Home Office

Interim Code of Practice on Online Child Sexual Exploitation and Abuse

December 2020

Contents

Overview of the interim code

S1 PRINCIPLE 1

Companies seek to prevent known child sexual abuse material from being made available to users or accessible on their platforms and services, take appropriate action under their terms of service, and report to appropriate authorities.

S1 PRINCIPLE 2

Companies seek to identify and combat the dissemination of new child sexual abuse material via their platforms and services, take appropriate action under their terms of service, and report to appropriate authorities.

S1 PRINCIPLE 3

Companies seek to identify and combat preparatory child sexual exploitation and abuse activity (such as online grooming for child sexual abuse), take appropriate action under their terms of service, and report to appropriate authorities.

S1 PRINCIPLE 4

Companies seek to identify and combat advertising, recruiting, soliciting, or procuring a child for sexual exploitation or abuse, or organising to do so, take appropriate action under their terms of service, and report to appropriate authorities.

S1 PRINCIPLE 5

Companies seek to identify and combat the use of livestreaming services for the purpose of child sexual exploitation and abuse, take appropriate action under their terms of service, and report to appropriate authorities.

S1 PRINCIPLE 6

Companies seek to prevent search results from surfacing child sexual exploitation and abuse, and seek to prevent automatic suggestions for such activity and material.

S2 PRINCIPLE 7

Companies seek to adopt enhanced safety measures with the aim of protecting children, in particular from peers or adults seeking to engage in harmful sexual activity with children; such measures may include considering whether users are children.

S2 PRINCIPLE 8

Companies seek to take appropriate action, including providing reporting options, on material that may not be illegal on its face, but with appropriate context and confirmation may be connected to child sexual exploitation and abuse.

S3 PRINCIPLE 9

Companies seek to take an informed global approach to combating online child sexual exploitation and abuse and to take into account the evolving threat landscape as part of their design and development processes.

S3 PRINCIPLE 10

Companies support opportunities to share relevant expertise, helpful practices, data and tools where appropriate and feasible.

S3 PRINCIPLE 11

Companies seek to regularly publish or share meaningful data and insights on their efforts to combat child sexual exploitation and abuse.

S4 PRINCIPLE 12

Companies seek to implement effective user reporting, complaints and timely redress processes to ensure users are empowered and protected.

S5 LAW ENFORCEMENT

Child sexual exploitation and abuse needs to be reported to appropriate authorities, which may include law enforcement. Which authority a report should be made to will vary depending on where a company is based. Reporting allows victims to be identified and offenders apprehended, removing children from abusive situations.

A4 APPENDIX 4

Specific guidance for SMEs on how to apply this code to their services and encourages SMEs to consider how services and users can best be protected using available resources.

Introduction

The interim code of practice on online child sexual exploitation and abuse

Child sexual exploitation and abuse (CSEA) is an abhorrent crime that has a devastating impact on victims and their families. It is imperative that companies do everything they can to tackle online CSEA, which includes the sharing of child sexual abuse material, the livestreaming of child sexual abuse and the online grooming of children. This interim code provides detailed guidance for companies on actions they can take to tackle CSEA that occurs on their services or platforms.

The volume of online child sexual abuse material continues to grow. In 2019, US technology companies referred 69 million child sexual abuse images and videos to the National Center for Missing and Exploited Children (NCMEC), up from 45 million in 2018; the UK's Internet Watch Foundation (IWF) identified and removed 132,700 webpages containing child sexual abuse material, a 26% increase on the previous year, and 39% of the children they identify in these images are under the age of 11. The sexual abuse of children online is also becoming easier and more extreme with offenders able to target multiple children online and orchestrate the abuse in real time.

In March 2020, the UK, US, Australia, Canada and New Zealand launched the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse. We welcome those companies that have endorsed these principles and declared their commitment to tackling online CSEA. This CSEA interim code of practice builds upon the Voluntary Principles, setting out the UK government's expectations on all companies in scope of the new regulatory framework to tackle CSEA. The government will separately produce voluntary best practice guidance for infrastructure service providers.

This interim code of practice provides detailed guidance for companies to help them understand and respond to the breadth of CSEA threats, recognising that this threat and the response that it requires will vary depending on the type and nature of the service offered. We have seen that positive action by industry can have a meaningful impact on the safety of children online, and we encourage all companies to be proactive and ambitious in how they consider and implement the recommendations within this interim code of practice.

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018

All measures that companies take under this interim code of practice must comply with all aspects of the data protection legislation. The Age Appropriate Design Code states that a compelling reason for sharing a child's data is for the purpose of preventing child sexual exploitation and abuse online. Appendix 2 provides further information on the application of data protection rules for this interim code.

Purpose of the interim codes of practice

The Online Harms White Paper committed the government to produce two voluntary interim codes of practice setting out the action companies are encouraged to take to combat terrorism and child sexual exploitation and abuse online ahead of a regulator becoming operational and issuing full codes of practice.

The Interim Code of Practice on Terrorist Content and Activity Online will be released in tandem with this code. While the two codes are designed to be aligned to one another as much as possible to assist companies with understanding and implementing both codes, there are some differences as they respond to two different threats.

The interim codes and all the principles contained within them are voluntary and non-binding. Companies should consider factors such as the nature of their services, the underlying architecture of their systems, the risks to their users, and the availability of established or emerging technologies appropriate for addressing the issues identified.

The principles are not reliant on the online harms legislation coming into force and all of the measures outlined in this interim code are steps that companies can take now, either on a voluntary basis or under existing legal frameworks. Government will work with the online harms regulator so that appropriate learning from companies' experience in adopting measures that are recommended in this interim code can inform the development of the regulator's codes of practice.

The aims and examples of good practice under each principle are intended to set out for all companies (including small to medium sized enterprises - see Appendix 4) action that can be taken to tackle the CSEA threat on a wide range of services and to allow companies to begin to prepare for the codes of practice which will be produced by the regulator once it is in place.

This interim code of practice is designed to be read in parallel with the Full Government Response to the Online Harms White Paper. It reflects the expectations set out in the White Paper and seeks

to mitigate a range of risks posed by CSEA online, building on existing industry and government-led initiatives.As far as possible, this interim code of practice takes into account how the future online harms regulation is likely to work, as set out in the Full Government Response. By taking action to protect their users from this serious harm now, companies will be better prepared when the online harms legislation comes into force.

The UK is committed to protecting fundamental rights, including freedom of expression and privacy, as well as to a free, open and secure internet.

Under the interim codes companies are encouraged to:

- have mechanisms for understanding the level and nature of threats on their services (as far as reasonably practicable), the impact of changes to systems, processes and policies they introduce, and remaining areas of high risk.
- take all reasonable steps to implement each principle in this Interim Code, where it is relevant for their services.
- review their existing safety processes and terms and conditions against each of the principles. Based on this review, identify and act on gaps in existing measures or where existing measures can go further, for example by improving and investing in tools and moderation processes and innovating to address areas of risk.
- share information, best practice, and tools across industry, particularly with smaller companies, for example through working collaboratively with industry bodies. Smaller companies are encouraged to proactively seek information, best practice and tools.
- be transparent about how the above steps have been actioned and, where appropriate, provide public reports, which may include content/account removal, user complaints received and user redress requests.

Section 1:
Identify, Prevent and Act on CSEA

PRINCIPLE 1: Companies seek to prevent known child sexual abuse material from being made available to users or accessible on their platforms and services, take appropriate action under their terms of service, and report to appropriate authorities.

Context: Companies, non-governmental organisations and law enforcement agencies have done significant work to identify and catalogue child sexual abuse material. This process can prevent the continued circulation of such materials and avoid further re-victimising the children depicted. These children suffer ongoing and additional trauma each time materials depicting their abuse are viewed. Reducing the availability of known material can also help avoid further offending, including offences concerning distribution. Interventions where offenders are sharing material on mainstream platforms without actually transmitting files are also critical.

Aims of the principle:

Under this principle companies should take reasonable steps to:

- proactively identify known child sexual abuse material such as images, pseudo images[1], video, URLs and paedophile manuals, and prevent it from being made available to users.
- act in the best interest of the child and adult victims of CSEA when considering the safety protections for children and the privacy interests of users in deciding which services to apply these measures across.
- where known child sexual abuse material cannot be identified until after it is uploaded, take all appropriate and feasible steps to remove it and minimise the likelihood of this material being made available to other users from that point onwards.
- ensure users are able to easily and swiftly report child sexual abuse material on their service.

Examples of good practice:

When implementing this principle, companies may wish to take steps including:

- develop in-house or integrate third-party tools to identify known child sexual abuse material, including images, video, and other material such as paedophile manuals.
- utilise reference lists of known CSA material, for example hash lists and URL lists provided by NGOs.
- create, maintain and share their own CSA material hash list.
- where possible, block any matching CSA images, videos or other materials (e.g. paedophile manuals) before they are posted, distributed or made available to users in any other way.
- maximise the effectiveness of these tools, for example through the level of certainty at which tools flag matches, which hash sets are being ingested and the overall size of the hash data set, the ability to detect altered images, and which parts of the service automated tools are applied across.

1 *This covers photographs (including moving images) and images made, for example, on a computer but which look like real photographs. This can include photos, videos, tracings and derivatives of a photograph and data that can be converted into a photograph.*

- ensure other indicators that may act as a signal for child sexual abuse material are considered. These indicators may include search terms, suggestive chat group or forum names, use of known offender terminology including named victims, and activity such as accounts that are connected to or have received CSA material from users already identified as sharing CSA material. All personal data should be handled sensitively – see Appendix 2.
- carry out a human review if necessary, have sufficient trained and vetted moderators to progress user and NGO reports and matches from automated tools, and make provision for the psychological assessment and welfare of staff viewing this distressing material.
- take steps to address indecent imagery of children in the older age range (13-17-year olds), particularly where supporting information is available such as an NGO confirming the image contains a child under 18. When it is probable that sexual material is of a child (under 18-years-old), take action that is in the best interest of the child. This could include removing an image from your service until the user can confirm that the image is of an adult.
- take steps to combat all child sexual abuse imagery, including that which does not show penetrative sexual activity. See Appendix 1 for the legal definition of an indecent image of a child.
- provide a streamlined reporting system for authorised NGOs (such as national hotlines) or other trusted organisations to report CSA material, and review (if necessary) and take down material as a matter of priority when reported by these organisations.
- provide a user/public reporting system that allows suspected CSA material and accounts to be flagged for urgent review. Once confirmed as CSA, material should also be taken down as a matter of priority.
- close accounts involved in child sexual exploitation and abuse and take steps to prevent individuals re-registering under different details.
- child sexual exploitation and abuse is a serious crime and a child could be at risk – report it to the authorities using the guidance at section 5.

