the internet for good" we share the commitment of the IWF of protecting victims. Via our membership support and our efforts to streamline the processing and evidencing of domains reported for victimisation, we ensure rapid assessment by IWF and mitigation via CleanDNS. There will be no concession in our efforts to mitigate and end these harms. We are proud to support IWF’s role in keeping the internet a safer place.”

Hutchison 3G UK Ltd (Three UK)

“The Internet Watch Foundation’s work has been invaluable to Three UK and has helped us deliver a step-change in how we go about combating online crime – in all its forms. We look forward to continuing to work with IWF over the next year and beyond, to build on this even further.”

George Robinson, Hutchison 3G UK Ltd Head of Government Relations

Jagex

“While most online activity is benign, fun, engaging and informative, less desirable parts of everyday society unfortunately also emerge. As with any online forum, games encounter this from time to time – ranging from internet trolls and harassment to account hijacking, child exploitation and self-harm. As living games are a microcosm of society, there is a responsibility for companies which develop those games to act responsibly, proactively seeking out these problems to tackle them effectively. As a business, one of our key areas of expertise is in how we monitor billions of lines of live chat – all day, all night, every day – to detect unwanted activity. To help this process, we have built our own heuristic computer-based tools, alongside a large and dedicated internal team. We are proud to continue to work closely with the Internet Watch Foundation, the National Crime Agency and its Child Exploitation and Online Protection command, local police, as well as other organisations and video games trade bodies such as UK Interactive Entertainment, to lean on their expertise. We form part of a network that helps identify trends and shape self-regulatory responses and official action. It’s an ecosystem to which we welcome even more living games makers to join.”

Crisp Thinking Group Ltd

“Crisp, a Kroll business, has partnered with the Internet Watch Foundation (IWF) for over a decade, working jointly on national and international policy, technology, AI and data solutions, as well as powering our Platform Risk Intelligence solutions with unique data sources from the IWF. As an active member of the global online safety community, Crisp recognises the critical value of a truly networked response. We continue to invest resources at all levels of memberships to ensure that we are helping to shape the future of a safer digital world for everyone.”

Coinbase

“Coinbase is committed to rooting out illicit activity within our business and the sector. As a company we are fully aware of the real damage that harmful content online can have on our society. This is why we have sought to work with the Internet Watch Foundation. The work they do is invaluable and makes a real difference to people’s lives. We look forward to continuing our partnership and helping them achieve their mission of making the online world a safe place for everyone.”

Coinbase Global Intelligence team

RM Education

“RM Education is proud to support the Internet Watch Foundation (IWF) in their work to remove child sexual abuse imagery online. In our work providing technology solutions to thousands of schools and trusts across the UK, RM has been leading the way in online safety in education for over 25 years. Working with partners such as the IWF brings us one step closer to improving safety for students and school staff online, without getting in the way of teaching and learning in an increasingly digital environment.

Senso

“Senso are proud to support the Internet Watch Foundation (IWF) in their mission to detect, disrupt, remove and prevent online child sexual abuse. Our safeguarding platform offers unprecedented safeguarding capabilities, protecting users using school-owned devices whether they are in school or learning from home, by proactively monitoring and indicating to relevant staff, any users who may be vulnerable or at risk, users who may pose a risk to others and inappropriate, off-task or harmful behaviour. Senso’s cloud-based solutions have enabled thousands of schools to monitor, manage and protect their students while online. We are committed to doing what’s necessary to ensure children are protected online with the help from partners like IWF.”

Bumble Inc.

“At Bumble Inc., safety is a top priority and at the core of everything we do. We approach safety through the lens of the most vulnerable users of online platforms: women, people of colour, and members of underrepresented communities. Although users under 18 years old are not allowed on our products, child and youth safety is paramount and something we take seriously. Our partnership with the Internet Watch Foundation helps us strengthen our capabilities to better and quickly detect and remove child sexual abuse material and those responsible for the distribution of these materials. This means that we can take swift action before it's shared on our platforms, preventing it from further perpetuating harm to victims and exposing others to this harmful content. It also enables us to report to authorities and aid in the investigation and prosecution of these crimes so that they can make the internet a safer place for everyone."

