Home Office

Voluntary Guidance For Internet Infrastructure Providers On Tackling Online Child Sexual Exploitation And Abuse (CSEA)

Contents

Introduction 3

Definitions 4

Section 1: Cross-cutting Actions 5

Section 2: Service-specific Actions 7

Sources of support and further information 13

Introduction

Child sexual exploitation and abuse (CSEA) is an abhorrent crime that has a devastating impact on victims and their families. It is imperative that all internet services do everything they can to tackle online CSEA, which includes the sharing of child sexual abuse material (CSAM), the livestreaming of child sexual abuse and the online grooming of children.

All parts of the internet eco-system have important but different roles to play in tackling online CSEA. For example, Internet Service Providers blocked 8.8 million attempts to access child sexual abuse content from the UK in a single month during lockdown in 2020, and some content delivery networks are making tools to detect child sexual abuse content available to their customers. In recognition of the important role that internet infrastructure providers play in protecting children, the Government's response to the Online Harms White Paper included a commitment to produce voluntary best practice guidance for infrastructure providers, to encourage them to take effective and proportionate steps to help identify and prevent online CSEA.

Infrastructure providers can also take steps to tackle the sharing and dissemination of terrorist content on their services. Please see the Voluntary Guidance for Infrastructure Providers on Tackling Terrorist Content Online for more information.

How this guidance relates to other government initiatives

This guidance is separate from but complementary to the Online Safety Bill 2023. Internet infrastructure providers are out of scope of the safety duties in the Online Safety Bill, but those same third-party ancillary and access service providers could be required, by court order, to withdraw services to enable business disruption measures on non-compliant operators.

This guidance builds upon the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse. These Principles were launched by the UK, US, Australian, Canadian and New Zealand governments, and have since been supported by G7 Interior Ministers, and endorsed by a growing range of companies.

Companies will need to continue to respect relevant legal requirements in different countries over and above this best practice guidance. Support to law enforcement (for example, providing data under warrant) is not covered here as this is dealt with under existing legal frameworks.

How to use this guidance

While not all the actions in this guidance will be relevant to all infrastructure providers, we still regard them as an important framework in terms of guiding their interventions, including judging whether their customers are fulfilling their terms of service, and downstream users are kept safe.

We do not have a fixed definition of "infrastructure providers", but this broadly refers to internet services that enable individual users to access websites, apps and other online content. We have suggested a non-exhaustive list, including internet service providers (ISPs) and mobile network operators (MNOs), cloud services, content distribution networks, anonymising services, registries and registrars, web hosting, browsers, app stores, and devices. We recognise that some companies will provide services across several of these categories. In addition to infrastructure providers, we are also providing some considerations for ancillary services, such as payments and advertising in this guidance.

We encourage all infrastructure providers to carefully consider this guidance and how it applies to their services, and to take all relevant and appropriate steps this guidance outlines to help tackle online CSEA. This guidance is not meant to be static and is likely to evolve and be expanded over time. We welcome any feedback on other areas of best practice.

Actions that companies can take are explained in the sections below. Companies may wish to consider reviewing all cross-cutting actions, and then look at additional service specific actions which may also apply. We recommend reading this guidance alongside the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse and the Interim Code of Practice on Online CSEA.

Nothing in this guidance affects companies' obligations under existing or future legislation, and any other legal obligations. This includes law that regulates the internet and data protection law. We also recognise that not all the guidance contained in this document will be relevant to all infrastructure providers.

Definitions

- Downstream service – Services using the infrastructure provider to run their own platforms. These are the customers of an infrastructure provider.
- Free tier - A tier of a service that is free for customers use. The service›s functionality will likely include restrictions that will be removed if a customer moves to a paid tier.
- Top Level Domain (TLD) - The last part of a domain name. For example, .com, .org and .xyz
- Top Level Domain hopping - Where a site maintains a constant Second Level Domain but changes its Top Level Domain. For example, badsite.com becomes badsite.org
- Second Level Domain (SLD) - The part of a domain name that is directly located before the Top Level Domain. i.e. example.com where ‹example› is the SLD.
- Strings - A sequence of characters. For example, “hello” or “4klp-5th”
- Hashes - A fixed-length alphanumeric string, obtained by performing a one-way function on a piece of data. In the context of this document, a hash is produced from a conversion of a known CSEA image.