Case study: Olivia

Olivia* was repeatedly raped and sexually tortured. It's highly likely that it was her abuser who first shared the images of Olivia's suffering. The police rescued Olivia when was eight years old - five years after the abuse first began. Her physical abuse ended and the man who stole her childhood was imprisoned. But those images are still in circulation and offenders continue to share and probably profit from Olivia's misery. The Internet Watch Foundation (IWF) see Olivia every day - five years after she was rescued. During a three-month period, the IWF saw her at least 347 times. On average, that's five times each and every working day. Some of her images were found on commercial sites. This means that in these cases, the site operator was profiting from this child's abuse.

*not her real name

Statistic

Globally 69 million images and videos of child sexual abuse material were reported by technology companies to the National Center for Missing and Exploited Children in 2019 - a 53% increase on 2018 (45 million). This reflects the work that companies already do to proactively identify and report CSEA.

Technologies

A number of organisations provide hash lists or URL lists that enable companies to detect known CSA images and videos, including the Internet Watch Foundation and the National Center for Missing and Exploited Children.

See the Safety Tech Innovation Network for more information about available safety technologies.

PRINCIPLE 2: Companies seek to identify and combat the dissemination of new child sexual abuse material via their platforms and services, take appropriate action under their terms of service, and report to appropriate authorities.

Context: The threat to children depicted in new materials is often different to the threat to children in known materials. Newly generated material is more likely to indicate current and ongoing offending, such as against an unidentified victim who continues to be abused or a child being groomed and coerced into producing new abusive images. The identification of these materials and their referral to appropriate authorities is time critical.

Aims of the principle:

Under this principle companies should take reasonable steps to:

- proactively identify new child sexual abuse material such as images, pseudo images[2], video, URLs and paedophile manuals, and prevent it from being made available to users.
- continue innovating towards this goal, recognising that technology to identify new material is less advanced than technology to identify known material.
- act in the best interest of the child and adult victims of CSEA when considering the safety protections for children and the privacy interests of users in deciding which services to apply these measures across.
- where new child sexual abuse material cannot be identified until after it is uploaded, take all appropriate and feasible steps to remove it and minimise the likelihood of this material being made available to other users from that point onwards.
- ensure users are able to easily and swiftly report suspected child sexual abuse material on the platform.

Examples of good practice:

When implementing this principle, companies may wish to take steps including:

- develop in-house or integrate third-party tools that are able to identify, based on previously seen characteristics, new child sexual abuse material, including images and video.
- where possible, block any identified images before they are posted, distributed or made available to users in any other way.
- maximise the effectiveness of these tools, for example through the data they are trained on, the level of certainty at which tools flag matches, and which parts of the service automated tools are applied across.
- ensure other indicators that may act as a signal for child sexual abuse material are considered. These may include search terms, suggestive chat group or forum names, use of known offender terminology including named victims, and account activity such as accounts that are connected to or have received material from users already identified as sharing CSA material.
- carry out a human review if necessary, have sufficient trained and vetted moderators to progress user and NGO reports and matches from automated tools, and make provision for the psychological assessment and welfare of staff viewing this distressing material.
- take steps to address indecent imagery of children in the older age range (13-17-year olds), particularly where supporting information is available such as an NGO confirming the

2 *This covers photographs (including moving images) and images made, for example, on a computer but which look like real photographs. This can include photos, videos, tracings and derivatives of a photograph and data that can be converted into a photograph.*

image contains a child under 18. When it is probable that sexual material is of a child (under 18-years-old), take action that is in the best interest of the child. This could include removing an image from your service until the user can confirm that the image is of an adult.

- take steps to combat all child sexual abuse imagery, including that which does not show penetrative sexual activity. See Appendix 1 for the legal definition of an indecent image of a child.
- provide a streamlined reporting system for authorised NGOs (such as national hotlines) or other trusted organisations to report material, and review (if necessary) and take down material immediately when reported by these organisations.
- provide a user/public reporting system that allows suspected CSA material and accounts to be flagged for urgent review. Once confirmed as CSA, material should also be taken down as soon as reasonably possible.
- close accounts involved in child sexual exploitation and abuse and take steps to prevent individuals re-registering under different details.
- child sexual exploitation and abuse is a serious crime and a child could be at immediate threat to life or risk of serious harm – report it to the authorities using the guidance at section 5.

Statistic – Project Arachnid

Project Arachnid is a tool that crawls websites to identify child sexual abuse material. Since its introduction in 2016, the tool has processed over 125 billion images and sent 6 million notices to electronic services providers requesting that the illegal material is removed. Eighty-five percent of the notices issued relate to victims who are not known to have been identified by police. More information is available on the Project Arachnid website

Case study: Investigating new CSAM content

In 2017 a British man filmed his sexual attacks on children four times and uploaded them to a messaging app. He did so because he wanted to join a private paedophile discussion group which had a condition that new members must post brand new abuse images. In October 2018 Homeland Security Investigations in America shared intelligence with the NCA which had stemmed from an industry report from the National Center for Missing and Exploited Children. The intelligence related to the video files being shared on a cloud storage provider and the British man was arrested by the NCA within 24 hours.

Case study: IWF Analyst

"I was very proud this year when I learned my actions helped to safeguard two girls. I was assessing a video which captured their abuse via a live stream. One of the girls held up a sign with a profile name and I got to work. I found a number of social media accounts and sent a victim ID referral to our partners at the National Crime Agency's Child Exploitation Online Protection team (NCA CEOP). It helped to narrow the search. We heard back from the police that actions to safeguard the girls were taking place. It's great to know I have played a part in that."

PRINCIPLE 3: Companies seek to identify and combat preparatory child sexual exploitation and abuse activity (such as online grooming for child sexual abuse), take appropriate action under their terms of service, and report to appropriate authorities.

Context: Online grooming is a preparatory phase in which someone builds trust and rapport with a child or a third party (such as their guardian or sibling) in order to gain access to that child for the purposes of sexual activity. Online grooming may include offenders encouraging the victim to engage in sexual activity or to send the offender sexually explicit material. It may lead to offenders meeting the victim or blackmailing them to produce more abuse material (for example by threatening to send images and videos to friends and family). Offenders may also convince a victim to migrate to other platforms in the grooming phase to evade detection.

Aims of the principle:

Under this principle companies should take reasonable steps to:

- use safety by design approaches to make predatory offender-child interactions less likely, and to deter offenders from these interactions.
- proactively identify, through language or behaviours, individuals engaging in criminal predatory behaviour such as sexual communication with a child or the procurement of a child for sexual services.
- continue innovating towards this goal, recognising that technology is still improving in this area.
- act in the best interest of the child and adult victims when considering how to balance the safety protections for children and the privacy interests of users in deciding which services to apply these measures across.

Examples of good practice:

When implementing this principle, companies may wish to take steps including:

- implement safety by design measures, for example to limit unsolicited approaches from adults to children and expedite displaying deterrent messaging to adults and restricting the functionality of geolocation for child users.
- reduce the ease of creating multiple and fake accounts where these are intended to cause harm.
- take steps to understand the age of users and offer age appropriate settings and protections – see principle 7.
- develop in-house or integrate third-party tools that are able to identify, based on previously seen characteristics, the language and behaviours indicative of online grooming and sexual communication with a child. Language based tools will need to be appropriate to the type of communications, for example based on keywords, comments alongside videos or interactions over direct message.
- maximise the effectiveness of these tools, for example through the data they are trained on, the thresholds at which tools flag matches, keeping them up to date to.
- incorporate changing language and offender techniques and ensuring they work for languages other than English.
- ensure account indicators that may act

as a signal for grooming are considered, for example accounts that systematically approach only child users. The presence of CSA material may be another signal, as offenders attempt to exchange indecent imagery with their victim.

- ensure action is taken to help prevent accounts of under 18s advertising sexual availability to adults or other exploitative practices, such as selling indecent imagery or linking to third party sites known to host sexual imagery of minors.
- carry out a human review if necessary, have sufficient trained and vetted moderators to progress user and NGO reports and matches from automated tools, and make provision for the psychological assessment and welfare of staff viewing this distressing material.
- restrict the functionality of geolocation for child users, which may include geolocation sharing being switched off by default.
- on platforms that are likely to be used by children, provide a child-focussed user reporting system that allows grooming instances and accounts to be flagged for urgent review, recognising that many children will not recognise grooming, or may find it difficult to report.
- take steps to encourage user feedback, provide signposting and encourage users to report signs of potential exploitation, such as predatory behaviour.
- close accounts involved in child sexual exploitation and abuse and take steps to prevent individuals re-registering under different details.
- child sexual exploitation and abuse is a crime and a child could be at immediate threat to life or risk of serious harm – report it to the authorities in line with the guidance at section 5.

Case study: Grooming

Evie* was 12-years old when she was groomed by multiple offenders via a live streaming platform. Over the course of an hour, she was filmed in her bedroom and bathroom chatting to people over webcam, revealing her name and age. Initially, the chat was innocuous, and at one point she broke off to speak briefly with a family member passing by the door of her room. However, after about 15 minutes she was coerced into exposing herself to the camera in exchange for "likes" on her profile. At that point, she said over 50 people were viewing the feed. As more people joined Evie was pressured into further sexual acts in order to receive 1,000 "likes" and virtual "coins". The live stream was recorded by one of the offenders viewing the feed and is still in circulation, frequently redistributed in forums dedicated to child sexual abuse material. (Internet Watch Foundation)

*not her real name

Technologies

A grooming detection technique has been developed by Microsoft in collaboration with The Meet Group, Roblox, Kik and Thorn. The technique uses artificial intelligence to analyse patterns in users' speech and language to spot potential grooming conversations by which online predators intending to lure children for sexual purposes can be detected, addressed and reported. The technique is available via Thorn to qualified online service companies that offer a chat function. Thorn is a technology non-profit that builds technology to defend children from sexual abuse.

