



UNITED NATIONS CHILDREN'S FUND

Protecting Children from Online Exploitation and
Cyberbullying.

LETTER FROM THE EXECUTIVE BOARD

Greetings Delegates of the committee,

It is a great honour for us to serve as the Executive Board of United Nations Children's Fund and we are really excited and looking forward to meeting you all at the conference. We are thrilled to have you join us for this exciting and academic discussion.

In the committee, you'll be young leaders who will be talking about the agenda at hand: Discussion on "Protecting Children from Online Exploitation and Cyberbullying.". Always remember that change begins when young minds decide to take action, let this be the motivation for everyone and anyone who walks into the conference.

We believe that through collaboration, diplomacy, and innovative solutions, we can make a meaningful impact on these challenges. Over the course of the conference, you will have the opportunity to engage in spirited debates, negotiate resolutions, and forge lasting friendships with delegates from diverse backgrounds. We encourage you to approach each session with an open mind, a spirit of cooperation, and a determination to make a positive difference.

This background guide only provides a rough idea of the agenda of the committee and will help you get a basic idea regarding the topic which the committee will be deliberating upon but remember this study guide is not exhaustive and we are forward to see your research for the debate in the committee.

As you embark on this MUN journey, remember that you are not only representing your assigned country or committee but also contributing to the larger goal of promoting peace, understanding, and diplomacy.

We'll also love to see your creativity and research in debate as well as the end document. You will be marked upon the criterion which includes your research, Debate, and diplomacy. We thank all of you for your commitment and wish you all a stimulating conference. The anticipation of a memorable session.

Akanksha Vats (*Chairperson*)

Shreyas Puri (*Vice Chairperson*)

ABOUT THE COMMITTEE

1. INTRODUCTION TO THE COMMITTEE

UNICEF, originally established as the United Nations International Children's Emergency Fund, is a cornerstone of the UN system. Their mission is clear: to help mothers and children in need, wherever they may be.

UNICEF tackles challenges on multiple fronts. They provide emergency relief during crises, while also offering long-term support for development in vulnerable areas. Their primary focus is on ensuring the well-being and rights of every child. This includes guaranteeing access to essential services and opportunities that allow children to thrive.

UNICEF has a vast network of partners, allowing them to create and deliver programs that address the specific needs of children and mothers facing hardship. As a result, they've become a symbol of hope for millions around the world. During times of crisis, UNICEF provides vital assistance, helping families weather difficult situations.

Through its unwavering commitment to humanitarian principles and its tireless efforts to alleviate suffering and promote resilience, UNICEF plays a pivotal role in advancing the global agenda for children's rights and wellbeing.

1.1. History:

Established by the United Nations General Assembly in December 1946, the United Nations International Children's Emergency Fund (UNICEF) emerged from the immediate post-war context. Its initial mandate was to address the dire humanitarian needs of children in war-torn Europe and China. Focused on emergency relief, UNICEF provided essential supplies like food and medical care, alleviating immediate suffering.

However, UNICEF's mission demonstrably evolved. Recognizing the ongoing challenges faced by children globally, the organization transitioned from solely responding to emergencies. It began implementing sustainable solutions, promoting the well-being and rights of children worldwide. This expanded focus encompassed key areas such as health, education, protection, and overall welfare. Consequently, UNICEF became a leading advocate, championing children's rights across diverse contexts.

1.2. Mission:

UNICEF is mandated by the United Nations General Assembly to advocate for the protection of children's rights, to help meet their basic needs, and to expand their opportunities to reach their full potential.

UNICEF is guided by the Convention on the Rights of Children and strives to establish children's rights as enduring ethical principles and international standards of behaviour towards children.

UNICEF insists that the survival, protection and development of children are universal development imperatives that are integral to human progress.

UNICEF works with all its partners towards the attainment of the sustainable human development goals adopted by the world community and the realization of the vision of peace and social progress enshrined in the Charter of the United Nations.

1.3. Mandate:

UNICEF has a mandate to safeguard the rights of all children, everywhere. That mandate is rooted in the 1989 Convention on the Rights of the Child (CRC), which sets out universal and indivisible rights that apply to every child, and the Sustainable Development Goals (SDGs) adopted by world leaders in 2015, which apply to every country.

In the 21 countries and territories in Europe and Central Asia where UNICEF have programmes, their focus is on the children who are overlooked and left behind by economic and social progress. Even in the most prosperous nations, there are always children who, because of who and where they are, do not get the childhood they deserve - and to which they are entitled under the Convention.

UNICEF remind governments in the region of the commitments they have made to all children through the CRC and the SDGs and help them monitor their progress.

1.4. Functions:

UNICEF, the UN's children's agency, is a global advocate for the well-being and rights of all children. Their unwavering commitment extends to areas facing poverty, violence, and crisis, where children are especially vulnerable.

UNICEF takes a multi-pronged approach. They fight for laws that prioritize children's welfare and hold violators accountable – from child recruitment to sexual abuse.

To address the complex challenges children face during crises, UNICEF offers a diverse range of programs. This includes education, job training, and crucial psychosocial support to help children heal from trauma. They even work to reintegrate child soldiers back into society.