Section 1:
Cross-cutting Actions

1. Safety by design

All infrastructure providers may wish to consider the risks posed by their services and the way their services are designed, and the potential for abuse, alongside their legal obligations. Contemplating safety in the design of a service or tool is the best way to prevent harms before they occur. Services should not design tools that pose a high degree of risk without adequate safety mitigations and may wish to take steps to ensure that their downstream customers cannot use their services to circumvent safety features on other services.

Existing Principles of safer online platform design - GOV.UK (www.gov.uk) may be applicable, and helpful to consider implementing.

2. Terms of Service

All infrastructure providers may wish to include in their terms of service suggestions (as appropriate) for downstream customers/clients to prohibit and prevent child sexual exploitation and abuse on their service. The Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse provide a framework for the steps that downstream services can take, which infrastructure providers could use or reference in terms of service. For example, suggesting that downstream services 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 when/if this material is identified, and report to appropriate authorities;
- identify and combat the dissemination of new child sexual abuse material via their platforms and services, take appropriate action under their terms of service when/if this material is identified, and report to appropriate authorities;
- identify and combat preparatory child sexual exploitation and abuse activity (such as online grooming for child sexual abuse);
- identify and combat advertising, recruiting, soliciting, or procuring a child for sexual exploitation or abuse, or organising to do so;
- prevent known images of survivors of CSEA that may not be illegal, but are connected to their exploitation and abuse.

Where possible, infrastructure providers may wish to put in place ‘know your customer’ checks to ensure that customers are identifiable and contactable in the event of breaches, and action can be taken where domains/services are used for child sexual abuse material (CSAM).

3. Receiving and acting on reports

Infrastructure providers may wish to regularly review compliance of their customers/ clients with their terms of service. We recommend that all infrastructure providers ensure they can receive reports about their customers/clients which breach their terms of service. These reports may come from individuals or from a trusted flagger, such as an NGO. There should be clear and transparent processes for resolving any breaches.

Companies may wish to assess reports against their terms of service, and other legal requirements.

Companies may also wish to respond to reports in a certain timeframe and act on those reports in a transparent way. This could include the ability to differentiate between urgent, high-risk reports, where a child is in immediate danger, and instances involving less harmful content.

4. Transparency

Infrastructure services may wish to regularly publish or share meaningful data and insights on their efforts to combat child sexual exploitation and abuse, directly and with their downstream customers. Where appropriate, companies could consider publishing information about the number of reports they receive, services withdrawn, and the measures they use to tackle and identify child sexual exploitation and abuse, such as the use of automated tools.

The Tech Coalition's resource, Trust: Voluntary Framework for Industry Transparency, provides principles-based guidance on transparency reporting for online harms.

5. Collaborating

Infrastructure services could engage with opportunities to share relevant expertise, helpful practices, data, and tools where appropriate and feasible across industry.

This could include collaboration through industry bodies, academics and governments. It could be as part of global groups that offer insights on the threat (e.g. WeProtect Global Alliance, Marie Collins Global Online Platform, Tech Coalition, Internet Watch Foundation, Internet Matters). Companies are also encouraged to form relationships with Government, law enforcement and CSEA focussed NGOs in countries where companies are operating. This will help to identify key challenges and share best practice for solutions

Section 2:
Service-specific Actions

The following are examples of actions that are more specific to certain sectors or services. There will be some duplication of actions, and some companies may offer services that fall into multiple categories.

