

Outline

Module objectives

1 Children and technology

1.1 Children's rights in the digital age

 Resources

1.2 The benefits of technology

 Case study

1.3 Children's use of technology

 Resources

 Reflection point

2 Online risks for children and young people

2.1 The online risks

 Reflection point

(a) Inappropriate content

(b) Inappropriate contact

(c) Inappropriate conduct

(d) Health-related risks

 Resource

(e) Consumer-related issues

 Case study

2.2 Child sexual abuse

 Reflection point

2.3 The impact of COVID-19 on child online protection

3 Measures to protect children online

3.1 Legislative measures

 Resource

3.2 Self- and co-regulatory measures

3.3 Technical measures

 Reflection point

 Resources

3.4 Awareness-raising and education

 Case study

 Resources

3.5 Developing a national strategy

 Resources

 Reflection point

4. The stakeholders involved in protecting children online

4.1 A shared responsibility of all stakeholders

 [Case study](#)

[Google's Be Internet Awesome Programme](#)

 [Case study](#)

[4.2 How are the stakeholders collaborating](#)

 [Reflection point](#)

[5. Resourcing Child Online Protection Initiatives](#)

 [Case study](#)

[6. Conclusion](#)

[7. Quiz](#)

Module objectives

Welcome to the **knowledge module on child online protection**, as part of the GFCE-Africa project.

What are the aims and objectives of this module?

This knowledge module consists of a set of responses to the key questions which policymakers ask – or need to ask – in relation to keeping children safe online. The responses are presented in the form of explanations, and include case studies, additional resources, reflection points, and other options for additional engagement by the participants.

The components of this KM can be used for different formats of delivery:

- (a) online self-paced course: participants can take a course through an online learning platform, step by step, at their own pace, with an option to exchange views with others that take the course; an option to download materials is included.
- (b) in-situ training or webinars: participants can use the content as background material, or as the basis for presentations, with reflection points serving as exercises.

What does this module cover?

This knowledge module starts by looking at the way and extent to which children are using technology, and discusses the benefits and threats of the internet and technology for children through a rights-based approach. It then discusses the different measures for tackling children's online protection, ranging from legislative frameworks to technical measures and other awareness-raising initiatives. It also discusses the main actors and their responsibilities towards ensuring children's well-being online.

What can you expect to learn?

Upon finishing the module, you will be able to respond to, and find additional resources for the following questions:


- What do the latest studies tell us about the way children are using technology? Has the COVID-19 pandemic affected children's use of technology?
- Why is it advisable for policymakers to look at child online protection through a rights-based approach, rather than focusing exclusively on the risks and threats?
- What are the types of risks involved? Does every risk lead to an actual threat?
- What are the different types of measures which stakeholders can use to protect children online?
- What are the key areas for consideration when developing a national child online protection strategy?
- In what ways do the stakeholders collaborate, and how can this collaboration be improved in a local context?

1 Children and technology

Access to the internet presents many opportunities for children's education, personal development, self-expression, and interaction with others. Despite the many benefits, however, children and young people face certain risks when using the internet and technology. While users of any age can face risks, children are particularly vulnerable as they are still developing. This has presented a cause for concern for governments, parents, and educators for quite some time.

Before we deep-dive into the online risks for children and how to mitigate these risks, it is important to first look at the internet and technology from a wider perspective. This includes understanding children's rights in the digital age, and the benefits and opportunities of the internet for children, as well as understanding how children access and use technology.

1.1 Children's rights in the digital age

-  *How can the issues around children's online protection be addressed through a rights-based approach, and why does this matter?*

Discussions on child online protection often focus on the risks for children, including the worrying trends related to online child sexual abuse. The term 'Child Online Protection' itself places the focus squarely on the online dangers which children face. However, policies that focus exclusively on online risks can derail the internet's potential to empower children.

A rights-based approach, which places children at the centre, balances the need to safeguard children from harm with an appreciation of the benefits of technology for children and the rights that children have in the digital age.

This is not to say that the protection of children is sidelined – far from it. Rather, the approach takes the [UN Convention on the Rights of the Child](#) (Video 1) as the starting point, and places children's rights at the heart of the discussion. With such an approach, practitioners can focus on maximising the opportunities of the digital world for children and young people, while fostering a safe and secure online environment.

[Embed video: https://www.youtube.com/watch?v=b7_QpJ9Ki5Q

Video 1. *Convention on the Rights of the Child explained*

Source: UNICEF Ghana

It is a well established rule that the rights that people have offline must also be protected online. That includes children and their rights.

Yet, one of the main questions which practitioners have been asking is how to apply the [UN Convention on the Rights of the Child](#) – a convention which entered into force in 1990, at a time when the internet was still picking up – to the digital age.

In 2021, the UN Committee on the Rights of the Child's 86th session adopted a few legal instruments which serve to explain how the convention applies to the digital age:

- [General comment no. 25 \(2021\)](#) on children's rights in relation to the general environment
- The [explanatory notes](#) to the general comment
- A [glossary of some of the main terms](#) used in relation to the internet, such as what 'data minimisation' and 'profiling' mean
- A [child-friendly version](#) to explain children's rights in a way they can understand.

1.2 The benefits of technology

In the [words of former Frank La Rue, UN Special Rapporteur on Freedom of Expression](#), 'the internet has dramatically improved the ability of children and adults in all regions of the world to communicate quickly and cheaply. It is therefore an important vehicle for children to exercise their right to freedom of expression and can serve as a tool to help children claim their other rights, including the right to education, freedom of association, and full participation in social, cultural and political life.'

The internet presents a wealth of opportunities for children and young people, including opportunities for learning, sociability, self-expression, creativity, and participation through online media accessed via fixed and mobile devices.

The use of technology empowers children to express their opinions and provides multiple ways to connect and communicate with their families and friends. The benefits include broader access to educational resources, and information about health and social services. Since the internet has increased access to information in all corners of the globe, it offers children and young people the ability to research almost any subject of interest, access worldwide media, pursue vocational prospects, and harness ideas for the future. In addition, the internet serves as an important tool for cultural exchange.

Technology is also used to gather and transmit data by child protection service providers, facilitating, for example, birth registration, case management, family tracing, data collection, and mapping of violence. As children and families use the internet and mobile phones to seek information and assistance, and to report incidents of abuse, these technologies can help protect children from violence and exploitation.

Case study

Can mobile technologies improve literacy?

A [2014 study by UNESCO](#) surveyed 4000 people in 7 countries – Ethiopia, Ghana, India, Kenya, Nigeria, Pakistan, and Zimbabwe – to find out how people are using mobile phones for reading, and what impact this has on their habits and attitudes towards reading.

The researchers concluded that access to books (via mobile devices) on its own is not sufficient to promote literacy. However, mobile devices facilitate more reading, especially in cases where the internet is accessed through mobile phones.

1.3 Children's use of technology

-  *How are children using technology, and to what extent?*

The online environment evolves quickly, and new technology is constantly being developed. This has significant consequences on children's lives.