Google

"Since Google's earliest days, we've been committed to fighting the spread of child sexual abuse material both on our platforms and in the broader online ecosystem. We've invested heavily in cutting-edge technology, specially-trained teams, and share our technical expertise, resources, and tools with NGOs and industry coalitions to help others fight child sexual abuse and exploitation, and build a safer internet for all. We have a long and valued partnership with the Internet Watch Foundation (IWF), an organisation deeply committed to the fight against this awful crime. The IWF Hash List is a valuable repository for the tech industry and specialist NGOs. Moreover, content flags from the IWF Takedown Notices service – combined with their proactive approach – help prevent the revictimisation of child victims around the world. We're proud to call the IWF one of our core trusted partners in the fight against child sexual abuse material."

Amanda Storey, Senior Director of Trust & Safety at Google

Nominet

"Nominet, as the .UK registry, greatly value our work with the Internet Watch Foundation (IWF) to create a safer and secure internet. We provide access to IWF to our domain portfolios, and are pleased that this year to date, the IWF have not identified any cases of child sexual abuse material in relation to .UK, .Cymru and .Wales domains. Nominet are also proud to support IWF through our Countering Online Harms Innovation Fund. IWF are already at the forefront of tackling online images and videos of children being sexually abused. Nominet's funding aims to ensure they can stay one step ahead of perpetrators by pre-empting emerging threats and by fast-tracking research and ideas with potential to make a vital difference to the lives of children. We've seen over the past year how IWF have achieved this in practice, using Nominet's funding to innovate solutions that allow more child sexual abuse imagery to be removed more quickly and efficiently."

Natterhub

"As an online safety solution provider for primary schools, we work with the Internet Watch Foundation (IWF) to raise awareness of children's online vulnerabilities. The IWF annual report provides us with key data on the greatest threats children face online today. We recently collaborated on a Natterhub campaign: 'Have the conversation before someone else does'. Our shared aim was to encourage regular and relevant discussions with young people about their online experiences, as a preventative measure. We used transcript examples provided by IWF analysts for the campaign messaging. Despite coming together over some very serious topics, it is always a pleasure to work with the IWF team."

Cyren

"Ridding the internet of child abuse imagery is simply a matter of good versus evil. The Internet Watch Foundation's mission is an unfortunate necessity, and a reminder of the darkness in the world. We are thankful for their dedicated efforts to protect children and proud to work with them to block harmful online content."

Verisign

"As a provider of critical internet infrastructure, Verisign is committed to its mission of helping to ensure the safety and security of the internet. Our partnership with the Internet Watch Foundation and the ability to trust the information that they provide to us has been invaluable in our efforts to make real, measurable differences in the fight against child sexual abuse material online."

Globe

"As the leading full-service telecommunications company in the Philippines, Globe connects its millions of customers to much-needed online services through its suite of digital solutions products. In its business operations, it understands that exposure to the digital world also comes with vulnerabilities and challenges. Under its #MakeITSafe programme, Globe partnered with the Internet Watch Foundation (IWF) to bolster their fight against online sexual abuse and exploitation of children by blocking, reporting, and removing sensitive content within its online network to promote child safety. In 2022, Globe and IWF celebrated World Safer Internet Day alongside partners from UNICEF Philippines and the SaferKidsPH Consortium, CitizenWatch, and Bantay Konsyumer, Kalsada, Kuryente (BK3) through a virtual public webinar that highlighted the importance of holistic cooperation among the public and private sectors, international and civil society organisations, and digital citizens in fighting online sexual abuse and exploitation of children. Globe has invested over $2.7 million for content filtering systems to block websites and online imagery that promote child sexual abuse and piracy. To date, it has blocked a total of 360,106 URLs and 1,614 domains linked to child sexual abuse material with the IWF. Globe remains steadfast in its commitment to keep its customers safe in their interactions online."