- Internet Service Providers and Mobile Network Operators
- Content Distribution Networks
- Anonymising services (VPNs, proxies)
- Domain Name registration services (registry and registrar)
- Auxiliary services (e.g. payments, certification authorities)
- Advertising networks
- Web hosting
- Browsers
- App stores
- Device operating systems
- Cloud storage

Internet Service Providers (ISP) and Mobile Network Operators (MNO)

Companies may wish to consider:

- Making use of URL block lists to prevent users accessing child sexual abuse material (CSAM), for example as provided by the IWF to their members;
- Using warning splash pages for users who do try to access these URLs, and provide counter-messaging/support links;
- Working with livestreaming providers and payment companies on signals from metadata that indicate a service is being used for CSEA;
- Using parental controls to prevent children accessing potentially high-risk sites;
- Using proactive CSAM detection methods in areas where the ISP or MNO is implementing messaging services (e.g. MMS).

Cloud Services

Companies may wish to consider:

- Supporting the use of tools which allow platforms to identify, remove, and report child sexual abuse material at scale (there are a number of tools available, for example, Thorn's 'Safer');
- Clearly stating that services cannot be used for criminal purposes including CSEA in terms and conditions;
- Ensuring terms of service require customers to have effective measures in place to prevent offences involving the hosting/sharing of CSAM;
- Ensuring there is a mechanism to receive trusted flagger reports, and removing service/business where companies knowingly fail to address CSAM;
- Implementing 'know your customer' measures to help ensure that illegal activity or material can be traced to an identifiable user;
- Augmenting terms of service to include the prohibition of images and videos of survivors that may not be illegal but are connected to their exploitation and abuse.

Content Distribution Networks (CDN)

Companies may wish to consider:

- Removing their services from sites dedicated to illegal CSAM when notified;
- Making use of URL block lists to scan CDN caches, for example as provided by the IWF to their members;
- Use hash lists to identify known CSAM;
- Developing or offering existing CSEA scanning tools to downstream services;
- Releasing IP addresses related to illegal content when requested by law enforcement/NGOs;
- Removing "free tier" customers, or implementing further scrutiny, control and 'know your customer' checks on this segment to help ensure that illegal activity or material can be traced to an identifiable user.

The Internet Watch Foundation's URL blocklist

The IWF's URL (webpage blocking list) is a dynamic list of webpages that the IWF has identified as hosting child sexual abuse material. Whilst the IWF seeks the removal of this content from where the material is hosted, they add the webpage to their blocking list, which if deployed by technology companies, enables them to prevent their customers and users from accessing known child sexual abuse material. In 2022, a total of 230,922 unique URLs were included on the list with an average of 1,029 URLs added to the list every day. The list is cleaned daily by the IWF team to ensure that links that are no longer displaying CSAM are removed, and any new links added. On average, the IWF's URL list contained 11,488 URLs per day in 2022.

Anonymising services (VPNs, proxies)

Companies may wish to consider:

- Making use of URL block lists to prevent users accessing CSAM, for example as provided by the IWF to their members;
- Clearly stating that services cannot be used for criminal purposes, including CSEA, in terms and conditions;
- Recording and retaining billing data for a specific amount of time to support the investigation into CSEA crimes;
- Services that are encrypted should nonetheless support the investigation into crimes and prevent the circulation of CSEA content;
- Ensure there is capability to mitigate the risk of CSEA irrespective of the design of the service, and/or when making changes to the design of a service;
- Implementing age checks for the provision of VPN services;
- Ensuring they do not promote the use of VPNs and other anonymising services to children, particular as a means of obfuscating protections that are in place for children, such as age checks;
- Clear demarcation of IP address blocks being used by VPN providers;
- Removing "free tier" customer options, or implementing further scrutiny, control and 'know your customer' checks on this segment to help ensure that illegal activity or material can be traced to an identifiable user.

Domain name registration services (registry and registrar)

The Department for Science, Innovation and Technology (DSIT) will be commencing sections 19-21 of the Digital Economy Act 2010 (DEA 2010), which set out the Secretary of State's powers of intervention in relation to internet domain name registries and abuse of their domain names. These prescribed practices and requirements will outline the policies that the registries in scope of the powers should adhere to, to avoid the threshold being met that could trigger the potential exercise of the powers. They will include a list of misuses and unfair uses of domain names that registries in scope must take action to mitigate and deal with. A consultation was opened between 20 July and 31 August 2023, which sought feedback on a proposed list of misuses and unfair uses; this included that registries should have in place adequate policies and procedures to combat the use of domain names administered by those registries which are registered to promote or display child sexual abuse material.