See the Safety Tech Innovation Network for more information about available safety technologies.

PRINCIPLE 4: Companies seek to identify and combat advertising, recruiting, soliciting, or procuring a child for sexual exploitation or abuse, or organising to do so, take appropriate action under their terms of service, and report to appropriate authorities.

Context: Disrupting preparatory actions such as procuring a child for sexual abuse is one potential intervention that can prevent more serious harm from occurring. These types of actions are often undertaken by offenders seeking to obtain greater access to a child with the intent of committing more serious online or contact offences. They also make it easier for likeminded offenders to work together to enhance individual and collective access to children for the purposes of sexual exploitation and abuse.

Aims of the principle:

Under this principle companies should take reasonable steps to:

- use safety by design approaches to make advertising, recruiting, soliciting, or procurement of a child for sexual services less likely, and deter offenders from these crimes.
- proactively identify, through language or behaviours, individuals engaging in advertising, recruiting, soliciting, or the procurement of a child for sexual services.
- continue innovating towards this goal, recognising that technology is still improving in this area.
- act in the best interest of the child and adult victims of CSEA when considering the safety protections for children and the privacy interests of users in deciding which services to apply these measures across.

Examples of good practice:

When implementing this principle, companies may wish to take steps including:

- develop in-house tools to detect indicators or signals of the recruitment, control, and sale of children for sex based on previously seen characteristics, including text, images, and emojis
- when available leverage third-party tools to cross reference identifiers with online escort/ advertising sites and buyers review boards.
- maximize the effectiveness of these tools, for example through the data they are trained on, the level of certainty at which tools flag matches and which parts of the service automated tools are applied across.
- ensure the indicators that may act as signals for child sex trafficking are considered, which may include:
    - use of prostitution terms/terminology within the accounts of children;
    - indicators appearing in images;
    - use of certain emojis to thwart text identification; and
    - account activity such as those of potential traffickers exerting control over child victims, recruiting and selling child victims and/or buyers negotiating the exchange of something of value for commercial sex with a child;
- carry out a human review if necessary, have

sufficient trained and vetted moderators to progress user and NGO reports and matches from automated tools, and make provision for the psychological assessment and welfare of staff viewing this distressing material.

- recognising the impact of vicarious trauma, ensure there is provision for the welfare of staff viewing this distressing material.
- take steps to address content of children in the older age range (13-17-year olds).
- take steps to remove content related to the promotion of commercial sex with children, including imagery which does not show penetrative sexual activity
- provide a streamlined reporting system for authorised NGOs (such as national hotlines) or trusted organisations to report material and review (if necessary) and take down material immediately when reported by these organisations.
- provide a user / public reporting system that allows suspected recruitment, control, advertising, solicitation, and procurement of children for the purposes of commercial sex materials and accounts to be flagged for urgent review.
- close accounts involved in the commercial sex of children (traffickers / controllers / buyers, not child victims) and take steps to prevent individuals re-registering under different details
- child sexual exploitation and abuse is a crime and a child could be at immediate threat to life or risk of serious harm - report it to the authorities using the guidance at section 5.

PRINCIPLE 5: Companies seek to identify and combat the use of livestreaming services for the purpose of child sexual exploitation and abuse, take appropriate action under their terms of service, and report to appropriate authorities.

Context: Whilst other emerging technologies may be used to commit child sexual exploitation and abuse, livestreaming is particularly complex because it allows offenders to interact with child sexual abuse production in real-time and leave limited evidence. Adult offenders may direct the child abuse whilst the acts are streamed live to an audience of offenders. Alternatively, offenders may entice or coerce children into using livestreaming platforms to produce child sexual abuse material. In some cases, a livestream is captured and distributed.

Aims of the principle:

Under this principle companies should take reasonable steps to:

- use safety by design approaches to make predatory offender-child interactions less likely and to deter offenders from these interactions.
- proactively identify, through language or behaviours, individuals engaging in criminal predatory behaviour such as sexual communication with a child.
- take steps to disrupt the use of livestreaming services by adults to broadcast contact abuse to other offenders, including in return for money.
- continue innovating towards this goal, recognising that technology is still improving in this area.
- act in the best interest of the child and adult victims of CSEA when considering how to balance the safety protections for children and the privacy interests of users in deciding which services to apply these measures across.

Examples of good practice:

When implementing this principle, companies may wish to take steps including:

- implement safety by design measures, for example to limit unsolicited approaches from adults to children and expedite deterrent messaging to adults - see Principle 9.
- take steps to understand the age of users, and to offer age appropriate settings and protections – see principle 7.
- develop in-house or integrate third-party tools that are able to identify, based on previously seen characteristics, the language, behaviour (such as suspicious financial activity) or imagery indicative of child sexual exploitation and abuse in livestreamed content or the user interactions around it. This will be particularly relevant where a platform facilitates the meeting and interaction of adults and children.
- consider whether the use of tools and processes may be needed to flag and address the vulnerability of child broadcasters (for example, underage children, partial nudity even in a legitimate context, or under 18s advertising sexual availability to adults or other exploitative practices) that whilst not necessarily illegal, might expose them to risk of abuse.
- ensure account indicators that may act as a signal for offending over livestream are considered, for example:
    - accounts that systematically approach

only child users;

- spikes in 'likes';
- accounts connecting with known offenders;
- the presence of child sexual abuse material (CSAM) in instant messaging; and
- account/group names that are overtly suggestive of CSAM or sexual interest in children.

- carry out a human review if necessary, have sufficient trained and vetted moderators to progress user and NGO reports and matches from automated tools, and make provision for the psychological assessment and welfare of staff viewing this distressing material.
- prioritise flagged livestreams for review, due to the likelihood there may be abuse or exploitation in progress.
- stop the livestream as soon as CSEA activity or a vulnerable child is identified. Capture any information necessary to help identify the offender and the child.
- where possible, store a copy of the livestream and report this in accordance with local guidelines or legislation.
- if appropriate, take additional action to safeguard vulnerable users. This could include explaining to a child why a livestream has been stopped, providing advice, signposting to support and seeking parental consent.
- provide a child-focussed user reporting system that allows grooming or other inappropriate behaviour and accounts to be flagged for urgent review – recognising that many children will not recognise grooming or may find it difficult to report.
- close accounts involved in child sexual exploitation and abuse and take steps to prevent individuals re-registering under different details.
- ensure action is taken to help prevent accounts of under 18s advertising sexual availability to adults or other exploitative practices, such as selling indecent imagery.
- child sexual exploitation and abuse is a crime and a child could be at risk – report it to the authorities using the guidance at section 5.

Case study: Grooming

Operation BLOOMERIA was an investigation of UK nominals who were present in an online chatroom on 22 July 2015, when the rape of a six-year-old male in the United States was streamed to the group in real time. The investigation involved the use by the NCA and its partners of specialist capabilities to identify offenders. The rape was perpetrated by a man from Pennsylvania, US. He was arrested and has subsequently pleaded guilty to a number of offences relating to this and other conduct. He is likely to serve up to 30 years' imprisonment.

PRINCIPLE 6: Companies seek to prevent search results from surfacing child sexual exploitation and abuse, and seek to prevent automatic suggestions for such activity and material.

Context: Prevention efforts such as addressing the avenues used to access child sexual abuse material are fundamental to ending this abuse. Searching for child sexual exploitation and abuse using related terms gives current or potential offenders an easy way to access child sexual abuse material. Mainstream routes of access to this material normalise the process of seeking it out. Algorithms that suggest child sexual abuse material could have the effect of encouraging or inspiring new offending, as well as increasing re-victimisation of those who are victims of abuse. Providing the user with details of how to report illegal material and, when appropriate and where available, information on interventions for those who are at risk of offending (for example, providing links to support services) is also critical.

This principle is designed to apply to both companies whose services host content and encompass search functionality, as well as search engines which do not host content themselves.

Aims of the principle:

Under this principle companies should take reasonable steps to:

- minimise the potential for search results linking to child sexual exploitation and abuse content or activity, including not allowing predictions (autocompletion) associated with child sexual exploitation and abuse.
- ensure, where possible, that users searching for child sexual exploitation and abuse are warned about the law and potential consequences of their actions, and directed towards alternative sources of information or support.

The way companies apply this Principle and the levels of control that they have will depend on whether the service is a search engine and does not host the content itself, or is a service that hosts the content and has search functionality, which they may not control, built in.

Examples of good practice:

Government is clear that it is the responsibility of companies on whose services CSEA content and activity is hosted to take action. Under this principle however, companies (including both search engines and companies whose services host content and encompass search functionality) should take reasonable steps to:

- ensure search activity for child sexual exploitation and abuse does not promote access to relevant results by ensuring:
  - autocomplete entries do not suggest child sexual exploitation and abuse search terms. This will require that companies maintain an awareness of current CSEA language and terms;
  - further CSEA related content or accounts/profiles are not suggested to users based on previous searches/ interests; and
  - URLs to CSEA content (including imagery and other offender forums, such as those targeting named victims) are demoted or delisted.
- use CSAM hash values to prevent the

indexing of known CSAM. Any URL's identified based on the hashes should be reported (see Section 5).

- signpost users, where possible, to alternative sources of information or support when CSEA search terms are used, such as deterrent messaging and links to services that support potential offenders to change their behaviour.
- use or develop in-house or third-party tools to identify CSEA content and search terms.
- keep lists of terms up to date as they are altered, or new terminology adopted.
- seek to prevent searches for known victims (for example, the name of a series of known images or terms known to be linked with CSA material) from returning illegal imagery.

Example

In just three clicks NCA Investigators found child sexual abuse material (CSAM) via common search engines, showing the lack of barriers to offending on the open web. The sheer volume of CSAM available online creates a permissive environment for offenders to develop a sexual interest in children. It is believed the vast majority of offenders will have begun offending by watching child sexual abuse on the open web.

Technology

The Internet Watch Foundation (IWF) provide a keywords list with over 4,000 words and terms known to be linked to child sexual abuse. This list is continually updated as the IWF's intelligence and proactive searches evolve. The use of the IWF's URL blocking list can also be helpful in assisting companies with and in line with the examples of best practice.