Education is a cornerstone of UNICEF's work. They support educators in conflict zones and rebuild schools, ensuring children have a chance for a brighter future. Alongside this, UNICEF provides essential humanitarian aid – food, water, and medical care – to meet children's basic needs.

Most importantly, UNICEF prioritizes protecting children during conflict. They use communication and mediation strategies to create a safer environment for them.

By combining expertise, resources, and global partnerships, UNICEF strives for a world where children's rights are respected, and their well-being is safeguarded, no matter the circumstances.



INTRODUCTION TO THE AGENDA

“Protecting Children from Online Exploitation and Cyberbullying.”

INTRODUCTION

The digital environment has the potential to offer children incredible opportunities. The UN Committee on the Rights of the Child has affirmed that meaningful access to digital technologies can support children to realise the full range of their rights. Children use the internet to learn, connect with others, and express themselves in ways previous generations could only imagine. Digital technology is an integral part of many children’s daily lives. However, the internet and many digital technologies were not designed with children and their rights in mind. While recognising the potential positive opportunities, there are serious risks of harm that need mitigation. The need to protect children online will only increase as countries become more connected and technology development accelerates.

Children can be exposed to cyberbullying, harmful information or abusive material, groomed by potential predators and subjected to abuse and exploitation, including through sexting, the production and distribution of images depicting child abuse and live web streaming. ICTs have significantly facilitated the production, distribution and possession of child abuse images and with rapidly developing technology, the number of perpetrators is growing.

Online child sexual exploitation encompasses several forms, some of which may intersect, such as the production, sharing and possession of child sexual abuse materials, including computer-generated child sexual abuse materials, grooming for sexual abuse, trafficking for sexual exploitation, and sexual extortion.

Online violence is often associated with incidents of abuse generated elsewhere, but the screen does more than reflect the multiple faces of violence that children are exposed to at school, in the community or in the family. ICTs become the entry point to an endless maze of mirrors that multiply its impact, where identifying and protecting victims, investigating criminal activities and dealing with illegal and harmful content become increasingly challenging.

Cyberbullying is defined as “an aggressive, intentional act carried out by an individual or a group using electronic forms of contact against a victim who cannot easily defend himself or herself. It is typically carried out repeatedly and over time, and is often characterized by an imbalance of power”. It does not require the physical presence of the victim; indeed, it can be facilitated by anonymity. A single act online can be observed and disseminated by a large number of people, making it very difficult to assess how the victim will experience or re-experience it.

Distinguishing Between Exploitation and Cyberbullying

Cyberbullying may include spreading rumours, posting false information or hurtful messages, embarrassing comments or photos, or excluding someone from online networks or other

communications. Often resulting from face-to-face interaction in the school or other social spaces, it can cause particularly profound harm, as it can affect the child victim at any time and quickly reach a very wide audience.

Cyberbullying is one of children's greatest concerns when navigating the online world. Research in Europe indicates that receiving hurtful messages is the least common risk for children online but is the most likely to upset them; the majority of children affected by such messages called on social support and 6 per cent used strategies to delete or block those messages.

Although there are still data gaps in different regions, it is clear that cyberbullying is weighing on children's minds and prompting them to seek support. Data collected by Child Helpline International confirm that around the world cyberbullying is a frequent reason for children to call a helpline: in 2014 there were 27,847 contacts relating to cyberbullying made to helplines.

Grooming is defined as a "process intended to lure children into sexual behaviour or conversations with or without their knowledge, or a process that involves communication and socialization between the offender and the child in order to make him or her more vulnerable to sexual abuse".

Cyberbullying may in fact include the posting and dissemination of sexual images and can be associated with different forms of sexual abuse.

Historical Background and Global Relevance

The number of images of child abuse on the Internet has reached an unprecedented level. Their dissemination by the millions to many individual offenders is facilitated by the use of smart phones. Encrypted networks allow sex offenders to share such material undetected, posing added challenges for criminal investigations and prosecutions. It is estimated that the number of child abuse images on the Internet increased by 1,500 per cent from 1997 to 2006. This growing trend persists: according to INHOPE (International Association of Internet Hotlines), a collaborative network of 51 hotlines, between 2012 and 2014 the number of URLs containing child sexual abuse material inserted into its reporting management system increased by 139 per cent. The children depicted are increasingly younger: more than 80 per cent are 10 years of age or under and 3 per cent are 2 years of age or younger. Once online, images of child sexual abuse can circulate indefinitely, perpetuating the abuse of the victim. Beyond the serious harm done to child victims, the circulation of such images sustains harmful social attitudes that tolerate the demand, which fuels the further exploitation of children and increases the risk of abuse.

In 2011, the OECD recognised a number of risks associated with children and the digital environment. At that time, the OECD placed online risks into three broad categories: content and contact risks; consumer related risks; and privacy and security risks. Whilst these categories persist today, the substantive acts underlying these risks have evolved and changed. For example, whilst cyberbullying was a definite concern in 2011, in the 2017 OECD Survey it was identified by member countries as the highest priority risk.