Companies may wish to consider:

- Implementing 'know your customer' measures, which are particularly important for registry services; use account assurance functionality so that customers are identifiable where domains are used for CSAM;
- Recording and retaining billing data for a specific amount of time in order to support the investigation into CSEA crimes;
- Ensuring terms and conditions state that CSAM is not permissible and that domain names will be removed if non-compliant;

- Taking steps to prevent top level domain hopping. Flag second level domain names that have previously been used for a dedicated CSAM site. Companies could also consider flagging similar second level domain names;
- Where strings are identified as containing CSAM, sending any other strings that are owned by that registrant as proactive reports to the appropriate authority.

The Internet Watch Foundation's Domain Alerts

Domain Alerts help registry operators stop their top-level domains (TLDs) from containing domains which host this child sexual abuse material. These alerts notify registry operators when any confirmed criminal child sexual abuse pictures or videos are hosted on any domain using their TLD. This means they can take immediate action to suspend the domain in question, or contact the owner, for example, through the registrar. They can do this, while the IWF are working to have the images removed.

Web hosting

Companies may wish to consider:

- Removing support for sites dedicated to illegal CSAM when notified. Companies could also store hashes of the content when removing a site to use as a deny list for future attempts;
- Actively monitoring hosted sites against a list of hashes and keywords for known indecent CSAM;
- Collect necessary data about all customers so that action can be taken where sites are used to host CSAM (in accordance with data protection law).

Example of a CSAM detection tool: Thorn 'Safer'

Thorn's Safer technology is an all-in-one CSAM detection platform for any platform with an upload button. Safer uses advanced AI technology to help platforms detect, review, and report child sexual abuse material (CSAM) at scale. Once content is flagged as potential CSAM by Safer, platforms can review and then either report using the Safer technology to NCMEC or the Royal Canadian Mountain Police (RCMP), or report to other bodies through alternative reporting mechanisms.

Browsers

Companies may wish to consider:

- Offering parental controls to prevent children accessing potentially high-risk sites;
- Making use of URL block lists to prevent users accessing CSAM, for example as provided by the IWF to their members;
- Ensuring implementation of any new standards and protocols (such as DNS over HTTPS) does not prevent ISP URL filtering;

- Use hash lists to identify known CSAM and then block users' access to this content. There are a number of hash lists available, for example the IWF hash list;
- Embedding help and resources for users, e.g. links to NGO sites, reporting buttons, block or redirect searches for terms that are indicative of CSEA;
- Embedding a 'report abuse' button into the browser or the browser's default homepage;
- Responding to user reports within a certain timeframe and act on those reports in a transparent way;
- Only embedding a search bar into browsers if they are confident that the search engine is safe and take appropriate measures to minimise the inclusion of CSEA in search results. This includes ensuring search providers:
    - Use a regularly updated key words list to flag search terms;
    - Use deterrence messaging with likely CSAM search terms;
    - Do not auto-complete with phrases linked to CSEA;
    - Do not proactively recommend CSEA content to users under "similar images" functions.

Support that can be signposted to users: Stop It Now

Stop It Now is a helpline for anyone with a concern about child sexual abuse and its prevention, whatever the worry or level of concern.
Advisers can support anyone struggling with their own or a loved one's sexual thoughts, feelings and behaviours towards children. The service also supports anyone worried about a child or young person's sexual behaviour around other children, or if they've got into trouble online.
The helpline can also be used by adults concerned about a child or young person who may have been abused, a professional calling for case advice or an adult survivor of child sexual abuse.