See the Safety Tech Innovation Network for more information about available safety technologies.

Section 2: A specialised approach for children, victims and survivors

PRINCIPLE 7: Companies seek to adopt enhanced safety measures with the aim of protecting children, in particular from peers or adults seeking to engage in harmful sexual activity with children; such measures may include considering whether users are children.

Context: There are identified risks that are unique to children online. These include content risks (which generally position the child as the recipient of unwelcome and inappropriate content), contact risks (where a child participates in risky communication, possibly unwittingly or unwillingly), and conduct risks (where a child's behaviour contributes to risky content or contact within a wider peer-to-peer or adult-to-child network). These risks require taking a considered approach to the safety of users, which may include efforts to understand whether users are children when appropriate and where possible.

Aims of the principle:

Under this principle companies should take reasonable steps to:

- understand the age of their users.
- have safety processes and default settings that are appropriate to the actual age of their users and that make provision for the possibility of underage users.
- recognise that children of different age groups have different needs.

Examples of good practice:

When implementing this principle, companies may wish to take steps including:

- adopt tools or processes at sign up or during platform use that can identify users age or age range, so that appropriate safety settings can be applied[3]. See Appendix 7 for more information about age assurance methods.
- apply default privacy settings, platform functionality and levels of moderation appropriate to children unless the platform design or age confidence outcomes justifies a different setting[4].
- platforms and services designed to be safe for younger children (e.g. applying very high levels of moderation, preventing links to external sites or sharing of contact details etc.) may have less need to identify the age of their

3 The level of certainty required from age confidence outcomes will be influenced by the level of CSA risk the platform or service faces, and the safety measures and features it offers all users by default.

4 Starting with a default high setting and reducing it when age outcomes support this is consistent with the ICO's Age Appropriate Design: a code of practice for online services which at P43 states the 'default position for each individual privacy setting should be privacy enhancing or 'high privacy'. This means that underage user's personal data is only visible or accessible to other users of the service to the extent that the child amends their settings to allow this.'

users.

- provide easy to use parental control options and support (or interoperability with third party services) for parents/carers to have a role in how a child uses the platform, particularly for younger children.
- have clear terms and conditions covering age requirements and take steps to protect younger users on the platform.
- take reasonable steps to make users aware of terms and conditions.
- minimise the risk of children interacting and communicating with user profiles that are dedicated to or advertising adult pornographic material or sexual practices or are on adult dating sites'.
- see the Verification of Children Online report for more information about age assurance.

Example

A social media platform that is popular among young people have integrated an age estimation tool into their platform. Whilst this technology is still improving, the platform is able to use this tool to analyse images to estimate the age of a user. The platform uses this information to provide age-appropriate settings for their users, such as having a separate community for under 18s (no adults are allowed in) and requiring parental consent for users under 18 to create an account.

Statistic

In 2019 Ofcom, research highlighted that a significant proportion of primary school-age children have their own social media profile, despite the minimum age often being set at 13. Twenty five percent of ten-year-olds who go online claim to have a profile, with this proportion almost doubling to 43% of 11-year-olds.

PRINCIPLE 8: Companies seek to take appropriate action, including providing reporting options, on material that may not be illegal on its face, but with appropriate context and confirmation may be connected to child sexual exploitation and abuse.

Context: Material depicting child sexual exploitation and abuse is illegal. However, certain images, videos, discussions and other recordings may fall below this threshold but still warrant action. Appropriate context and confirmation are required to demonstrate that material in the following and other relevant examples is connected to child sexual exploitation and abuse:

- self-generated materials,
- materials that form part of an abuse series (and may show content directly before or after the abuse occurred),
- discussions relating to victims depicted in child sexual abuse material (including where offenders are discussing non-illegal imagery of a victim as a child or an adult), and
- otherwise innocent materials that have been misappropriated and used in connection with child sexual exploitation and abuse.

Identifying and taking appropriate action on this material can reduce new and ongoing opportunities for victimisation. For example, self-generated images can indicate a child is being groomed and coerced into producing images, or can be shared beyond the original recipient causing significant distress to the child.

Aims of the principle:

Under this principle companies should take reasonable steps to:

- proactively identify material linked to child sexual exploitation and abuse where indicators or data sets are available. This material may include images, videos and text-based conversations. See Appendix 8 for examples of this type of content.
- where material cannot be identified until after it is uploaded, remove it and take all appropriate and feasible steps to prevent it being made available to other users in future.
- consider the role of users, NGOs and victims in reporting material linked to child sexual exploitation and abuse on their platform.

Examples of good practice:

When implementing this principle, companies may wish to take steps including:

- make use of reference lists of known legal images that are linked to CSEA that have been verified by an authorised body such as an NGO. For example, the NGO may have information available to them to confirm age, or that the image is taken from an abuse video, even though this cannot be seen from the image alone. Where possible, these images should be removed and blocked from future upload or circulation.
- proactively identify material that may not be visibly illegal but is linked to CSEA where indicators are available. For example, offender comments alongside legal videos of children, offenders discussing or pursuing named victims or offenders advertising availability of material that is hosted elsewhere.
- provide reporting routes for victims (children and adults who were abused/exploited as children) or connect victims with reporting routes provided by NGOs so that images that may not be visibly illegal can be removed and blocked from future upload/circulation. This includes the legal Right to be Forgotten.

- children may produce images that do not meet the definition of an 'indecent image' so are not illegal but could be harmful to the child because of the risk of wider circulation or the image being picked up by an offender. When requested by the child in the image, steps should be taken to remove and prevent future circulation of these images.
- where material is not illegal, reporting to authorities is not required but associated illegal CSEA activity should be reported. Where information is available that might differentiate between consensual self-produced indecent imagery and grooming, this should be included in any report to assist law enforcement.

Case study: Report Remove

The IWF, in partnership with the NSPCC's Childline, have developed "Report Remove", a unique reporting portal for children to anonymously report sexual imagery of themselves which they are concerned may be subject to wider distribution. By creating a Childline account, children can verify they are under 18 using the Yoti app, then report URLs, images or videos to the IWF. Imagery assessed as illegal is hashed and shared with tech companies, while the NSPCC via Childline supports the child.

Taking a child-centered approach, the solution aims to ensure that children aren't criminalised for "taking and distributing indecent images of children". To address this concern, the IWF/NSPCC worked with NCA CEOP, Home Office, GCHQ, National Police Chiefs' Council (NPCC) and NCMEC to implement a process to identify that the imagery had been reported by a young person via the Report Remove platform to enable the case to be handled appropriately in accordance with national guidelines.

The project is currently in pilot phase and a full launch is currently anticipated to take place in 2021.

Statistic

In 2019, the Internet Watch Foundation found that a third of all reports it confirmed as containing child sexual abuse were of self-generated indecent images of children. Of those, 76% showed a young girl in the 11-13 age range. This is a trend that the Internet Watch Foundation has continued to see rising in 2020, with them confirming that 44% of everything they have acted upon in 2020, contained self-generated content.

Example

Content that may not visibly illegal but is connected to child sexual abuse and exploitation includes 'where are they now' threads. These threads are created for the purpose of posting about a specific victim/survivor. This includes posts in which offenders discuss the abuse history, the victim's current whereabouts, post or link to legal and illegal imagery, links to the victim's social media pages, personal/identifying information, and links to sites that act as archives for previously available websites posting about the victim. In some instances, survivors are being located online which presents significant personal safety risks. The Canadian Centre for Child Protection's victims' group, the Phoenix 11, will only speak under anonymity for this reason.

Section 3: Collaboration

PRINCIPLE 9: Companies seek to take an informed global approach to combating online child sexual exploitation and abuse and to take into account the evolving threat landscape as part of their design and development processes.

Context: Criminal means and methods evolve quickly as offenders exploit new technology to commit online child sexual exploitation and abuse. To respond effectively to the evolving threat and changing behaviours, companies should seek to design their products with child safety in mind. This includes routinely reviewing efforts to tackle child sexual exploitation and abuse, adapting internal processes and technology, participating in multi-stakeholder processes to keep up to date with the threat landscape, collaborating across industry and considering the privacy interests of their users alongside safety protections for children.

Aims of the principle:

Under this principle companies should take reasonable steps to:

- keep up to date with the threat, sharing trends where possible.
- adapt safety processes as the threat changes.
- implement safety by design measures to reduce the risks incurred by child users and reduce the attractiveness of the platform to offenders.
- consider safety alongside privacy in product design, including the potential impact on safety in the wider online ecosystem.
- ensure that new implementations do not degrade existing processes and tools to combat online child sexual exploitation and abuse.

Examples of good practice:

When implementing this principle, companies may wish to take steps including:

- analyse own data and work in partnership with government, law enforcement, survivors of CSEA and NGOs to identify and share new CSEA risks, trends and indicators.
- review their existing response, including any CSEA cases known to have bypassed safety measures, on a regular basis.
- continue to innovate to develop new approaches to understand risk and improve safety.
- assess the safety risks of any new products or design changes, to own users and victims of abuse, including safety impacts on the wider online ecosystem, and take steps to mitigate those risks.
- some risks can be reduced through service/ platform design and user options and defaults, preventing offending rather than detecting and reporting it once it occurs.

- educate users about online safety and Online Safety, and the options available to them. Evaluate the impact and consider where messaging needs to be refined.
- implement stronger account verification, to deter offenders, for example, requiring a user's phone number or verified photograph, and taking steps to prevent banned users re-registering.

The Australian e-Safety Commissioner has Safety by Design guidance. Government will publish Safety by Design guidance by March 2021.

Case study

A dating site has been rolling out photo verification since January. This has a number of benefits in addition to deterring CSEA offenders, such as helping to ensure that catfishers, scammers and users under the age of 18 are not present on their platforms.

Example: 'Risky-by-Design'

Research by the 5Rights Foundation highlights how certain design features within platforms create risks for children. For example, 'hobbies, interests, and other factors are used by the friend suggestion systems to match users. A recent investigation found that adult predators adopting similar interests to children were being steered towards children's accounts, including those as young as 11, on popular social media platforms.' See the Risky By Design website.