Cloudflare

"The Internet Watch Foundation (IWF) Member services are integral components to Cloudflare's child safety efforts across our vast global network and the millions of web properties that use our services. Cloudflare greatly values the expertise and dedication of the IWF as we work together in supporting the critical mission of the swift detection and removal of child sexual abuse material."

SafetoNet

"SafeToNet is a Member of the Internet Watch Foundation (IWF) and regular attendee at the Funding Council meetings. The role the IWF play in worldwide efforts to tackle online harms is well known and rightfully widely acknowledged and lauded. In addition, the assistance, and opportunities they provide to companies such as SafeToNet to partner and develop innovative technologies is priceless. Over the past few months, we have worked closely with the fantastic information technology team led by IWF CTO Dan Sexton to jointly create technology that seeks to prevent the creation and widespread distribution of child sexual abuse material."

Zoom

"Half a million businesses and hundreds of thousands of schools and higher education institutions globally choose Zoom for their critical communications. We take seriously our responsibility to ensure the safety, privacy and security of our users and their data, but this work is not done alone. Zoom is a proud Member of the Internet Watch Foundation (IWF) and our membership is a critical element in our effort to combat child sexual abuse material online. We are fortunate on a daily basis to collaborate with, and learn from, non-profits, industry peers and government institutions to refine our policies and how we detect, deter and prevent the spread of child sexual abuse material online. We look forward to working closely with the IWF on our shared mission in the years ahead."

Welsh Government

"As a government, we are absolutely committed to playing our part in keeping children and young people safe online. We are proud that we were the first government body to become a Member of the Internet Watch Foundation (IWF) in 2021. Membership allows us to deploy IWF services on Hwb, the national digital learning platform in Wales. As well as helping to keep our learners safe online, we consider our membership as an important way to support IWF's ongoing work to eliminate online child sexual abuse content globally and ensure the vital continuation of their report services. We have renewed our membership for 2022-23 and value IWF membership as a core part of our Hwb service."

NetSupport

"Part of NetSupport's mission is to support safer online environments in schools through our education solutions. We have immense respect for the valuable and challenging work the Internet Watch Foundation does, and we are proud to incorporate their keyword list into our technology to help us protect thousands of students worldwide from online risks as they learn." – Al Kingsley, NetSupport CEO

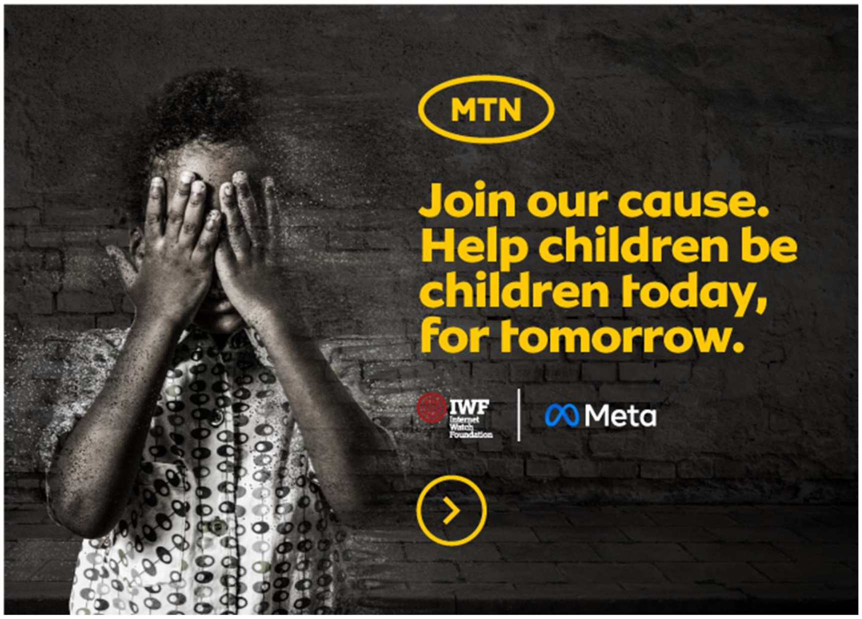
G2 Web Services

"G2 is proud to have worked alongside the Internet Watch Foundation (IWF) since 2014. The level of knowledge and dedication shown by the team is outstanding. The services IWF provide in ridding the internet of child sexual abuse material are invaluable. We will continue to work with the IWF in combatting child exploitation and creating a safer digital landscape for children across the globe.”