Research shows that:

- One in three online users among the global online population [is a child under the age of 18](#). In the Global North, children make up 1 in 10 users, but in other countries, this number rises to almost half of the online population.
- Children's most popular device for accessing the internet [is the mobile phone](#), and in many cases, this is [often the only way](#) children access the internet.
- In some regions, children [access the internet daily](#).
- Children and young people [are increasingly using](#) instant messengers and wearable technology, whereas social networking sites (such as Facebook) are slowly giving way to YouTube and newer apps such as Instagram and TikTok, used primarily for watching videos (Figure 1).

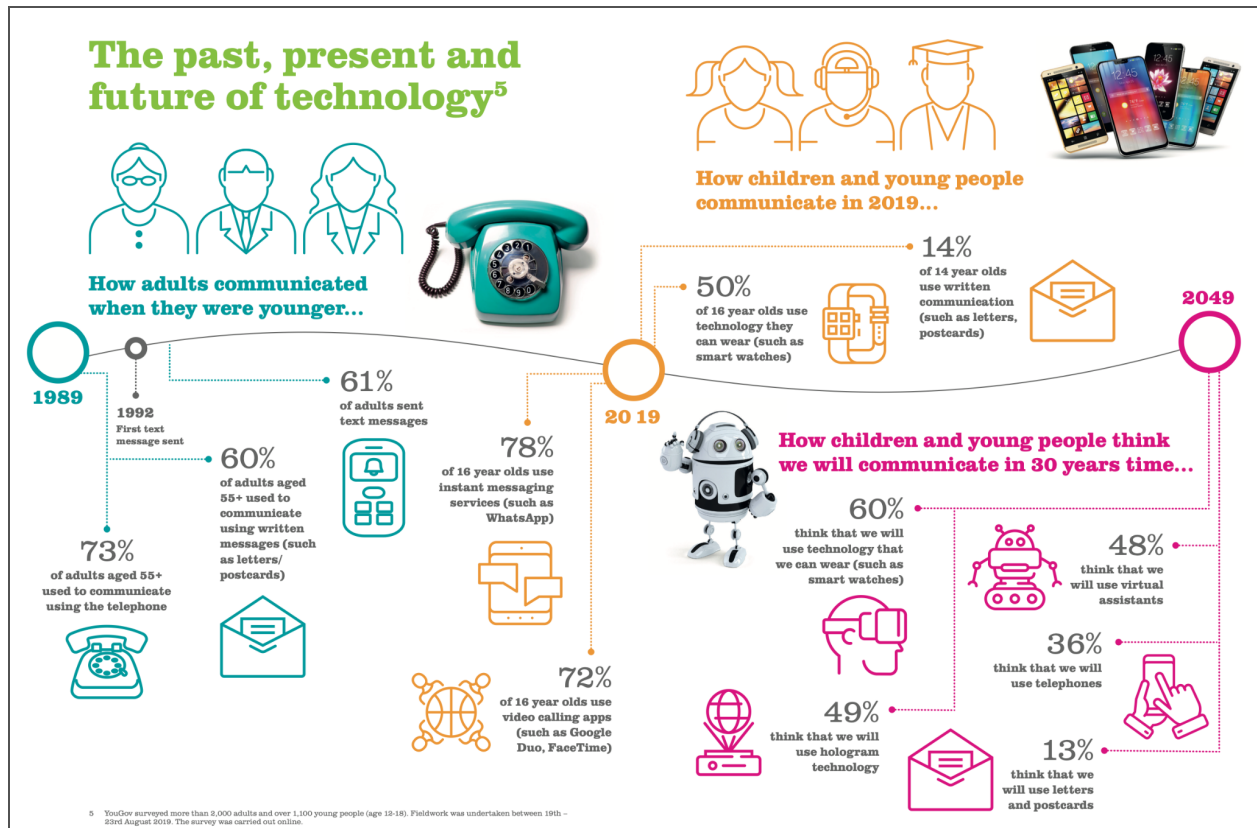


Figure 1. The past, the present, and the future of technology.
Source: Barnardo's [Generation Digital](#) report (2019)

Resources

There are multiple studies on how children around the world and in different regions are accessing and using the internet. These include:

- The [Global Kids Online comparative report](#) (2019), published by UNICEF Innocenti, the organisation's Office of Research. Global Kids Online is a multi-country programme coordinated by UNICEF Innocenti which studies the opportunities and risks that children from around the world may encounter in the online world.
- The [EU Kids Online report](#) (2020), published by the EU Kids Online project, which tracks how European young adults aged 9 to 16 are accessing and using the internet.
- [Statistics collected by the security company Kaspersky](#) (2019-2020), which include trends about the content children access.




Reflection point

The way children use technology and the internet informs policymaking processes and mobilises stakeholders to act. Does any research exist on the way children in your country or region use the internet? If yes, what do the trends show? If not, why do you think this is lacking?

2 Online risks for children and young people

2.1 The online risks

-  Which are the risks that children face online? Is there an easy way to categorise them, in order to understand the risks and tackle them more effectively?

Experts have developed several ways of identifying online risks. We can summarise the main risks in five categories: (a) inappropriate content, (b) inappropriate contact, (c) inappropriate conduct, (d) health-related risks, and (e) consumer-related issues.

Reflection point

Before we go into further detail, it is good to note what various studies have concluded: although children and young people are exposed to risks, [not every risk leads to actual harm](#). In other words, the levels of harm are 'significantly lower' than those of risk, in that the children could be taking risks but not necessarily experiencing harm. For example, making online contact with strangers is perhaps the most serious risk, and many children do make such contacts. However, few of them go on to make offline contact with that person, and most of such meetings do not lead to harm.

How do you feel about this finding? Does it impact the way you look at child online protection? Should it impact stakeholders' approach towards protecting children online?

(a) Inappropriate content

Children can be exposed to content inappropriate for their age. This includes sexual and adult content, which affects children and young people in different ways.

Pro-anorexia, self-harm, and drug-related content is particularly damaging to vulnerable teenagers struggling with image issues and other personal and social problems.

Inappropriate content also includes violent content. Violent games, for example, involve sophisticated weapons (showing features of real weapons and fantasy features) and bloodshed. In recent years, several online challenges have induced young adults to commit dangerous – even life-threatening – acts.

(b) Inappropriate contact

Children can be exposed to harmful and violent contact, such as bullying and harassment, when using social apps and networks, chat rooms (including gaming chat rooms), and messaging platforms. A child or young person can also be a perpetrator in a peer-to-peer context or harass their peers (also described as inappropriate conduct).

Inappropriate contact can include more heinous or dangerous activities such as grooming by potential perpetrators of sexual abuse, and other abusive and illegal interactions. Such contact places the child as a participant in an adult-initiated online interaction, possibly unwillingly or unknowingly.

(c) Inappropriate conduct

In addition to cyberbullying and harassment, conduct such as sharing inappropriate comments, self-generated indecent images (also known as self-generated explicit material), or sensitive personal information can expose children to more serious harm. This happens because children and young people often fail to fully comprehend the implications for themselves and others of the permanence of content posted online (digital tattoos), or the long-term effect of their content (digital footprint).

(d) Health-related risks

The risks arising from internet addiction and online gaming are becoming more evident. Children under the age of five are more prone to internet addiction, especially social media, due to early access to electronic devices.

Resource

In 2018, the World Health Organization recognised 'gaming disorder' as a medical condition (Video 2). This prompted some countries, such as the UK, to open specialised centres for treating digital-related addiction.