Example: Project Protect

The Tech Coalition's membership is made up of 18 technology companies, large and small. They have recently announced Project Protect, which commits the members to high-impact information, expertise and knowledge sharing across the industry to disrupt and help prevent online CSEA.

PRINCIPLE 10: Companies support opportunities to share relevant expertise, helpful practices, data and tools where appropriate and feasible.

Context: Companies have been working together, sharing helpful practices, data, tools and techniques for many years via a range of collaborative forums and non-governmental organisations. Companies plan to continue to expand this collaborative work, sharing outcomes and outputs across the technology sector.

Aims of the principle:

Under this principle companies should take reasonable steps to:

- share expertise and best practice, including with smaller companies.
- make tools available to other companies and NGOs.
- share relevant data sets where possible.

Examples of good practice:

When implementing this principle, companies may wish to take steps including:

- active membership of industry groups to enable information and expertise sharing.
- proactively sharing technologies and tools particularly with smaller companies, to improve industry-wide capability to respond to online CSEA.
- share data sets where possible and within data protection principles, for example training data, image and video hashes, or other identifiers to enable CSEA to be detected as it moves across platforms (see Appendix 2 for data protection considerations).
- consider the potential for technology and data approaches to be compatible across platforms, to improve the overall response.
- work across sectors where others may have relevant expertise.

PRINCIPLE 11: Companies seek to regularly publish or share meaningful data and insights on their efforts to combat child sexual exploitation and abuse.

Context: Regular and transparent reporting will improve available data about the production, distribution, blocking and removal of child sexual exploitation and abuse. Combined with data from governments and non-governmental organisations, this will result in a better understanding of the threat and provide support for ongoing initiatives to combat this crime. Reporting will also ensure cooperative efforts between governments, law enforcement agencies, companies and other stakeholders are focussed on areas of greatest need.

High volumes of CSEA reports can indicate more proactive work being done by companies as well as the possibility of more offending, so transparency of the steps being taken to address the problem are also important.

The government established a multi-stakeholder Transparency Working Group, chaired by the Minister for Digital and Culture, which included representatives from industry and civil society. The objective of this group was to bring together a wide range of stakeholders to discuss transparency reporting and to build consensus on what transparency reporting should look like. The group fed into the Government Report on Transparency Reporting in relation to Online Harms, which was published alongside the Full Government Response.

Section 4: User reporting

PRINCIPLE 12: Companies seek to implement effective user reporting, complaints and timely redress processes to ensure users are empowered and protected.

Aims of the principle:

Under this principle companies should take reasonable steps to:

- have appropriate, clear and easily accessible reporting processes for users of all ages.
- signpost users who have accessed or attempted to access CSEA content to appropriate help and support.
- ensure users or persons affected by content or activity on a platform have an effective and accessible complaints function for both concerns about harmful content or activity.
- have appropriate redress/appeal functions for users who have had their content removed.
- have processes in place to ensure that the most serious user reports are prioritised, such as child sexual exploitation and abuse, so that action can be taken quickly.

Examples of good practice:

When implementing this principle, companies may wish to take steps including:

- ensure there are clear and accessible reporting functions for users if they discover CSEA content or activity within a platform or service.
- ensure that the reporting mechanisms are clear, easy to use, and provide sufficient granularity of information to allow a company and law enforcement to prioritise and act promptly upon notification of CSEA content or activity.
- as far as practicable, ensure users receive timely, clear and transparent responses to their reports on CSEA content or activity, and are informed about decisions taken based on their report to a level which would not benefit any bad actor.
- ensure users who have been exposed to CSEA content on a platform or service are directed to appropriate help and support.
- enable users who have posted content that is subject to a complaint to appeal any decision by the provider. Where this has been verified as CSEA there is no prospect of appeal.
- ensure that user redress, complaints and reporting functions are resourced to provide an effective response, and that any correspondence includes appropriate coverage of user rights to challenge actions taken.
- there may be certain circumstances where the appropriate reporting process is through an NGO, for example, if the company doesn't host the CSEA content.

- encouraging public reporting by ensuring tools are easy to use, prominently placed on the platform, and that their existence is communicated to users.
- ensuring initial acknowledgement and eventual response are timely, and where practicable that the user receives relevant information about any actions taken.

Case study

A popular search engine provides a process for users to report images on both their desktop and mobile versions of the site. It is easy for users to locate where to report and how to flag concerns. Once users have selected that they want to report the content, they are offered four options for the type of content they are reporting, which includes 'child sexual abuse'.

Section 5: Law Enforcement/ Reporting To Appropriate Authorities

PRINCIPLES 1-5 reference the need to report child sexual exploitation and abuse to appropriate authorities, which may include law enforcement.

Context: Online child sexual exploitation and abuse is a crime and it is important it is reported. Behind every image or instance of grooming is a victim that could be subject to ongoing abuse. Reporting allows victims to be identified and offenders apprehended, removing children from abusive situations.

For companies based in the United States of America, reporting is mandated via the National Center for Missing and Exploited Children (NCMEC). Companies based in the UK are encouraged to report voluntarily (see Appendix 6). In other jurisdictions, different reporting frameworks will apply (whether under law or as otherwise arranged). All reporting to authorities must be compliant with applicable legislative frameworks.

Aims of the principle:

Under this principle companies should take reasonable steps to:

- expeditiously report information about all instances of suspected online CSEA offending which involves a suspected victim or offender. This process will vary depending upon where your company is based, as set out in Appendix 6.
- ensure that all necessary and available information is included in the report, to ensure it is actionable. Prioritise the protection of children by reporting any available associated data that may help in the identification of victims and offenders (see Appendix 6). Whilst there is no legal requirement to report CSEA within the UK, this can be done voluntarily in alignment with the GDPR - see Appendix 2;
- retain all data related to the offence, in accordance with national data protection legislation, so that it can be provided if lawfully requested by UK law enforcement.

Examples of good practice:

When implementing this principle, companies may wish to take steps including:

- Use existing mechanisms for informing law enforcement of imminent threats to life or risk of serious harm, including making an emergency telephone call (999 within the UK). Larger companies may already have specific arrangements in place with law enforcement for reporting content, which should continue to be used.
- report all instances of child sexual abuse material, grooming, offender activity such as the commissioning of abuse and other CSEA offences to relevant authorities. These reports enable global law enforcement to quickly apprehend offenders and safeguard victims from further abuse, providing sufficient information is included:
    - UK companies should report to their local law enforcement;

    - US based companies are required to make a report to NCMEC; and
    - companies outside the UK and US should report to their local law enforcement or other available routes.
- retain any material relating to reports made to authorities for a minimum of 90 days. This will ensure material needed for evidential purposes to bring offenders to justice is retained and available when law enforcement submit an MLAT or other lawful request for access to data held by a company. The current retention period for US companies (USC 2258A) is 90 days. Law enforcement may make requests to preserve data for a longer period, on a case by case basis.
- Detailed guidance on reporting is in Appendix 6.

Appendix 1: DEFINITIONS

<table>
<tr><th>Term</th><th>Definition</th></tr>
<tr><td>Age assurance</td><td>Age assurance is the broad term given to the spectrum of methods that can be used to assure a user's age online. Age assurance allows companies and users to jointly choose from a range of measures that are appropriate to the specific risks posed and their service needs. The selected methods may rely on different sources of data, which may have different privacy implications and cost models.</td></tr>
<tr><td>Age Verification</td><td>Age verification is a form of age assurance where a user's age is established through a full identity verification process to a high level of confidence. Currently, age verification is most commonly used to help businesses meet legislative requirements concerning age-restricted products and services by restricting access to users who cannot provide officially held evidence (e.g. passport or driving licence) that they are over 18 years of age.</td></tr>
<tr><td>Child</td><td>Anyone under the age of 18 in accordance with the UN Convention on the Rights of the Child. In the context of child sexual abuse material, NGOs, law enforcement or companies may confirm whether the material contains a child. When the age is confirmed by a law enforcement body or an NGO that provides a hash list for user-generated content an NGO or law enforcement body that supplies a known CSA-related UGC hash set, further assessment by the company is not required. Alternatively, the material may be assessed by the company itself, but assessments should not require total certainty the child is under eighteen years of age for action to be taken.</td></tr>
<tr><td>CSA facilitated by livestreaming</td><td>Covers the offending types of production/sharing of CSAM, grooming and incitement of sexual abuse. The use of livestreaming technology to commit these offences may require a different response due to the likely presence of a current, real time victim and the need to ensure data is retained.</td></tr>
<tr><td>CSA imagery (including video and still images)</td><td>Defined by the UK sentencing council as follows, and for the purposes of this Code should include all three categories A-C. Category C would include images that show erotic poses without sexual activity, but not include images that show nudity in a legitimate setting.
<table>
<tr><th>Category</th><th>Description</th></tr>
<tr><td>A</td><td>Images involving penetrative sexual activity; images involving sexual activity with an animal or sadism.</td></tr>
<tr><td>B</td><td>Images involving non-penetrative sexual activity.</td></tr>
<tr><td>C</td><td>Other indecent images not falling within categories A or B.</td></tr>
</table>
</td></tr>
</table>

Term	Definition
Grooming (UK legal threshold)	Sexual Offences Act 2003: Sexual communication with a child is included in this Act (Section 15A) and states that it is an offence for a person over the age of 18 to intentionally communicate with another person under the age of 16 for the purpose of obtaining sexual gratification if the communication (written, verbal or in picture form and can be sent in person, by phone, internet, or by other means such as a gaming device) is sexual or if the adult encourages the minor to make a sexual communication. Offenders face up to two years in prison and a place on the sex offenders register if they carry out an offence under Section 15A. It is also an offence under this Act to meet a child following online sexual grooming (Section 15) and this can carry a much longer prison sentence.
Grooming (US definition for NCMEC reports)	In the US, the CyberTipline Modernization Act already facilitates CSA reporting to NCMEC for 'imminent or planned violations' and provides an opportunity for intervention before further harm to a child. Companies may apply their own judgement to reporting these cases in addition to those meeting the UK legal threshold above.
Online Child Sexual Exploitation and Abuse (CSEA)	When child sex offenders view and share child sexual abuse material (CSAM) online, groom children online, and live stream the sexual abuse of children. See Appendix 5 for a list of grooming and other related offences.
Prohibited image of a child	These images include non-photographic images of child sexual abuse, such as Anime, but do not include "indecent photographs", or "indecent pseudo-photographs", of a child. The possession of a "prohibited image of a child" is an offence under Section 62 of the Coroners and Justice Act 2009.
Pseudo photograph of a child	This covers photographs (including moving images) and images made, for example, on a computer but which look like real photographs. This can include photos, videos, tracings and derivatives of a photograph and data that can be converted into a photograph. The possession of 'pseudo-photographs of children' is an offence under Section 69 of the Coroners and Justice Act 2009.
Self-generated indecent images (SGII)	Indecent images, including nude or semi-nude photographs, that a child takes of themselves and then sends or posts via mobile phones or over the Internet. A child (under 18) may be coerced into taking and sharing these images or may share them consensually with a peer.