Converge

“The Internet Watch Foundation (IWF) has been instrumental in the safer internet advocacy of Converge. It has helped the company put forward its campaign against the online sexual abuse and exploitation of children by blocking unsafe sites in its network. The timely advice of IWF and prompt communications have allowed Converge to act decisively on issues that matter most to our customers and the society in general. By providing Converge with quality information on malicious websites, the company can filter its network. The consistent updates have helped the company’s network operations team to keep up with dangerous trends online. Moving forward, Converge sees its partnership with IWF as an integral part of its advocacies. Converge sees this collaboration as a foundation in its journey to create a better, secure, and safe digital highway for the most vulnerable online users – our children.”

IWF reporting portals


MTN
Join our cause. Help children be children today, for tomorrow.
IWF Internet Watch Foundation
Meta

Many countries around the world have no current way for their citizens to report suspected online child sexual abuse imagery. This is why we have established a global network of reporting portals which provide an online link directly to our team of expert analysts in the UK.

We work in partnership with local government, police, industry, funders and charities to set up and promote the portals, which are customised webpages locally branded to suit the host country. When reports are confirmed as criminal by the team in our UK Hotline, we work to have the images and videos removed from the internet.

We're proud to have 50 active portals today – 51 including the UK – which give billions of people globally a safe place to report suspected pictures and videos online and help to prevent the repeat victimisation of those who've already suffered the worst kinds of abuse.

In 2022 we partnered with two leading global organisations to launch portals for use in more than one country or nation.

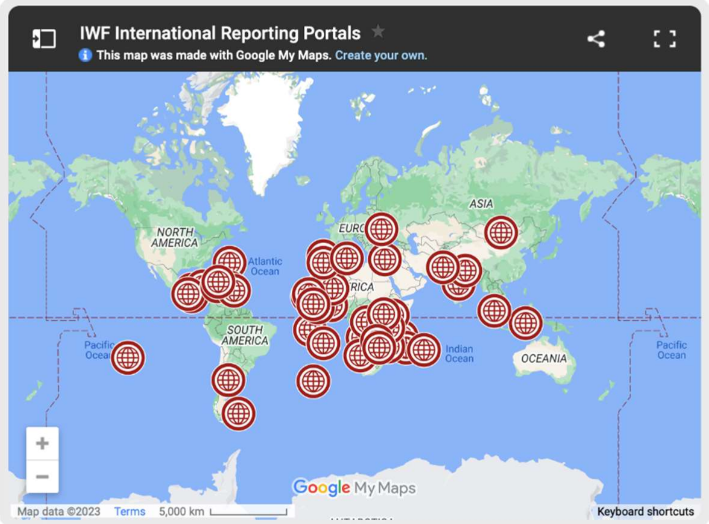
Our long-term partnership with the US-based International Centre for Missing and Exploited Children (ICMEC) led to the launch of the IWF/ICMEC Reporting

Portal for people in any country without a reporting solution to anonymously report child sexual abuse imagery.

ICMEC CEO, Bob Cunningham said: “Child sexual abuse material is a global problem that demands a global solution. The trauma for victims of child sexual abuse continues every time images or videos of their abuse are viewed. Through our partnership with IWF to bring reporting capabilities to every citizen around the world, we are stopping the further abuse of children and making the internet a safer place for everyone.”

We also partnered with one of Africa’s largest telecommunications providers and IWF Member MTN to launch the Child Safety Online Africa Portal. While 23 countries in Africa already have their own reporting portal or hotline, the Child Safety Online Africa Portal will be accessible in countries where there is not yet a reporting mechanism to ensure even more countries on the continent are able to report child sexual abuse material.