[Embed video: <https://www.youtube.com/watch?v=IJ71KAO0mtc>]

Video 2. Gaming disorder: questions and answers (Q&A)

Source: World Health Organization (WHO)

(e) Consumer-related issues

Risks related to online use (often referred to as consumer-related or commercial risks) are mainly linked to data misuse and privacy, and can be interpersonal, institutional, and commercial. Risks include identity theft, breach of privacy, receiving inappropriate advertising and spam, and exposure to hidden costs (such as apps or games inviting users to make in-app purchases). Children's data, including geo-location, biometric, and other sensitive information, is

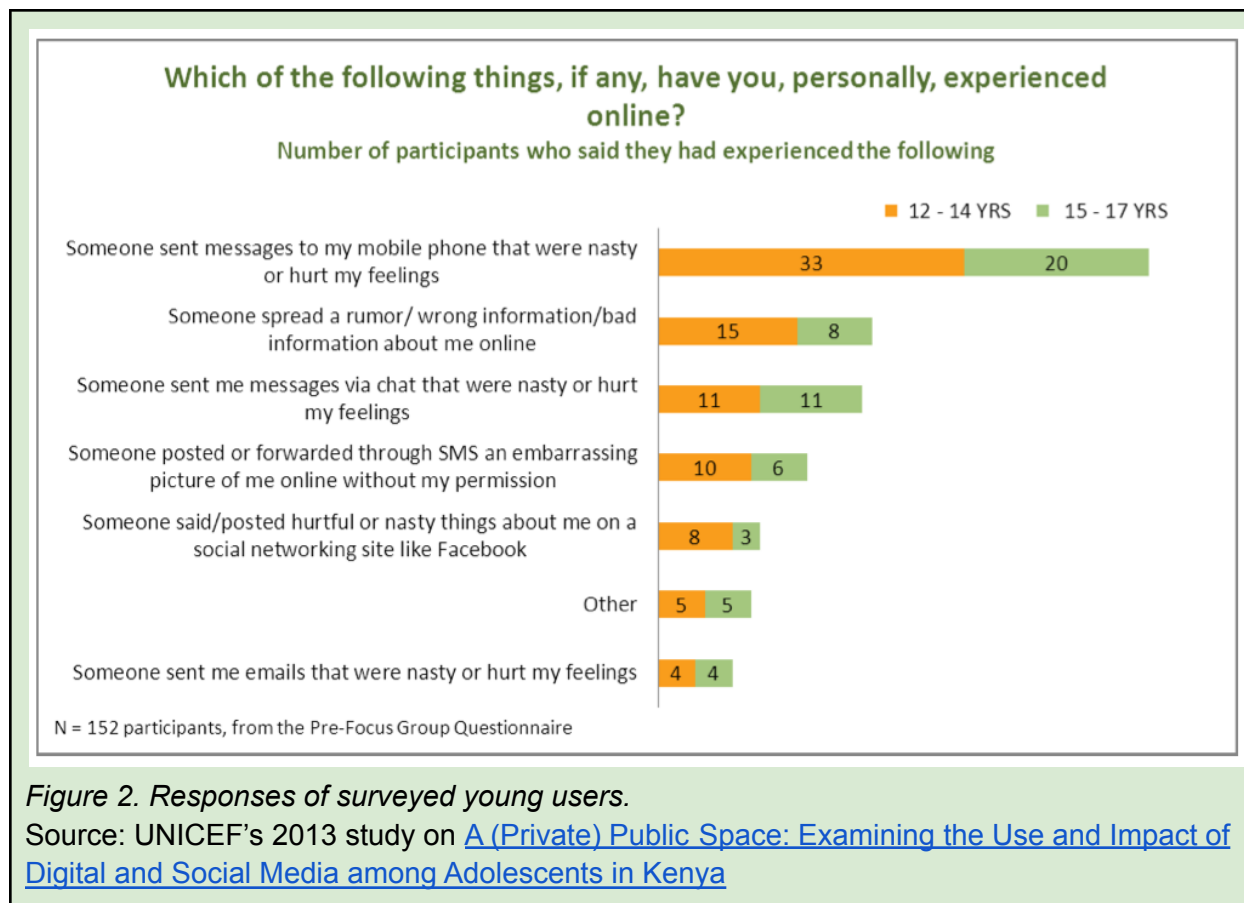
often gathered and processed without true informed consent, resulting in a violation of their rights – from their right to protection from abuse and violence, to their right to privacy.

Case study

Young people in Kenya and their online experience

A 2013 study, commissioned by UNICEF among 12 to 17-year-olds who have access to mobile phones and the internet, was focused on the behaviour and perceptions of safety and risk among these young users. The study, [A \(Private\) Public Space: Examining the Use and Impact of Digital and Social Media among Adolescents in Kenya](#), found that:

- Many young people consider digital and social media an integral part of their lives and use the internet regularly. They use social media platforms and chat forums, access audio/video content, play games, and search for information. Their explorations and social interactions may occasionally lead to risky behaviour.
- They tend to have blurred distinctions between online-only and other friends from their schools, neighbourhoods, or other areas of their daily lives, referring to people in both groups as 'friends'. Some of these young people may try meeting online-only friends in person.
- Many report having encountered sexually explicit content via the internet, and some have shared such content with others. Interactions with online friends sometimes lead to suggestive self-exposure and sexually explicit conversations (Figure 2).
- They want to learn about digital safety but prefer to do so from peers and information they can find online. They feel their parents may not have necessary information or skills. Parents are often unaware of how digitally engaged their children are and tend not to supervise the use of the internet. Due to parents' lack of understanding of digital media, discussions about the internet and social media tend to revolve around restricting young people's use.



2.2 Child sexual abuse

Some of the risks described above can be a precursor to child sexual abuse. Children may receive illegal content, such as child sexual abuse imagery (CSAM), and they could be exposed to predators, leading to grooming and online or offline abuse or exploitation.

Technology has amplified the problem since perpetrators can capture the abuse through digital means (images or videos). A more recent trend has been the commercialisation of child sexual abuse such as through live distant child abuse (LDCA) – also referred to as on-demand child sexual abuse, or cybersex trafficking – where perpetrators can direct abuse in real time.

The internet – including the darknet – has also amplified the issues, since it provides a relatively easy means of accessing and consuming CSAM. Predators often can explore their inclinations anonymously and find ways of evading law enforcement (which is among the typical behaviour of offenders, as shown in Figure 3). Another major concern, linked mainly to livestreaming, is the difficulty of detecting the live act due to the challenge of intercepting encrypted content. Online spaces accessed by children are also often used by abusers to make contact with their victims.

(Note that 'child sexual abuse material' is the [preferred terminology](#) when referring to 'child pornography').