Appendix 2: CSEA and UK data protection rules

Companies must ensure that any action taken to tackle CSEA, as outlined in this Code, is done in accordance with national data protection legislation and guidance. In the UK, this includes the General Data Protection Regulation (GDPR), which is supported and augmented by the Data Protection Act 2018, and the Age Appropriate Design Code.

All aspects of the GDPR and Data Protection Act apply, not just the aspects highlighted below.

Under the GDPR, companies should not share or process personal data unless they have a fair and lawful reason to do so, taking account of the best interests of the child. The Age Appropriate Design Code states that '[o]ne clear example of a compelling reason [to share or process personal data] is for safeguarding purposes, preventing child sexual exploitation and abuse online, or for the purposes of preventing or detecting crimes against children such as online grooming.' Even in these circumstances, careful consideration still needs to be given to all other aspects of GDPR compliance.

For further information, see the guidance on children and the GDPR and the Age Appropriate Design Code from the Information Commissioner's Office.

Identifying and combatting CSEA

Companies may process personal data when taking steps to identify and combat CSEA. For example, an offender's email address to stop them re-registering for a site once banned, or users' ages to protect children from inappropriate interactions with adults (for example, identifying that an adult is sending multiple friend requests or predatory messages to children). There may even be circumstances where the names of victims in well-known and publicly available abuse material can be processed for the purpose of identifying and removing offender forums that discuss the abuse.

Where automated technology that searches communications to identify CSEA is used, a company's privacy notice should make this clear to users.

Great care needs to be given to the rights of an individual under the General Data Protection Regulation when processing any type of personal data, which includes any data or information about a victim of CSEA. Any data or information about a victim (even if publicly available) must be handled extremely sensitively. This includes considering and putting in place processes to ensure personal data is stored in a secure way and only shared where this is necessary and appropriate.

Key Articles of the GDPR to consider include:

- Article 6 – Lawfulness of processing
- Article 9 – Processing of special categories of personal data
- Article 10 - Processing of personal data relating to criminal convictions and offences

Reporting CSEA

UK data protection law is not a barrier to reporting CSEA, but companies must share and process personal data within the GDPR framework.

Reporting CSEA that relates to UK users of a service to law enforcement or relevant authorities requires the sharing of identifying information about victims and offenders. The data that companies report (see Appendix 6) is personal data and the GDPR therefore applies. As the information relates to potential sexual offences, it is highly likely to contain special category personal data and/or criminal offence data, in which case additional requirements of the GDPR will apply.

As set out above, UK legislation permits the sharing of personal data for safeguarding and law enforcement purposes. When doing so, any data or information about a victim must be handled extremely sensitively. This includes considering and putting in place processes to ensure personal data is stored in a secure way and shared in a way that is lawful and compliant (i.e. where necessary for safeguarding or law enforcement purpose).

When assessing what data should be shared, companies should consider what is in the best interest of the child. Personal data should not be collected on the basis that it might be useful, and companies should consider whether they are being consistent with the principle of data minimisation. However, there may be instances where companies share information beyond that which is recommended or required as this could aid in the identification, and therefore safeguarding, of a victim of CSEA.

Some information about offenders, or alleged offenders, will need to be retained to help in the identification and investigation of offending. Only data relating to suspicious activity should be retained and subject to human intervention as required and there should be prompt disposal of data which doesn't show illegality. Appropriate retention and data disposal policies will be required here. Companies should also make due provision for the rights of adults accused maliciously, or mistakenly.

Right to be forgotten

GDPR gives individuals the right to have personal data erased (Article 17). This is also known as the 'right to erasure' or the 'right to be forgotten'. There is emphasis on this right if the request to erasure relates to data collected from children, due to their enhanced protections under the GDPR.

Guidance from the ICO explains: 'If you process data collected from children, you should give particular weight to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet.'

Appendix 3: Background to the threat

CSEA threat

The scale and severity of the threat of online child sexual exploitation and abuse is significant and growing. The National Crime Agency (NCA) estimate that there are a minimum of 300,000 individuals in the UK who pose a sexual threat to children, either through contact abuse or online[5]. In the year ending March 2020, there were over 7,200 arrests and over 8,300 children safeguarded or protected in relation to online CSEA in the UK[6], including as a result of industry reporting. Online CSEA can take various forms, and the threat continues to evolve.

5 *The estimate of 300,000 UK offenders is a minimum and is supported by data from various sources. They include the number of offenders on dark web sites, registered sex offenders, estimates in the Crime Survey of England and Wales, police recorded crime statistics, the scale of child sexual abuse material hosted online and 94,342 UK residents in 2019 contacting the Lucy Faithfull Foundation for themselves or someone close to them who was sexually attracted to children*

6 *Based on Management Information, which has not undergone quality assurance.*

Child sexual abuse material (CSAM)

Technological developments, data sharing and increased awareness have helped to facilitate a substantial increase in the number of reports made by companies of child sexual abuse material (CSAM). In 2019, NCMEC received 16.8 million referrals, containing nearly 70 million images, from US companies. This is compared to just one million in 2014. From its launch in 2017 to November 2019, Project Arachnid, owned by the Canadian Centre for Child Protection, has triggered over 13 million suspicious images to be reviewed by analysts, resulting in 4.6 million takedown notices being sent to providers. The Internet Watch Foundation (IWF) is the UK hotline for CSAM. They receive and process reports of suspected CSAM from the public, police forces and other international hotlines, as well as proactively searching the web for this material. In 2019, they assessed nearly 132,700 websites that they confirmed as containing CSAM - a 26% increase from 2018. Ninety-four percent of these images contain children under 13 years old, and 39% contain children under 11.

Other technologies and services are making the detection of images and those sharing them more difficult. This includes end-to-end encryption, which significantly hinders or prevents companies from detecting CSAM. The dark web also provides detection challenges for law enforcement. The UK's NCA has identified 3.45 million global registered accounts across just the ten most harmful CSAM sites on the Dark Web.

CSAM creates a permanent record of a child's abuse. Research has found that the children in these images experience ongoing trauma through the knowledge that images of their abuse are available online to be viewed over and again, making the removal of known CSAM crucial. The Canadian Centre for Child Protection found that 70% of victims feared being recognised as a result of their image being viewed online – and 30% had been recognised in real life by a stranger. The quick identification and reporting of unknown CSAM is also vital, as this likely suggests that a child is currently experiencing abuse.

This is not just about removing material – in the UK, it is estimated that every month law enforcement is making over 700 arrests and safeguarding or protecting over 900 children as a result of these referrals and other intelligence led operational activity.

Online grooming

This is when digital technology is used to communicate with a child with the intention of coercing or enticing the child to engage in sexual behaviour. This may lead to contact offending or could occur solely online.

Initial contact with the child is commonly made on social media sites, online gaming platforms, chat rooms and sites targeting children. Offenders may then encourage children onto other, more private platforms. The scale of online grooming is unknown, as many children do not report it, either through fear or because they do not recognise what's happening to them as abuse. Police recorded crime figures for offences recorded under Sections 15 and 15A of the Sexual Offences Act 2003, show there were 5,116 in 2019, an increase of 11% from 2018.

Offending may result in a physical meeting but often remains online, with abuse occurring through coercing the child to share sexual imagery or livestream themselves. The impact of online grooming on children can include behavioural problems, eating disorders, depression, low self-esteem and post-traumatic stress disorder. These affects may be experienced regardless of whether the grooming included contact abuse or was online.

See Appendix 5 for further guidance on online grooming.

Livestreaming

Livestreaming technologies enable the sharing and viewing of videos of child sexual abuse with a perceived reduced risk of detection. Livestreams may be pre-recorded videos of abuse that are later livestreamed for an audience of offenders. Offenders may entice children into using livestreaming platforms to self-generate CSAM.

Livestreaming platforms may also be used by offenders to direct child abuse in real time. The livestreaming of abuse often involves victims based in low-income countries, with offenders paying to view and direct the abuse from other parts of the world. This is also referred to as cybersex trafficking or live distant child sexual abuse. The Philippines

is a known hotspot for livestreaming and receives 3,000 reports of suspected cases of online CSE from overseas every month.

Offender groups (sharing tips, normalising the behaviour etc)

There has been an emergence of offender communities sharing not only images, but also tips and information on how to groom children and how to stay hidden from law enforcement. On both the open and dark web, offenders discuss their interests, send illegal images, and share information about how to carry out abuse and give tips on which platforms are 'best' for targeting children. There is evidence that online communities of offenders help to normalise offending behaviour and encourage greater levels of abuse and the targeting of younger children to win status within these communities. However, offenders are not a homogenous group, and more research is needed to understand the breadth of behaviours, motivations and the factors that facilitate their offending.

Self-Generated Indecent Images

Self-generated indecent images (SGII), also referred to as youth-produced sexual imagery, are indecent images, including nude or semi-nude photographs, that a child takes of themselves. A child (under 18) may then send or post these images via mobile phones or over the Internet. This may be the result of coercion or a child may share them consensually with a peer. In either scenario the images may later be shared more widely, either by peers without the victim's consent or by offenders and distributed to those with a sexual interest in children.

In all circumstances, it is illegal to make, possess and distribute any imagery of someone under 18 which is 'indecent', including where an under 18 has sexual imagery of themselves. Where there has been consensual sharing between children, the incident will be listed as a crime but Outcome 21 and NPCC guidance state that it should primarily be treated as a safeguarding concern and not as a criminal offence. However, in some cases of child to child sharing of indecent images, outcome 21 might not be appropriate, for example, if there is a big age difference between the children or there was any suggestion of coercion.