Nompilo Morafo, Chief Sustainability and Corporate Affairs Officer at MTN said: “Protecting children online is a global challenge, which requires a global approach. As we lead digital solutions for Africa’s progress, we have a critical role in ensuring that every African child is kept safe online. In alignment with our African values, we need to join forces to create a safe online village for our children. One where they are free from fear, humiliation, and abuse. One where they can have a normal childhood.”



IWF International Reporting Portals

This map was made with Google My Maps. Create your own.

Charity of the year

We began our Charity of the Year partnership programme in 2021. Through this scheme we currently work with firms, both in Cambridge and from the wider UK, who select the IWF as their charity of the year and support us in a variety of ways, including running fundraisers on our behalf, and raising the profile of the IWF through their networks.

These partnerships allow us to collaborate closely with organisations with whom we share common values and ethics but who we would otherwise not normally get the opportunity to work alongside.

We engage positively with our partners, helping them to fulfil their corporate social responsibility objectives through activities that encourage teamwork and positive staff participation while bringing attention to the vital work that we do at the IWF.

We hope to grow this programme with organisations that would like to work with us, whether from the UK or further afield.

BDB Pitmans

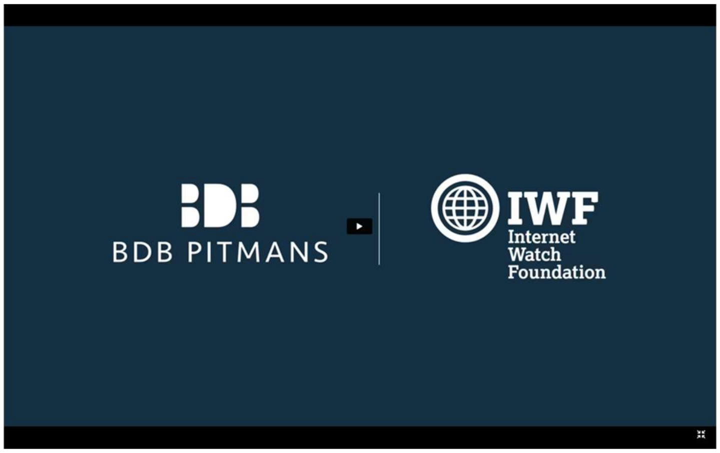
BDB PITMANS

BDB Pitmans is a law firm with offices in London, Southampton, Reading and Cambridge. The Cambridge branch chose us as their Charity of the Year in summer 2021, and we're proud that they want to continue working with us until at least summer 2023.

Fundraising activity has included events such as sponsorship of charity runners and charity running vests at the Cambridge Half Marathon and selling branded lanyards to their staff across the UK.

BDB Pitmans have also provided regular use of their London and Cambridge offices to host IWF meetings and training sessions. Their nationwide client magazine, Building Better, featured a double-page spread focused on IWF’s tech-for-good work, to encourage support and increase awareness of our organisation.

The firm regularly promotes the IWF on their website and social media and offers a wealth of in-house expertise, including specialist charity lawyers who can be on hand for advice.



BDB Pitmans Marketing Director Kevin Peake

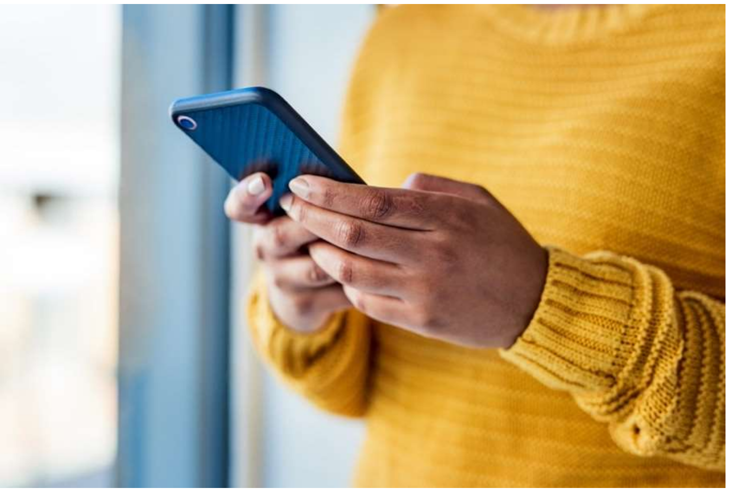
Trenches Law

We were delighted to partner with Hampshire firm Trenches Law in the summer of 2022. Legal experts in electronic communications, the firm’s responsibilities include working with alternative network ISPs in the UK. This is a key future sector for the IWF to engage with in our work to protect all internet users.