App stores

Companies may wish to consider:

- Having clear terms and conditions for app developers, that state CSAM is not tolerated and that apps will be removed;
- Mandating minimum safety by design requirements for relevant apps to be published on the app store;
- Proactively reviewing app compliance with app store terms and conditions, including whether sufficient trust and safety processes are in place to prevent user generated or shared CSEA, and remove apps that aren't compliant;
- Providing options for users to report apps in the app store, and respond to user reports within a certain timeframe and act on those reports in a transparent way;
- Offering training for app developers on safety by design and CSEA;

- Putting in place and enforcing additional safety requirements for “high-risk” categories of app, such as stranger-matching chat/video services and pornographic content, if those services are permitted in the app store;
- Implementing age assurance at app store level, and consider age-gating “high-risk” apps and apps which aren’t taking action to safeguard children, such as stranger-matching chat/video services and pornographic content, where those are permitted;
- Providing clear information to users about the risks of different apps;
- Displaying warning messages or signposting support to anyone searching for blocked or illegal apps.

End-User Device Operating Systems

Note: this section refers solely to protecting the user by blocking content (and preventing them from inadvertently accessing CSAM) rather than focussing on reporting to law enforcement. End-User Device Operating Systems vary significantly, so some options may not be applicable to all.

Companies may wish to consider:

- If applicable, use hash lists to identify known CSAM and then block users’ access to this content. There are a number of hash lists available, for example the IWF hash list;
- Supporting apps, and associated tech development, that want to implement device level hashing or AI to detect CSAM, including on end-to-end encrypted services;
- If applicable, working on device level solutions for the detection of CSEA, including working with other services and companies who might be looking to develop these solutions;
- Providing safety information and links to external support (e.g. Childline) on devices registered to a child;
- Implementing default safety settings;
- Offering parental controls, primarily at the point of set up;
- Embedding device-level age assurance.

Ancillary services

Payment services and certification authorities

Companies may wish to consider:

- Clearly stating that their services cannot be used for criminal purposes, including specifically highlighting CSEA in terms and conditions;
- Ensuring terms of service require customers to have:
    - effective measures in place to prevent and detect the hosting/sharing of CSAM;
    - a mechanism to receive trusted flagger reports, and removing service/business where companies knowingly fail to address CSAM;
    - effective spot checks to enforce terms and conditions;

- ‘know your customer’ checks to help ensure that illegal activity or material can be traced to an identifiable user;
- mechanism for monitoring and reporting suspicious activity to law enforcement.

Advertising networks

Companies may wish to consider:

- Clearly stating in terms and conditions that services cannot be used for criminal purposes including CSEA, and publicising that they will inform the authorities of illegal activity;
- Ensuring terms of service require advertisers to have effective measures in place to prevent the hosting/sharing of CSAM;
- Ensuring there is a mechanism to receive trusted flagger reports, and removing service/business where companies knowingly fail to address CSAM;
- Conducting rigorous spot checks to enforce terms and conditions;
- Implementing ‘know your customer’ checks to help ensure that illegal activity or material can be traced to an identifiable user;
- Making use of URL block lists to avoid advertising on illegal CSAM sites, for example as provided by the IWF to their members.

Sources of support and further information

- Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse - GOV.UK (www.gov.uk)
- Interim code of practice on child sexual exploitation and abuse (publishing.service.gov.uk)
- Principles of safer online platform design - GOV.UK (www.gov.uk)
- Memorandum of Understanding Between the Crown Prosecution Service (CPS) and the National Police Chiefs’ Council (NPCC) concerning Section 46 Sexual Offences Act 2003 | The Crown Prosecution Service
    - This memorandum helps to clarify the position of those professionally involved in the management, operation or use of electronic communications networks and services who may face jeopardy for criminal offences, so that they will be re-assured of protection where they are acting to combat the creation and distribution of images of child abuse.
- WeProtect Global Alliance
- Tech Coalition
- Resources & Research: Project Arachnid: Online availability of child sexual abuse material – protectchildren.ca
- Stop It Now! child sexual abuse helpline - Stop It Now
    - Anyone with a concern about child sexual abuse and its prevention can anonymously call the Stop It Now! helpline. This could be: advice for someone worried about another adult’s online or offline sexual behaviour towards children; help for someone concerned about a young person’s sexual behaviour; or confidential

help for anyone worried about their own sexual thoughts, feeling and behaviour towards children.