Issues that did not exist or were not highly visible in 2011, such as sexting or sextortion, are identified as new concerns. The concept of a conduct risk that is, where the child is the actor in a peer-to-peer exchange, such as in sexting was not previously recognised by the OECD. Children today are more

likely to face increased privacy risks, be exposed to hateful, harmful or offensive content online, and may be the subject of targeted advertising or face financial inducements associated with online gaming.

All countries report a variety of approaches, including legislative, self- and co-regulatory, technical, awareness-raising, and educational measures. These multi-layered policy approaches depend on a range of agencies and distributed governance, raising a number of challenges. Compared to 2011, there are promising moves by a number of countries to address this complexity through the development of a strategic vision and the creation of a centralised institution.

SCOPE AND DIMENSIONS OF THE PROBLEM

Gender-Based Vulnerabilities

Violence online that threatens girls and women with sexual violence and killing has been employed to intimidate them and has been found to result in significant psychological trauma, causing loss of confidence and self-exclusion from the internet. Subsequently, this can restrict girls from accessing educational, social, and political opportunities. In a single international poll, 38% of girls reported being harassed or abused online and 24% of those who reported being harassed stated it occurred on a social network site. Girls are disproportionately targeted in image-based abuse, including the non-consensual sharing of intimate images.

The sexualisation of the online abuse of girls is common, encompassing sexual assault threats, sending unwanted explicit material, and sexist or degrading language. For boys, violence also occurs but is more likely to be physical threats, homophobic language, or bullying boys into aggressive or hypermasculine acts. Stigma towards online sexual abuse can prevent girls from reporting the experiences or seeking assistance, resulting in underreporting and longer suffering.

Psychological, Social, and Educational Effects on Children

Watching violent and exploitative material, or being bullied or groomed, can have serious psychological effects on children, such as anxiety, depression, trauma, self-inflicted harm and even suicidal thoughts. Victims of cyberbullying tend to perform badly academically as they stay away from school to avoid bullying or witness a decline in concentration and school work because of stress and anxiety. Most children pull back from online spaces because of fear or distress and risk ending up isolated with no online social support networks. In children and youth, the psychological consequences of bullying and cyberbullying can be stress, anxiety, low self-esteem, and a feeling of helplessness.

Chronic mental health conditions and long-term developmental effects can result from long-term exposure to online abuse. Long-term psychological and psychiatric care might be needed for children suffering from online sexual exploitation. Research into the effects of cyberbullying has shown that the adverse emotional consequences can last several years, especially when the abuse is the sharing of

images or constant public humiliation. In extreme circumstances, online victimisation is associated with post-traumatic stress disorder (PTSD) and long-term social isolation.

Lack of Digital Literacy and Awareness

Despite the growing risks children face online, digital literacy education remains inconsistent across regions. Many school curricula do not include comprehensive education on online safety, leaving children ill-equipped to identify and respond to potential threats. Parents and caregivers often lack awareness of the risks children face online, and may not know how to guide them in safe digital behaviour. This knowledge deficit is aggravated by differences in digital skills among generations. Teachers and schools are not normally trained to respond to online harm and digital safety concerns, leading to low intervention and prevention opportunities. Most children do not report online harm incidents because they are afraid of being excluded from the internet or penalized by parents who lack an understanding of the digital sphere. Low-income and rural children can experience increased risks from non-use of digital literacy schemes, less parental control, and fewer state support services.

Internet use in some localities is communal, using shared access in the context of cybercafés, for instance, which can increase exposure to predatory conduct and diminish the likelihood of adult supervision. Resource-poor governments lack the infrastructure to design and implement online child protection policies, and even when policies are in place, enforcement tends to be poor. Children without online monitoring or access to content filtering are at higher risk of viewing inappropriate material or becoming victims of grooming and online exploitation.

Cultural Barriers and Underreporting

Most types of online abuse are an extension or echo of violence in the home, community or school, and may be compounded by discrimination along lines of gender, disability, ethnicity or other characteristics. Young people do not always tell parents, carers, teachers or other adults about harmful things that have happened to them online because they are afraid of getting into trouble or being blamed. In some other situations, they fear losing access to their devices or the internet in general. When caregivers lack digital literacy, it makes it challenging for children to report or for adults to identify the risks and react accordingly.

In most cultures, sexual abuse is not openly discussed, particularly among young women and girls. This can discourage victims from reporting abuse based on shame, stigma, or fear of isolation. In societies where family honour and reputation are prioritized, reporting sexual exploitation can result in victim-blaming or even punishment for the child. Peer pressure and social norms tend to discourage children from informing others when they experience harassment or bullying online. There is frequently a fear of reprisal, either from peers or adults. Girls are potentially at increased risk of being blamed for harassment, and exploitation and having a culture of silence maintained. Within marginalized communities, restricted access to support services and lack of confidence in authorities further decrease the opportunity for reporting. Underreporting is also increased by the lack of child-friendly reporting procedures. The majority of systems are inaccessible or not culturally suitable, and children are likely unaware of how or where to report abuse. