



to Counter Online Child Sexual Exploitation and Abuse

Introduction

Online child sexual exploitation and abuse is a global crime that demands a global response. In an increasingly digital and borderless world, this crime is becoming easier to commit, more extreme in nature and growing in scale. These crimes have a devastating and lasting impact on victims and survivors, and offenders continuously adapt and diversify their methods as technology rapidly evolves.

Keeping children safe from online sexual exploitation and abuse and limiting their revictimisation by preventing the sharing and viewing of child sexual abuse material can only be achieved through systematic cross-sector collaboration. Only by strengthening collaboration among governments, industry and others and drawing on our collective skills and resources will we achieve the safe online environment that our children and the global community expect and deserve.

Digital industry delivers many benefits through its services and ability to connect people. This industry is also instrumental in preventing online services and platforms from being used to facilitate online child sexual exploitation and abuse. Platforms and services, including but not limited to social media, gaming, livestreaming, messaging services, app stores and devices, and infrastructure providers such as internet service providers, web-hosting and virtual private networks can all play a part in combating online child sexual exploitation and abuse. These varying parts of the ecosystem will respond and the principles will apply differently depending on the provider's role, available technology, the nature of their terms of service and contractual obligations.

Governments acknowledge the extensive existing industry efforts to combat these crimes. Companies have dedicated significant resources to develop and deploy policies, tools and processes in the fight to protect children online and to detect, disrupt and identify offenders. While significant progress has been made, there is much more to be done to strengthen existing efforts and enhance collective skills.

Our goal is the prevention of child sexual exploitation and abuse. To this end, our five Governments, having consulted with a wide range of stakeholders including a leading group of industry representatives, have developed this set of voluntary principles.

The principles aim to provide a framework to combat online child sexual exploitation and abuse, and are intended to drive collective action. It is anticipated that they will evolve over time, as they are discussed with and adopted by a much broader range of companies and stakeholders. The WePROTECT Global Alliance, which currently comprises 97 governments, 25 technology companies and 30 civil society organisations, will promote and support the adoption of the principles at a global level to drive collective industry action.

It is important to recognise that every service to which these principles may apply is different. Some services' primary risk in combating online child sexual exploitation and abuse will relate to the sharing of abuse material, while others may be more likely to be used for grooming or livestreaming. As a result of the services they offer, many companies will have a combination of risk factors. A company's risk profile will determine the way in which it applies the voluntary principles, and which ones are relevant. When applying these principles, companies will take into account technical limitations, available resources, and legal and privacy considerations.

These principles are intended to provide a consistent and high-level framework for industry actors that is flexible and can be applied across different services. Some companies have already implemented measures similar to those outlined in these principles. Regardless of whether a company chooses to adopt these principles, existing laws and regulations in relevant jurisdictions continue to apply to all companies. Nothing in these principles overrides or is contrary to the need for companies to act according to law.

Examples of the types of things a company may want to do to apply these principles include:

- review existing safety processes against each of the applicable principles
- understand the level and nature of the online child sexual exploitation and abuse threat and areas of high risk on its platform
- identify gaps, consider where existing measures can go further, and improve and invest in innovative tools and solutions
- respond to the evolving threat and changing societal and offending behaviours to reduce foreseeable and unexpected risks for users.

The voluntary principles are part of wider efforts to protect children, both on and offline. Governments, law enforcement agencies, industry companies, non-governmental organisations and other partners all have a critical role to play as set out in the WePROTECT Global Alliance's Model National Response.

The Voluntary Principles



Prevent child sexual abuse material

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 revictimising 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.

Note on reporting to appropriate authorities (applicable to all relevant principles 1-5):

for companies based in the United States of America, reporting is mandated via the National Center for Missing and Exploited Children (NCMEC). 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.

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.



Target online grooming and preparatory behaviour

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.

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 like-minded offenders to work together to enhance individual and collective access to children for the purposes of sexual exploitation and abuse.



Target livestreaming

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.



Search

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 revictimisation 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.



A specialised approach for children

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.



Victim/survivor considerations

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 is 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.



Collaborate & respond to evolving threat

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.

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.

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.