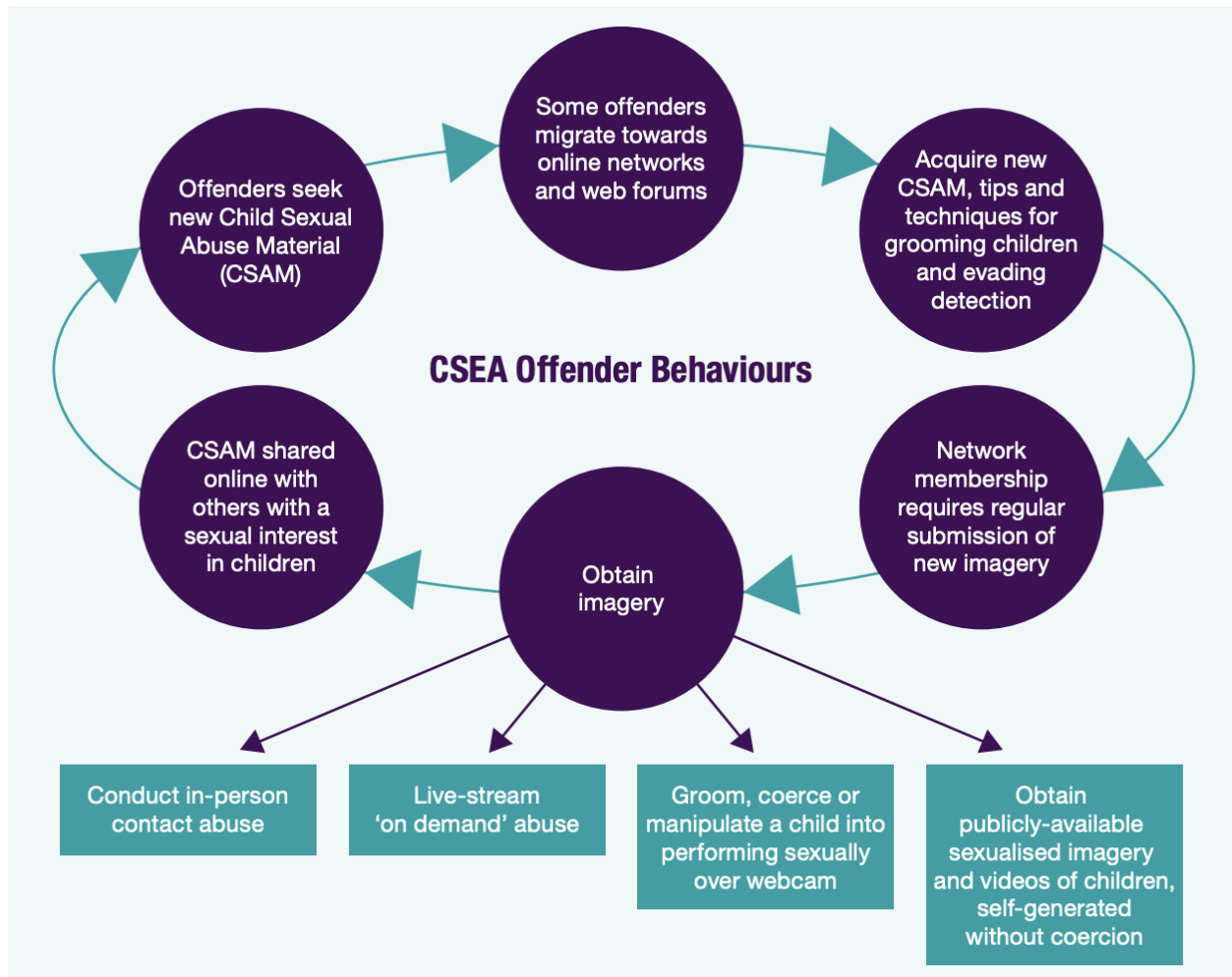


Figure 3. Typical child sexual exploitation and abuse (CSEA) offender behaviours

Source: WeProtect's [2019 Global Threat Assessment report](#)

Reflection point

[INTERPOL notes](#) that child sexual abuse imagery is 'real not virtual':

'Images of child sexual abuse found on the web are not virtual; they are a crime involving real children and real suffering'.


2.3 The impact of COVID-19 on child online protection

-  *How is the pandemic affecting children's use of technology?*

As of April 2021, [more than 1.53 billion children were affected by school closures around the world](#). Schools in only a handful of countries remained open; the rest closed for weeks on end – in some cases, for up to more than a full school year.

To cope with closures, many schools shifted to online learning to support continuity in children's education. Millions of children and educators connected through remote classrooms [facilitated by platforms such as Microsoft Teams, Zoom, and OnlineMeeting](#). Although online learning could not substitute face-to-face interactions, it still provided students with a good option to continue their learning.

This also meant that children spent more time online for entertainment, social, and educational purposes.

-  *Is the pandemic increasing the risks and threats for children online?*

The effects of closures and other lockdowns led to heightened risks for children, which was compounded by the fact that due to restrictions children had limited access to support services.

- INTERPOL concluded that this has led to [under-reporting of child sexual abuse cases, and an increase in sharing of child exploitation material](#) through peer-to-peer networks (see the [full study](#)). This stood in stark contrast to the trends and threats in pre-pandemic times.
- The US' National Center for Missing and Exploited Children (NCMEC) [reported that it received 4.2 million reports of online child sexual abuse material in April 2020](#), up 2 million from March 2020 and nearly 3 million from April 2019.
- The UK's Internet Watch Foundation (IWF) also announced that the [amount of abuse material increased by 89% in just four weeks of lockdown](#), and that there was also an [increased risk of children being groomed and coerced online into making explicit images and videos of themselves](#).
- The Australian Federal Police warned that [online predators were targeting new child victims online](#). The police suspect that offenders are using the lockdown as an opportunity to find more potential child victims, since young people are spending more time online with limited adult supervision.
- The WeProtect Global Alliance said that economic hardship and the inability of offenders to travel due to COVID-19 lockdown was [likely to increase the potential for livestreaming abuse in home environments](#).

The WeProtect Global Alliance's analysis on [The Impact of COVID-19 on Online Child Sexual Exploitation](#) (2020) brings together even more available material on the impact of COVID-19 restrictions on children, in particular, related to abuse and exploitation.

3 Measures to protect children online

No single solution can mitigate the risks children face using the internet. Rather, a combined approach can tackle the risks in a broad way.

This approach combines policy – including legislation, self- and co-regulation, and other policy measures aimed at creating an appropriate digital environment – with the work of law enforcement, the use of technical tools, the increase of education and awareness, and the provision of support for children seeking advice and help, and for victims of abuse. Such an approach is required both on a national level and as a global response.

When it comes to combatting online child sexual abuse and exploitation, a combined approach, involving collaboration among stakeholders on a global level, is important (Figure 4).