Youth-produced sexual imagery should be reported to law enforcement, who will develop a coordinated and proportionate response. There is a need for more education for young people and adults about what is and is not illegal.

From January to November 2020, 138,000 reports sent to the IWF were confirmed to contain child sexual abuse imagery, which was then removed, compared to 132,730 in all of 2019. In the first six months of 2020, 44% of all the child sexual abuse content the IWF dealt with involved images filmed by the victims themselves, up from 29% in 2019.

Appendix 4: Small and medium sized enterprises (SMEs)

The principles in this code are intended to be applied on a risk-based and proportionate basis and not all of the principles will apply to every company. SMEs may not know how to apply this code to their services and are likely to have less capacity and resources to safeguard their services and therefore may not be able to take the same measures as large companies. However, evidence shows that those targeting children exploit services of all sizes and varying functionalities, and we therefore expect companies to do everything they can to identify and combat CSEA, whether they are a start-up or an international corporation.

This Appendix aims to provide advice on this topic and encourages SMEs to consider how services and users can best be protected using available resources.

Companies are encouraged to identify which of the principles in this code apply to them, and to use their discretion to consider which of the recommended measures they can take to meet each relevant Principle.

The minimum measures outlined below propose a basic framework of measures that any company (including SMEs) might implement to meet minimum expectations under this interim code. This is not prescriptive and companies are encouraged to do as much as they can to identify and combat CSEA.

Harms and risk factors to consider

It is vital that SMEs reflect upon potential harms on their services, and (as the experts on the functionality of their platform) potential, practicable measures to mitigate the risks these harms create. These harms could include, but are not limited to:

- the sharing and posting of child sexual abuse images and videos;
- online grooming, whereby children are coerced or enticed to engage in sexual behaviour;
- the livestreaming of child sexual abuse;
- commercial sexual exploitation of children online.

The following questions will help ascertain key risk aggravating factors (this is not an exhaustive list). Do your services:

- allow users to create, share, promote, repost or share sentiment on any type of content?
- offer private messaging spaces (both in access-controlled groups and as 1-to-1 messages)?
- offer ephemeral, encrypted or self-deleting content?
- use end-to-end encryption to place user content out of reach of provider moderation systems?
- offer features that enable exchange of rich media including video (stored and livestreamed), audio, images, link sharing (including via URL shortening services), virtual reality, location sharing and contact details on other platforms or services?
- offer user profiles that facilitate adults finding and contacting children and that may enable real-world identification of vulnerable people, including children?

Examples of measures that can be taken by companies of any size to mitigate potential CSEA:

- offer prominent and accessible user reporting mechanisms for content or behaviour that a user is concerned about and have a mechanism in place to action this swiftly. This may include fast-track responses to user reporting on the most harmful types of content, such as CSEA.
- dedicated human review of select forms of child sexual abuse material.
- gaining access to low/no-cost knowledge, practical support and tools (e.g. automated moderation and detection of CSEA) from existing cross-industry groups or NGOs, such as the Internet Watch Foundation. For more information about safety technology companies see the Directory of UK Safety Tech Providers and the Safety Tech Innovation Network website.
- signposting users to the IWF's online reporting tool for child sexual abuse material and encouraging them to report to law enforcement where a child is at immediate risk.
- publication of clear and accessible terms and conditions, which should describe what the company considers to be acceptable content and behaviour on their services, including specific reference to child users.
- publication of clear privacy notices, including information about where material may be reviewed or analysed by automated processes and by human review.
- state in a clear and accessible way the sanctions for any failures to comply with terms and conditions, for example, that the provider will remove identified content, suspend, close or otherwise restrict user accounts, make reports to UK or international law enforcement where this is justified or required.

ensure services are as safe by design as practicable (please see Part 5 in the Full Government Response and the Australian e-Safety Commissioner's Safety by Design guidance).

- apply the sanction framework in a consistent and transparent way.
- implement measures that will prevent or deter adults from making unsolicited contact with children.

One Stop Shop for Companies on Protecting Children Online

In Spring 2021 the government will publish a 'One Stop Shop' with practical guidance for companies on how to protect children online. It will be designed as an interim tool to support businesses ahead of the regulatory framework.

The One Stop Shop will support smaller companies in particular, providing practical advice to help them better understand child Online Safety and their existing legal requirements.

Appendix 5: Online grooming guidance

Similar and related terms:

- **The solicitation of children for sexual purposes** – the only definitions of this are in the Lanzarote Convention and EU Directive 2011/93. In both cases it is defined as meeting or attempting to meet a child, and does not consider that such solicitation may occur solely online.
- **Child sexual exploitation (CSE)** - Child sexual exploitation is a form of child sexual abuse. It occurs where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity (a) in exchange for something the victim needs or wants, and/or (b) for the financial advantage or increased status of the perpetrator or facilitator.
- **Online or technology-assisted child sexual exploitation** – where a CSE offence occurs solely or partly on digital technologies.

Definition of online grooming

When digital technology is used to communicate with a child with the intention of coercing or enticing the child to engage in sexual behaviour. This may lead to contact offending or could occur solely online. Online grooming can happen through one-off contact or over a longer period. The offender may be an unknown adult who the child has met online, they could be an adult that is known to the child offline but uses technology to communicate with the child, or they could be another child (peer-to-peer grooming) who may or may not be known to the child offline.

The act of an adult offender attempting to groom, can severely affect a child. Unfortunately grooming will often take place in the pursuit of facilitating further crimes against children, such as sexual assault, rape, and the creation of indecent images of children. Successfully detecting or preventing grooming, prevents offenders from further hurting children.

Online grooming may include the following behaviours:

- emotional manipulation, including the use of compliments and flattery so the child believes themselves to be in a relationship with the offender, or seeking to emotionally detach the child from their friends of family;
- building trust and rapport with the child and the child's family;
- targeting particularly vulnerable children, such as those experiencing social isolation, a lack of adult supervision, mental health problems or eating disorders. The fault is never the child's, but the offenders who target online spaces where such children are known to be;
- coercing children into sharing sexual images, videos or live streams of themselves;
- blackmailing children through intimidation and threatening to share sexual images of them unless the child sends them more;
- sending sexual messages to children, which could include explicit language, pornography and requests for sexual images, videos or live streams;
- moving children from public to private platforms; and
- arranging to meet a child in person with the intention of committing contact sexual abuse.

Stages of online grooming

- Online grooming may involve some, or all, of the following stages. These stages may happen quickly through one-off contact, or over time through a series of interactions. These stages do not necessarily happen in a linear way, but may be cyclical as offenders start, stop and re-start different behaviours. When grooming a child, an offender may commit one or several offences (see Section 3), depending on which of these four stages are present.

1. **Initial contact**
   Public platforms, including social media, online games, dating sites and chat rooms may be used to make initial contact with a child. Offenders may then move the communication onto a more private service with a perceived lower risk of detection. Fake accounts may be used to make children think the offender is a child. They may target children that appear unpopular or have low self-esteem. Initial contact may also occur offline or the child may already know the offender, and then a public platform may be used to initiate an online relationship with the child.
2. **Relationship and trust building**
   Offenders use various techniques to build trust and to make the child believe they are in a relationship. Offenders are known to target children who are perceived as or are particularly vulnerable, and who may therefore respond more positively to their attention.
3. **Sexual communication and image sharing**
   The offender will introduce sexual themes into the conversation. This may follow a period of building trust with the child, or sexual content may be introduced almost immediately. This will normalise sexual behaviour and gives the offender increasing control over the child. If the offender succeeds in manipulating the child into sharing sexual content, the child is then at risk of further harm and threats.
4. **Coercion and blackmail**
   An offender may then use sexual content that the child has shared with them to blackmail the child. This could include threats to share

the child's sexual images or videos unless the child sends the offender more sexual content.

Stages 1 and 2 are preparatory stages, and do not constitute an offence unless they result in sexual communication or enticement. The preparatory stages would still constitute suspicious behaviour and should be cause for further investigation. Stage 2 may occur later to sustain the contact, or the offender may cease to communicate with the child once they have committed the offence of sexual communication with a child.

Detecting and reporting online grooming

This is a non-exhaustive list and companies should continually look to develop and expand the steps they take to identify online grooming.

Companies should take their own appropriate action in relation to accounts that are acting suspiciously. Indicators of suspicious activity could include:

- an adult sending multiple messages or friend request to children;
- an adult that joins online groups or chats that are known to be used by children;
- adults posting comments on children's livestreams or other content that could be indicative of grooming;
- adults encouraging children to move conversations into private channels;
- multiple accounts being set up from one device, particularly in different names or different ages with the intention of causing harm. This could be a family using the same platform on one device, but it's likely to be offending behaviour, and could be a flag for further monitoring;
- VPN and Tor use, particularly at the point of account set-up.
- companies should report online grooming where they have evidence that an offence has taken place. See Section 4 for the full list of grooming and related offences. This could include:
    - an adult sending a sexual message to a child, which could include written messages, images, videos and livestreams; and
    - an adult enticing a child to send indecent or sexual content, including images.
- Companies should monitor (or prevent) anyone that is blocked for violating their terms and tries to resign up.
- If you detect suspected online grooming, you should report this to the relevant body or law enforcement agency. See Appendix 6 for more information.

Online grooming and related offences

- Communications Act 2003: Section 127 – offence to send an electronic message by means of a public electronic communications network that is grossly offensive or of an indecent, obscene or menacing character. This offence has a maximum penalty, on summary conviction, of six months.
- Coroners and Justice Act 2009: Section 62 – offence to be in possession of a prohibited image of a child, which is an image that is pornographic, 'grossly offensive, disgusting or otherwise of an obscene character', focus on the child's genitals anal region or portray sexual acts. An image may not be pornographic if it cannot be assumed to have been produced solely or principally for the purpose of arousal. The offence has a maximum penalty of three years and/or a fine.
- Criminal Justice Act 1998: Section 160 – offence to have in their possession any indecent photograph (or pseudo-photograph) of a child. This offence carried a maximum penalty of five years and/or a fine.
- Malicious Communications Act 1988: Section 1 – offence to send a communication (including electronic) with the intention of causing distress or anxiety, which includes messages that are indecent, grossly offensive or contain a threat. The maximum sentence for this offence is 12 months or a fine (or both).
- Protection of children Act 1978: Section 1(1) – offence to take, permit to be taken, make, distribute and share an indecent photo/ pseudo photo of a child.
- Serious Crime Act 2015: Section 69 –

offence to be in possession of any item that contains advice or guidance about abusing children sexually ('paedophile manual'). The maximum sentence is 3 years imprisonment, a fine or both.