At the Connected Britain Conference in September 2022, Trenches Law promoted the IWF at their exhibition stand and aided introductions on our behalf with prospective Members.

As well as future fundraising efforts, Trenches Law employees run an annual charity day when they'll carry out their chosen fundraising activity in support of the IWF.

Cryptocurrency unit



In 2022 we launched a 'crypto unit' in the Hotline to respond to the increasing use of cryptocurrencies by offenders to pay for sexual content of children online.

Our analysts had found that websites offering cryptocurrency payment for child sexual abuse images had doubled almost every year since 2015.

We record valuable data from child sexual abuse website payment pages, including information about the wording used, the type of virtual currency and the amount, as well as the cryptocurrency wallet address of the provider.

The unit works closely with law enforcement from around the world who use the information we provide to trace and identify criminals through crypto and other currency transactions online.

Analysts in the unit receive daily queries from organisations such as the Metropolitan Police in the UK to the US Internal Revenue Service's Criminal Investigation branch who request information about websites and crypto addresses that may be linked to illegal activity.

As part of their responsibilities, the crypto unit also provides data sets to IWF Members for specific projects, monitors new payment sites and sends regular cryptocurrency updates via virtual alerts.

By sharing the payment information displayed on commercial child sexual abuse websites with partners in the financial industry we can help to prevent misuse of their services and disrupt further spread of the criminal imagery.

Detective Inspector Darren Young, from the Online Child Sexual Abuse and Exploitation unit at the UK Metropolitan Police said: “The Metropolitan Police Service is committed to using all avenues possible to identify victims and perpetrators of online child sexual abuse and exploitation.

“We are seeing cryptocurrency being used to pay for the distribution of abusive images and the online sexual exploitation of children, with perpetrators believing they can hide behind the anonymity of these virtual currencies.

“The IWF has been a key partner to law enforcement for many years and the newly formed crypto unit provides greater opportunities to combat these horrendous crimes, rescue children from sexual abuse and arrest offenders.”

Glossary

Banner site: A website or webpage made up of adverts for other websites with text links or images that take you to third-party websites when you click on them.

Blog: A blog is a discussion or information site made up of separate entries, or posts. Most are interactive, and visitors can leave comments and even message each other on the blog. The interactivity is what makes them different from other static websites.

CAID: The Child Abuse Image Database (CAID) is a project led by the Home Office which enables UK law enforcement to assess, categorise and generate unique hashes for tens of millions of child abuse images and videos found during their investigations.

Category A, B and C:
We assess child sexual abuse images and videos based on UK law, according to the levels in the Sentencing Council's Sexual Offences Definitive Guidelines. Since April 2014, there have been three levels:
A: Images involving penetrative sexual activity; images involving sexual activity with an animal or sadism.
B: Images involving non-penetrative sexual activity.
C: Other indecent images not falling within categories A or B.

Child sexual abuse images/videos/imagery/content/material: Images or videos that show the sexual abuse of children. We use the term 'child sexual abuse' images to reflect the gravity of the images we deal with.

Cryptographic hash: A cryptographic hash is a digital fingerprint of any form of digital data. Cryptographic algorithms can hash a single word, an mp3, a zip file – anything digital. Cryptographic hashes can be used to identify exact matches of that digital data.

Cyberlockers: File hosting services, cloud storage services or online file storage providers. They are internet hosting services specifically designed to host users' files.

Dark net: The dark net, also known as the dark web, is the hidden part of the internet accessed using Tor. Tor is anonymity software that makes it difficult to trace users' online activity.