A Global Strategic Response to Online Child Sexual Exploitation and Abuse						
Theme	Policy/Legislation	Criminal justice	Victim support services and empowerment	Technology	Societal	Research and insight
Capabilities	<ol style="list-style-type: none"> Political will Accountable leadership and a willingness to collaborate at the highest level. Adequate government resources dedicated to fighting the epidemic Legislation Comprehensive technology, including common definitions, terminology and thresholds to facilitate the harmonisation of criminal offences, obtain evidence, hold the private sector accountable and prevent unaccountable 'sovereign' companies International commitments To capacity development (both cross-border technology-based improvements and systemic improvements within countries) and the prevention of ineffective state response systems 	<ol style="list-style-type: none"> Information sharing and collaborative targeting Shared access to international databases, particularly those regarding child sexual abuse material and offender targeting methodologies, formal data sharing frameworks, high value collective targeting Risk/threat assessment matrix For victim ID and offender targeting Modernised cybertip reporting systems Collaborative online expertise Collaborative tech development to investigate offenders Dedicated, trained officers and prosecutors with expertise in tackling online child sexual exploitation and solutions for investigating encrypted content 	<ol style="list-style-type: none"> Crisis response Effective and timely support Victims' voice groups Advocates for change Victim empowerment to protect victims' privacy and dignity by the timely removal of all exploitative material Victim identity protection Preserve the anonymity of victims 	<ol style="list-style-type: none"> Innovative solutions The use of technology, including artificial intelligence, to detect, block and prevent illegal and exploitative material, live streaming and online grooming Technology-led risk and safety assessment across platforms and upstream/ downstream providers Voluntary principles for child safety, including safety by design Wide and consistent adherence among tech sector Increased transparency Regularly publish transparency reports on detection and removal of child sexual abuse material, and ensure data are supported by explainable methodology 	<ol style="list-style-type: none"> Digital culture development A demand for online child safety to be prioritised, built into and evolving the technology, increased public/online accountability of governments and companies Informed media reporting Ethical approach, consistent terminology Restriction of children's exposure to illicit and harmful content online Systemic restrictions to prevent child access to illicit content Education and outreach Regular messaging appropriate to age, gender and culture Offender outreach Develop targeted early interventions strategies 	<ol style="list-style-type: none"> Threat analysis and monitoring Detailed and up-to-date assessments of threats and trends Research to understand online vulnerabilities and effective safety education systems Online safety and preventative approaches Offender research Offender behaviour, drivers, pathways and effective intervention Long-term victim trauma analysis increased and sustained investments in ethical AI and safety-enhancing solutions
Outcomes	<ul style="list-style-type: none"> Renewal of high-level commitment at a national and international level Sufficient funding, focus and legal frameworks in place at a national level to prevent child sexual exploitation and abuse internationally Formally renew WePROTECT Global Alliance (WPGA) commitments Increase number of country members to WPGA and strengthen engagement Centralise child sexual abuse material consistent with Lanzarote Convention; develop common framework for content classification Prioritise the protection and privacy of children online in domestic and global policy Best practice legislation menu with regional samples Ensure laws and technology, including data retention, do not evolve in ways that increase online harms to children 	<ul style="list-style-type: none"> Resources are pooled to identify, pursue and apprehend offenders and rescue victims Successful joint investigations and prosecutions are conducted Centralised online resource centre for all countries Investigative tools to counter anonymisation tech Consolidated image repository for Collective Victim ID analysis and targeting Formalise global investigative taskforce for collective high value targeting Formal data sharing frameworks, universal cooperation frameworks, and standards for legal interoperability 	<ul style="list-style-type: none"> Victims have access to the support they require Standardised procedures for reporting images, material and contextual information to rescue victims Increase dedicated Child Advocacy Centres for all forms of child exploitation Standardised practices to protect the identity of victims Expand victims' voice groups 	<ul style="list-style-type: none"> Industry, leverage and legislation to prevent their platforms being used as a tool for abuse Government and non-governmental organisations use technology and legislation to ensure platforms are not used as tools for abuse Regular reporting Strong law enforcement engagement and policies on legal compliance Proactive and responsive international engagement with technology sector Increase volume of technology sector prioritising child risk assessment and safety by design Broader use and application of Anaschmid notice and takedown platform 	<ul style="list-style-type: none"> Children are protected from sexual exploitation and abuse, no matter where they live. Parents are empowered to protect their children from online harm, no matter where they live. Public action holds government and companies accountable Global public service announcement elevating priority of child protection in the digital world Further measures taken to reduce offending Children, carers, teachers and other responsible adults aware of risks and protection measures Awareness raised among the public Offenders and potential offenders can obtain services to prevent first-time offending and re-offending Understanding and countering increase in self-generated child sexual abuse material 	<ul style="list-style-type: none"> Government, law enforcement, civil society, academia and industry have a clear understanding of the latest threats Regularly updated insight into global trends and the impact of interventions, including through an annual Global Threat Assessment Deeper understanding of the long term impact of abuse, including the economic cost Deeper understanding of the impact of abuse into adulthood, including the economic cost Assessment of online safety education programmes
Partners	National governments, regional organisations, UN agencies and industry partners	National law enforcement, Interpol and regional partners	National and international civil society organisations with specialist expertise	International and national technology companies, industry associations, and national and international law enforcement	National governments, regional organisations, international and national civil society organisations	National governments, regional organisations, international and national civil industry, society organisations, national and international law enforcement, and academic institutions


Coordinated capacity building

- Establish comprehensive model of capacity building that incorporates all sectors of Model National Response
- Establish coordination between countries conducting bilateral capacity building
- Dedicated training for policy leaders to develop the Model National Response
- National and regional policy leaders trained to identify strengths, gaps and opportunities

Figure 4. A global strategic response to online child sexual exploitation and abuse

Source: WeProtect Global Alliance. [Full version available here.](#)

3.1 Legislative measures

-  Which aspects are addressed (or criminalised) by laws, as opposed to other non-binding measures?

Do you recall the categories of risks which children face? We mentioned five categories – inappropriate content, inappropriate contact, inappropriate conduct, health-related risks, and consumer-related issues – as well as the more heinous crime of sexual exploitation and abuse which these risks can lead to.

When it comes to legislation, some laws make certain content, contact, or conduct illegal, with varying degrees of interpretations from country to country. Certain contact- and conduct-related activities, in fact, are punishable as criminal offences in many countries. This largely depends on the type of risk or behaviour we are referring to.

For instance, when it comes to sexual exploitation and abuse, there are a number of primary instruments on an international level, which have inspired other instruments on a regional level. The international instruments include:

- The [UN Convention on the Rights of the Child](#), which, among other provisions, obliges states to ‘undertake to protect the child from all forms of sexual exploitation and sexual abuse’ (Article 34).
- The [Second Optional Protocol on the sale of children, child prostitution and child pornography](#) (and the UN Committee on the Rights of the Child’s guidelines), which imposes further obligations on states concerning child sexual abuse content, among other topics.
- The Council of Europe’s [Convention on Cybercrime](#) (known also as the Budapest Convention), which obliges countries to criminalise every act related to child pornography (Article 9).
- The [Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse](#) (known as the Lanzarote Convention), which requires states to prevent all forms of sexual exploitation and sexual abuse of children and to protect children (Article 4); to encourage the reporting of suspicion of sexual abuse (Article 12); and to support the setting up of helplines (Article 13).
- The International Labour Organization’s [Convention Concerning the Prohibition and Immediate Action for the Elimination of the worst forms of Child Labour](#), which calls on members to take immediate and effective measures to secure the prohibition and elimination of ‘the worst forms of child labour’, including prostitution (Article 3).


The [International Centre for Missing & Exploited Children \(ICMEC\)](#)'s framework for assessing legislation is an important resource for enacting, reviewing, and updating legislation. Introduced in 2006, the framework is updated regularly, and includes a 'menu of concepts' to be considered when drafting legislation.