Sexual Offences Act 2003 including:

Section 8 - Causing or inciting a child under 13 to engage in sexual activity

Section 10 - Causing or inciting a child to engage in sexual activity

Section 11 - Engaging in sexual activity in the presence of a child

Section 12 - Causing a child to watch a sexual act

Section 14 - Arranging or facilitating commission of a child sex offence

Section 15A – Sexual communication with a child

Section 15 – Meeting a child following sexual grooming etc.

Section 48 – Causing or inciting sexual exploitation of a child

Please note:

- It is also an offence to attempt to commit any of the above offences.
- You should also consider corresponding legislation applicable in Scotland.

Appendix 6: Reporting guidance

Companies should use the following process to report online child sexual exploitation and abuse. This process may vary for companies based outside of the UK, who may be subject to local reporting requirements or processes:

1. Determine whether a report is needed

You should make a report of suspected CSEA if you:

- have identified suspected grooming behaviour or the livestreaming of child sexual abuse;
- have identified suspected coercion or blackmail involving children; or
- have identified child sexual abuse material (photos, videos, virtual reality, paedophile manuals) created, stored and/or shared using your services.

See Appendix 1 for definitions of CSAM and sexual communication with a child.

2. Collect the necessary information

When making a report, companies are encouraged to prioritise the protection of children by reporting any available associated data that may help in the identification of victims and offenders. This may involve sharing data that is not listed below.

Companies should do so in line with their national data protection legislation.

Required data:

All referrals:

- Email address and/or mobile number.
- Linked or associated email addresses.
- Mobile IP details.
- Port numbers.

For images:

- IP address(es) used for upload(s) with date and time stamp.
- IP login details – these should be from the most recent logins and at least three are required for corroborative purposes, particularly if they are mobile IP addresses.

For chat-based reports:

- Dates of the offending period – as a minimum this is the start and end date and time of the chat.
- The IP address(es) used - this would ideally be provided for each line of the chat.
- Some context of the chat – such as other images that have been shared to help identify the victim, whether the communication is peer-to-peer or between adults.

Additional data (if available)

- Billing addresses.
- Credit card details associated with account/ service user.
- Cookies that identify devices being used and sites being visited.
- Device IDs.
- Details relating to any recipient of IIOC and any associated chat that falls under CSEA offences.

3. Make a report

To make a report about suspected child abuse material or suspicious sexual contact between an adult and a child, companies should follow the relevant guidelines below.

Companies must process personal data in accordance with the requirements of their national data protection legislation. In the UK, this is the Data Protection Act 2018. See Appendix 2 for more information.

Companies without a US office

UK companies

- Contact your local police force and provide full details of the incident.
- Contact information can be found on POLICE.UK or by calling 101.
- For reporting to Police Scotland please find information on the Police Scotland website.
- Please note: Companies should not send indecent images of children as part of their referral to police. The relevant law enforcement agency will contact you to request the image if necessary. (See below information on data retention)
- If you have immediate concerns about the safety of a child you should always call 999.

Companies based outside the UK

- Report suspected online CSEA offending on your platform to the local police or reporting body/hotline in your country
- If there are existing reporting mechanisms in place in your country, you should follow these. Reporting CSAM for removal across multiple platforms
- If you suspect that CSAM present on your platform has been shared on other online platforms you can report it to an InHOPE hotline, who will assess the image for inclusion on their hash list of known child sexual abuse images.
- Find your national InHOPE hotline.
- UK companies should report to the Internet Watch Foundation. See the IWF's website for information on when and how to report to the IWF

4. Retain data

You should retain all available account data related to the report, including content and metadata, where the company has the capacity and capability, in accordance with national data protection legislation. Law enforcement may request this data through a lawful process at a later stage to support an investigation or prosecution.

For companies reporting through NCMEC, the retention period is 90 days. For all companies, UK law enforcement will issue a preservation order when necessary on receipt of a report. The preservation order will stipulate the retention requirements.

Appendix 7:

Age assurance methods

There are a number of methods and data sources that can be used to ascertain the age or age range of users. The method and data source(s) that a platform may use will be heavily dependent on required level of confidence (based on the nature and level of risks on their platform), data available and the context of user privacy on a platform.

Some methods for ascertaining the age of users are more developed than others. The following list of methods are options that companies may wish to consider.

Methods:

- You have told me your age
- I know your digital parent and they have established a profile (or similar) which states your age
- A trusted online provider has authenticated your age
- You have suggested contacting individuals in your peer group and one or more of them have confirmed your age
- You have provided hard evidence, from an official source, that enables me to confirm your age
- Your physical characteristics are consistent with your declared age
- The way that you use your body to interact online is consistent with your declared age
- Your behaviour online is consistent with your declared age
- Your environment is consistent with your declared age
- I know your identity

Data sources:

Source	Generator	Description	Example	Considerations
Officially provided	Large Central Databases	Data accessible through discrete, official databases, which are managed at national level by central government or agencies	Passports Visas Electoral register	High confidence verifying an individual's age where they have engaged with Govt. agency. However, potentially disadvantages elements of society who aren't represented in Govt. databases, coherence and security. Statutory restrictions apply to data use
	Distributed Information	More dispersed, less structured data sources. Equally authoritative but might require significant resources, (human or otherwise) to support the synthesis and supply of data	Medical records	Authoritative. However, may require significant resources (human or otherwise) to support the synthesis and supply of data
User Reported	Digital parent provided	Data generated or provided by the digital parent of the potential child user, who is turn may be required to verify themselves	Financial consent for online purchases School enabled access	Trust in the data is only as good as trust in the parent. May also cause administrative and technical burden for the parent. Delays may case user friction
	Child provided	Data generated or provided by the potential child user	Account handles	Children (and adults) may lie about their age to gain access to age restricted platforms. Minimising user friction is central to an effective industry response
	Peer provided	Data provided by other (trusted) users of the app, service or platform, who have some presumed social relationship with the potential child user and can effectively vouch for their credentials	Peer based attestation	Delays cause user friction and may impact on user experience. Peers need to vouch for their credentials which introduces unreliability. Validation could include other age assurance data sources to enhance accuracy, such as online behaviour analysis
Automatically Generated	Body Metrics	Data derived by the user's physical movements or interactions with a device	Haptics (though data) Gait/motion analysis	Experimental data source Delivers minimal user friction. Would need to be combined with other age assurance data sources to enhance accuracy
	Environmental	Data derived from the physical or infrastructure environment in which the used is based	Technology environment Audio environment	Experimental data source Delivers minimal user friction. Would need to be combined with other age assurance data sources to enhance accuracy Could provide additional information about user risk due to setting
	Behavioural	Data generated by users while using an app, service or platform	Social network data Pattern of app/ platform use	Maturing data source Delivers minimal user friction Needs to be combined with other data sources to enhance accuracy
	Biometrics	Data derived from static (or long-term) physical characteristics of the user	Facial morphotype	A range of maturity depending on data type Delivers minimal user friction Potential for high accuracy Some public perception concerns over anonymity/ privacy concerns might impact on user adoption

For more information about age assurance, see the Verification of Children Online report'. For information about available technologies see the Online Safety Technology Industry Association (OSTIA) and the Age Verification Providers Association.

Appendix 8: Examples of legal but harmful content related to CSEA

There is some imagery which may not be visibly illegal but is connected to child sexual exploitation and abuse. This imagery can continue to traumatise and compromise the safety of victims long after their abuse and is used by offenders to facilitate their activities. The following are examples of legal but harmful CSEA content that companies are encouraged to address:

- **'Where are they now'** threads created for the purpose of posting about a specific victim/survivor. This includes posts in which offenders discuss the abuse history, the victim's current whereabouts, post or link to legal and illegal imagery, links to the victim's social media pages, personal/identifying information, and links to sites that act as archives for previously available websites posting about the victim. In some instances survivors are being located online which presents significant personal safety risks. The Phoenix 11 victims group will only speak under anonymity for this reason.
- **A series of images**, including those taken immediately before and after the abuse. The before and after images could be completely 'normal' such as the child sitting on the bed before being abused, or they may show signs of sexual activity for example semen or use of bondage equipment.
- **Cropped images of abuse**, for example just showing the child's head or with genitals blocked out. Quote from a member of the Phoenix 11 victims group: "We are demanding that ALL images associated with a child's abuse be removed quickly. Because whether it is a smiling headshot, or a tearful action shot, I can tell you first hand that the smile in the head shot is hiding just as many tears."
- **Using legal imagery of a victim as an 'advert'** to draw people to the illegal material on another site. Some offenders may view the legal images in the series as a collectable, publishing them to demonstrate to other offenders their expertise on a particular victim. This also includes the use of 'legal' video frames as a way to advertise a complete video set of that particular victim.
- **Self-generated imagery** (arising from sexting or grooming), which in some cases may not quite make the legal threshold but is still a nude/partially nude image of a child, being shared online against their will and can be posted on offender forums or used by offenders to extract more imagery. This also includes imagery of that same child which may not include nudity (example: image of a child in a bra or underwear).
- **Images that have been photoshopped** to include either the face of a victim onto a sexual/nude image of another individual or altered the image in some capacity to sexualize the child. This also includes the animation or drawn images of child exploitation material (example: taking a known CSAM image and altering it to be animated CSAM).
- **Innocent images of child nudity** (for example, gymnastics videos) with offender commentary highlighting for the benefit of other offenders where genitals become visible. This is an example where the comments,

rather than the image itself need to be addressed as they may not be illegal but are facilitating offender activity.

Victim led approach

Further details on this victim-centred approach, focussing on the harm caused by the imagery, have been set out by the Canadian Centre for Child Protection (a global NGO on CSEA) and the Phoenix 11 (a victims group).