Disguised websites: Websites which, when loaded directly into a browser, show legal content—but when accessed through a particular pathway (or referrer website) show illegal content, for example child sexual abuse images.

Domain alerts: Details of domain names that are known to be hosting child sexual abuse content.

Forum: Also known as a 'message board', a forum is an online chat site where people talk or upload files in the form of posts. A forum can hold sub-forums, and each of these could have several topics. Within a topic, each new discussion started is called a thread, and any forum user can reply to this thread.

Gateway sites: A webpage that provides direct access to child sexual abuse material but does not itself contain it.

GPUs (Graphics Processing Units): sometimes called "graphics cards" are designed to do lots of simultaneous calculations independently. Typically, they're used in gaming but they can also be used to solve more general purpose computational problems on large scale data.

Hash/hashes: A 'hash' is a unique code, or string of text and numbers generated from the binary data of a picture. Hashes can automatically identify known child sexual abuse images without needing to examine each image individually. This can help to prevent online distribution of this content.

Hidden services: Websites that are hosted within a proxy network, so their location can't be traced.

Image board: An image board is a type of internet forum that operates mostly through posting images. They're used for discussions on a variety of topics, and are similar to bulletin board systems, but with a focus on images.

Image host/Image hosting site: An image hosting service lets users upload images which are then available through a unique URL. This URL can be used to make online links, or be embedded in other websites, forums and social networking sites.

IWF Reporting Portal: A world-class reporting solution for child sexual abuse content, for countries which don’t have an existing Hotline.

Keywords: A list of terms associated with child sexual abuse material searches.

Newsgroups: Internet discussion groups dedicated to a variety of subjects. Users make posts to a newsgroup and others can see them and comment. Sometimes called ‘Usenet’, newsgroups were the original online forums and a precursor to the World Wide Web.

Non-photographic child sexual abuse content: Images and videos of child sexual abuse which aren’t photographs, for example computer-generated images.

Perceptual hash: A perceptual hash is a digital fingerprint of an image which has been created using an algorithm. Perceptual hashes enable near-duplicates of that image to be identified.

Proactive/proactively searching/proactively seeking: We can now actively search for child sexual abuse content, in addition to taking public reports. We’re one of only a few Hotlines in the world that can do this.

Proxy network: These are systems that enable online anonymity, accelerate service requests, encryption, security and lots of other features. Some proxy software, such as Tor, attempts to conceal the true location of services.

Revictimisation: Revictimisation, or repeat victimisation is what happens to a victim when their image is shared online. A single image of a victim can be shared hundreds or thousands of times.

Service Provider/Internet Service Provider: An internet service provider (ISP) is a company or organisation that provides access to the internet, internet connectivity and other related services, like hosting websites.

Social networking site: A social networking service is a platform to build social relations. It usually has a representation of each user (often a profile), their social links and a variety of other services. Popular examples include Facebook and Twitter.

'Self-generated' child sexual abuse imagery: We regard the term 'self-generated' child sexual abuse 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, we will continue to use the term 'self-generated' as, within the online safety and law enforcement sectors, this is well recognised.

Top-level domain (TLD): Domains at the top of the domain name hierarchy. For example .com, .org and .info are all examples of generic top-level domains (gTLDs). The term also covers country code top-level domains (ccTLDs) like .uk for UK or .us for US and sponsored top- level domains (sTLDs) like .mobi or .xxx

URL: An acronym for Uniform Resource Locator. A URL is the specific location where a file is saved online. For example, the URL of the IWF logo which appears on the webpage www.iwf.org.uk is www.iwf.org.uk/themes/iwf/images/theme- images/logo.png.

Webpage: A document which can be seen using a web browser. A single webpage can hold lots of images, text, videos or hyperlinks and many websites will have lots of webpages. www.iwf.org.uk/about-iwf and www.iwf.org.uk/Hotline are both examples of webpages.

Website: A website is a set of related webpages typically served from a single web domain. Most websites have several webpages.