Access the latest version – the [9th edition, published in 2018](#) – and check out ICMEC's review of the legislation in your country. How is your country doing? What should be improved?

Exercise

What are the legal provisions in your country's cybersecurity strategy or legislation that explicitly protect children online?

3.2 Self- and co-regulatory measures

-  *Are non-binding measures as effective as laws?*


The industry favours self-regulation (voluntary agreement on the part of the industry) and co-regulation (a combination of government and private regulation), which is considered an effective approach. Although these are often non-binding, they have produced good results in protecting children from online harm.

For example, internet service providers (ISPs) may voluntarily provide for notice-and-takedown measures and may also filter certain types of illegal content, while social media platforms can set minimum age requirements for children.

A good working relationship between the industry and law enforcement, including clearly defined processes and protocols for working together, is also important. In 2008, the Council of Europe published its [Guidelines for cooperation between law enforcement and ISPs against cybercrime](#) which are still applicable today.

In 2020, the Five Country governments (Australia, Canada, New Zealand, the UK, and the USA) in consultation with six tech companies (Google, Microsoft, Twitter, TikTok, Facebook, and Roblox), and other experts, launched a [Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse](#) for companies to implement.

3.3 Technical measures

-  *What are some examples of technical measures? Can they be used independently, in lieu of other types of measures?*

National policies rely, to different extents, on technical measures that should be used only in conjunction with other measures. In addition, technical measures can be either voluntary – as in many countries – or a legal requirement. For example, in some countries, ISP filtering forms part of self-regulatory measures, while in others, filtering is a mandatory requirement.

Various technical and process-based measures can combat child sexual abuse. Hotline reporting mechanisms and notice-and-takedown requests often work hand-in-hand, and are typically the first line of defence for industry players seeking to rid their services of illegal content.

Technical measures also include maintaining victim-identification databases and preventing access to specific sites, such as Europol's and INTERPOL's databases that help identify victims of child sexual abuse. Hashing technology, which assigns a unique fingerprint (or hash value) to identify child sexual abuse images, has become an important tool in combatting CSAM. Other technical measures make use of data mining and analytics to assist investigations.



Reflection point


Hotlines are typically a first line of defence for the public and the industry to report and remove illegal content. Does your country have a national hotline for reporting child sexual abuse content or cases of child exploitation?



Resources

The GSMA INHOPE guide [Hotlines: Responding to Reports of Illegal Online Content](#) (2014) is a useful resource for setting up a hotline.

3.4 Awareness-raising and education

-  *What is the added-value of providing awareness and educational support and resources to parents, educators, and children themselves?*

Education and awareness of kids, as well as parents and educators, are generally considered to be the first line of defence, hence their continued importance. At the national level, many campaigns have targeted children and young people, parents and guardians, and educators. A wealth of awareness-raising resources, including online resources, is also available and growing. Such resources typically provide advice on safe ways of using technology and the internet.

For instance, the International Telecommunication Union (ITU) Child Online Protection (COP) initiative provides [guidelines for children, parents and guardians, as well as for educators, industry, and policymakers](#) (published in 2020). Providing resources in different languages is also important. [Safer Internet Day](#), organised by the INSAFE network each year in February, promotes the safe use of the internet and mobile technology, especially among children and young people worldwide. These are just a few examples.

Case study

Kenya study provides several education-oriented recommendations

The UNICEF study we cited earlier, [A \(Private\) Public Space: Examining the Use and Impact of Digital and Social Media among Adolescents in Kenya](#) (2013), made several recommendations. Among those:

- 'Understand digital use and digital safety from the perspective of young people first, before designing the content of digital safety information programs...
- Involve parents and school authorities in digital safety programs aimed at young people.
- Balance digital safety messages with emphasis on the usefulness of the internet in areas such as education, research and commerce.
- Encourage young people to use the internet also as a resource for reporting online or offline abuse or other inappropriate behaviour.
- Create online and offline digital safety campaigns for placement on the full spectrum of traditional and digital media outlets [...] young people commonly access and use.
- Foster young digital safety champions who can speak to their peers through digital media, audio and video spots on mass media, and offline spaces like schools and universities.'

Resources

The [International Centre for Missing & Exploited Children \(ICMEC\)](#) is one of the many organisations which provided educational resources on dealing with child online protection during the COVID-19 pandemic. For instance, these short videos, aimed at youth-serving professionals, tackle specific issues.

[Embed

[Introduction to child protection during the pandemic](#)

[Question 1 – What should we watch for?](#)

[Question 2 – Who is vulnerable at this time?](#)

[Question 3 – How can I support colleagues and parents?](#)

[Question 4 – What reporting and response options are available?](#)


[Question 5 – What resources are useful right now?\]](#)

[ICMEC's COVID-19 resource page](#) has many other resources for dealing with other child protection issues, including multilingual content, webinars (recordings) for parents and educators, and resources for children.

Awareness campaigns (ACE community to share)

As part of the [Safer Internet Day celebrations, in 2021](#), the regulator Communications Authority of Kenya, GSMA and mobile operators: Safaricom PLC, Airtel Kenya, Telkom Kenya and Jamii Telecommunications Ltd launched [a micro-site](#), with an interactive Child Online Protection Guide under the umbrella of the GSMA #WeCare initiative. The site offers safety tips for children and parents/guardians on four pillars: [Smart Tips](#) [Cyber Bullying](#) [Online Fraud](#) [Internet Addiction](#).

3.5 Developing a national strategy

-  *Why is a national strategy on child online protection essential?*

In order to protect children from online risks while promoting access to information and the safe use of technology and the internet, it is necessary to develop, run, and assess an inclusive, multifaceted child online protection strategy. This can ensure coordinated action and cooperation across all levels. For a strategy to be effective, it should have targeted measures and activities, including financial and human resources to implement the strategy .

The International Telecommunications Union (ITU), together with expert partners, has produced [a number of guidelines on child online safety as part of its Child Online Protection \(COP\) initiative](#) (within its Global Cybersecurity Agenda, a framework for international collaboration on cyberspace). The special value of these guidelines is that they were written for specific stakeholder groups, and address those stakeholders' particular roles and needs.


In particular, the [guidelines for policymakers](#) offer governments and policymakers 'a user-friendly and flexible framework that supports the development of targeted and effective measures for child online protection at the national level'.

Resources

The ITU Guidelines on Child Online Protection are a comprehensive set of recommendations for all relevant stakeholders on how to contribute to the development of a safe and empowering online environment for children and young people.

There are four sets of 2020 Child Online Protection (COP) Guidelines:

- Guidelines aimed at [policymakers](#);
- Guidelines for the [industry](#);
- Guidelines for [parents and educators](#); and
- Guidelines aimed at [children](#).

-  *What are the steps, requirements, and measures that need to be considered when formulating a national strategy on online child safety?*

From a practical point of view, the [ITU Guidelines on Child Online Protection for Policymakers](#) provide a 'national checklist' of requirements and measures that can address the risks, aimed at helping policymakers with planning a national strategy.

The checklist is based on several key areas. Table 1, reproduced from the guidelines, describes a number of factors that policymakers need to keep in mind.

	#	Key areas for consideration
Legal framework	1	Review the existing legal framework to determine that all necessary legal powers exist to enable law enforcement and other relevant agencies to protect persons under the age of 18 online on all internet-enabled platforms.
	2	Establish, mutatis mutandis, that any act against a child which is illegal in the real world is illegal online and that the online data protection and privacy rules for children are also adequate.
Regulatory framework	3	Consider regulatory policy development. This may include a self- or co-regulatory policy development as well as a full regulatory framework. The self- or co-regulatory model might include the formulation and publication of codes of good practice or basic online safety expectations, both in terms of helping to engage, coordinate or orchestrate and sustain the involvement of all relevant stakeholders,

		<p>and in terms of enhancing the speed with which appropriate responses to technological change can be formulated and put into effect.</p> <p>A regulatory model might define the expectations and obligations across stakeholders and enshrine within a legal context. Penalties for policy infringement may also be considered.</p>
Reporting - illegal content	4	<p>Ensure that a mechanism is established and is widely promoted to provide readily understood means for reporting the variety of illegal content found on the internet. For example, a national hotline, which has the capacity to respond rapidly and have illegal material removed or rendered inaccessible.</p> <p>Industry should have mechanisms to identify, block, and remove abuse of children online, taking all services relevant to their organisations.</p>
Reporting - user concerns	5	<p>Industry should provide users with the opportunity to report concerns and issues to their users and respond accordingly.</p>
Actors and stakeholders	6	<p>Engage all the relevant stakeholders with an interest in online child protection, in particular:</p> <ul style="list-style-type: none"> - Government agencies - Law enforcement - Social services organisations - Internet Service Providers (ISPs) and other Electronic Service Providers (ESPs) - Mobile phone network providers - Public Wi-Fi providers - Other relevant hi-tech companies - Teacher organisations - Parent organisations - Children and young people - Child protection and other relevant NGOs - Academic and research community - Owners of internet cafés and other public access providers e.g. libraries, telecentres, 'PC Bangs', and online gaming centres, etc.
Research	7	<p>Undertake research of the spectrum of national actors and stakeholders to determine their opinions, experiences, concerns, and opportunities with regards to child online protection. This should also appreciate the extent of any responsibility together with existing or planned activities to protect children online.</p>
Education digital literacy and competency	8	<p>Develop digital literacy features as part of any national school curriculum that is age appropriate and applicable to all children.</p>
Educational resources	9	<p>Draw on the knowledge and experience of all stakeholders and develop internet safety messages and materials which reflect local cultural</p>

		<p>norms and laws, and ensure that these are efficiently distributed and appropriately presented to all key target audiences. Consider enlisting the aid of the mass media in promoting awareness messages. Develop materials which emphasise the positive and empowering aspects of the internet for children and young people and avoid fear-based messaging. Promote positive and responsible forms of online behaviour.</p> <p>Consider developing resources to help parents assess their own children's online safety and learn about how to minimise risks and maximise potential for their own family through targeted education.</p>
Child protection	10	Ensure that universal and systematic child protection mechanisms are in place that oblige all those working with children (social care, health, schools, etc.) to identify, respond, and report incidents of abuse and harm that occur online.
National awareness	11	Organise national awareness campaigns to create the opportunity to universally highlight child online protection issues. It may be beneficial to harness global campaigns such as Safer Internet Day to build a campaign.
Tools, services, and settings	12	<p>Consider the role of device settings, technical tools (such as filtering programmes), and child protection apps and settings that can help.</p> <p>Encourage users to take responsibility for their devices by encouraging updates of the operating system, plus the use of suitable security software and apps.</p>

Table 1. Developing a national child online protection strategy: A national checklist - Key areas for consideration

Source: The table has been reproduced from the [ITU Guidelines on Child Online Protection for Policymakers 2020](#)

 **Reflection point**

Does your country have a national strategy on child online protection? Or is it in the process of developing one, or updating an existing one? If yes, which stakeholder has been the driving force behind it? And which key areas are the most challenging to tackle?

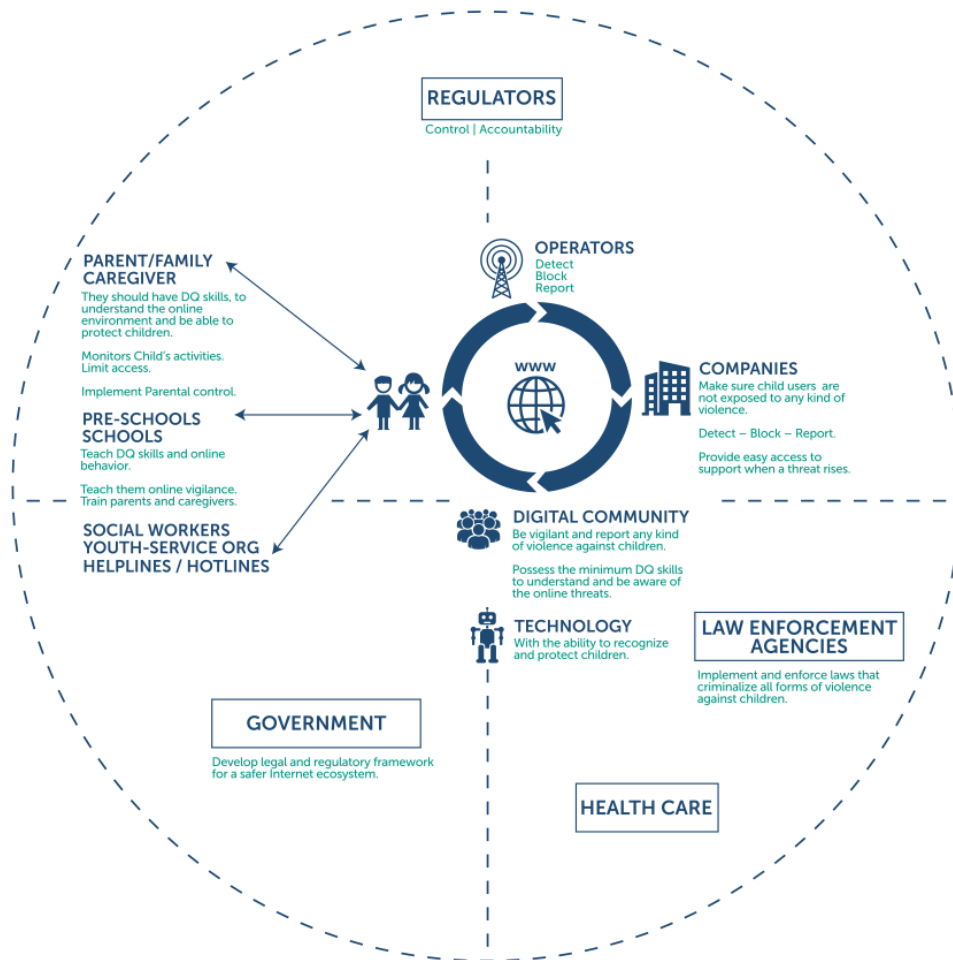
If not, what has been the main setback for not having a national strategy? Who would/could be the driving force behind such an initiative?

4. The stakeholders involved in protecting children online

As was discussed in the previous section, there is no single solution to mitigate the risks children face using the internet. Rather, a combined approach can be used to tackle the risks in a broad way.

The combined approach requires the involvement of all stakeholders, including parents, educators, governments, and the industry (Figure 6).

Safer Internet Ecosystem



Source: Lina Fernandez del Portillo.

To fully protect children from online harm or exposure to unacceptable online risk, all relevant stakeholders must be informed, empowered and engaged.

Figure 6. A safer internet ecosystem

Source: [Report by ITU/UNESCO Broadband Commission on Child Online Safety](#) (2019)

4.1 A shared responsibility of all stakeholders

-  *What are the roles and responsibilities of each stakeholder?*

The stakeholders involved in ensuring that children are protected online include:

- National governments have an obligation to protect children and young people both online and offline. Some of the key requirements for online protection include ensuring that national legislation is fit for this purpose, that law enforcement has the right skills, and that hotlines are in place.
- At the national level, law enforcement agencies need the capacities and skills to combat online child sexual abuse. Based on evidence, provided in part by child sexual abuse content, law enforcement agencies work to locate victims and remove them from harm, as well as to locate the perpetrators. Law enforcement also works at regional and international levels to combat online child sexual abuse. The capacities, skills, and other resources required by law enforcement are crucial: unless laws are actually enforced, children cannot be protected to the extent that they should.
- The industry also has a responsibility to ensure that the online environment is safe and secure. Service providers can play a key role in creating such an environment, and many tools – such as filters and reporting mechanisms – can be used to this effect. The industry favours self- and co-regulation, which has been recognised as an effective approach. In addition, the industry has been particularly highly active in the area of combatting online child sexual abuse. Apart from individual actors in the ICT industry, a number of industry coalitions have also been formed (more on this further down).
- Children’s NGOs and child helplines and hotlines are key stakeholders in the fight against child sexual abuse and exploitation – both online and offline – and are valuable partners in understanding the scale and nature of the problem, and also in providing counselling and support for victims of abuse. National NGOs may also cooperate through international networks.
- Parents and educators have a responsibility to guide and support children, especially younger children, to use services that promote positive behaviours. They play an important role in education and awareness, which is considered to be an important first line of defence in mitigating the risks.

Case study

Google’s Be Internet Awesome Programme

Google in 2020 launched its child online safety programme, [Be Internet Awesome](#), in South Africa and Nigeria. Through the programme children learn qualities such as being smart, alert, strong, kind, and brave that enable them to explore the online world with confidence.

The Be Internet Awesome curriculum offers resources for educators and children in five fundamental topics:

- Share with Care: Digital Footprint and Responsible Communication
- Don't Fall for Fake: Phishing, Scams, and Credible Sources
- Secure Your Secrets: Online Security and Passwords
- It's Cool to Be Kind: Combating Negative Online Behaviour
- When in Doubt, Talk It Out: Questionable Content and Scenarios

Case study


How stakeholders in Kenya have teamed up to run a national child safety campaign

In September 2021, the Communications Authority of Kenya launched a three-month [awareness campaign to protect children and their digital footprint](#), as it steps up advocacy on responsible use of the internet.

The stakeholders involved, together with the Communications Authority, are:

- The Ministry of Education
- The Ministry of ICT Innovation and Youth Affairs
- The Justice sector under the auspices of the National Council on the Administration of Justice
- The private sector, which is exploring ways of deploying technology to facilitate teaching and learning for children during school closures.

4.2 How are the stakeholders collaborating

-  *How are the stakeholders collaborating on national, regional, and global levels? What are some of the main examples?*

Protecting children online requires the involvement of all stakeholders, who must act together in an effective and coordinated manner to safeguard children online, and to combat online child sexual abuse. Ongoing efforts, which are particularly relevant in the fight against child sexual abuse, include:

- Public-private partnerships, such as the [WePROTECT Global Alliance](#); the [Global Partnership to End Violence Against Children](#); and the [Alliance to Better Protect Minors Online](#).
- Financial coalitions, such as the [US Financial Coalition Against Child Sexual Exploitation](#) and the [Asia-Pacific Financial Coalition Against Child Sexual Exploitation](#).

- Industry alliances, such as the [Technology Coalition](#), and [GSMA's Mobile Alliance Against Child Sexual Abuse Content](#).
- UN agencies, such as UNICEF, UNESCO, the United Nations Office on Drugs and Crime (UNODC), the ITU, and the ITU/UNESCO Broadband Commission, including its [Working Group on Child Online Safety](#).
- National NGOs, which may cooperate through international networks, such as [ECPAT International](#), and [ICMEC](#).
- Children's helplines and NGOs, such as [Child Helpline International](#) and [Childnet International](#).
- Other regional and global initiatives and organisations focusing on child online safety, such as the [Better Internet for Kids](#), [EU Kids Online](#) and [Global Kids Online](#).



Reflection point

The involvement of all stakeholders is vital. In your country, how are the different stakeholders involved in child online safety?

5. Resourcing Child Online Protection Initiatives

Child online protection initiatives require resources: people (champions) and funding. In most cases, resources to support initiatives come from the government, international organisations, and the civil society.



Case study

Africa Online Safety Fund

In partnership with South African social impact advisory firm [Impact Amplifier](#) and [Institute of Strategic Dialogue](#), in recognition of the Safer Internet Day, Google announced a US\$1M pan-African fund to support innovative ideas around privacy, trust, and safety for families online across sub-Saharan Africa, in 2020.

The Africa Online Safety Fund aimed to support transformative and catalytic solutions that address identity theft, bullying and harassment, sex trafficking, hate crimes, terrorist recruitment and promotion, misinformation and disinformation, and financial scams, particularly for women and children in Nigeria, South Africa, Kenya, Senegal, Ethiopia, and Côte d'Ivoire.

[Winners of the fund](#) included 8 organisations awarded US\$100,000 for transformative solutions, and 18 winners of US\$10,000 offering catalytic projects.

6. Conclusion

This module looked at the opportunities and risks for children and their use of technology. There are a few important takeaways from this module, which we will now summarise.

First, discussions on children's protection online can benefit greatly from a rights-based approach, which places children's rights at the heart of the discussion. With such an approach, practitioners can focus on maximising the opportunities of the digital world for children and young people, while fostering a safe and secure online environment.

Second, there is no doubt that there are many online risks for children, which we identified as (a) inappropriate content, (b) inappropriate contact, (c) inappropriate conduct, (d) health-related risks, and (e) consumer-related issues. Without downplaying these risks, it is good to keep what various studies have concluded: although children and young people are exposed to risks and could be taking risks online, they are not necessarily experiencing actual harm.

Third, no single solution can mitigate the risks children face using the internet. Rather, a combined approach can tackle the risks in a broad way. This approach combines policy, the work of law enforcement, the use of technical tools, the increase of education and awareness, and the provision of support for children seeking advice and help, and for victims of abuse. Such an approach is required both on a national level and as a global response.

Fourth, when it comes to child abuse and exploitation, technology has amplified the problem since perpetrators can capture the abuse through digital means (images or videos). The internet, including the darknet, has also amplified the issues, since it provides a relatively easy means of accessing and consuming abuse material. This raises significant issues for all stakeholders.

Fifth, combatting online child sexual abuse and exploitation also requires a combined approach, involving collaboration among stakeholders on a national, regional, and global level.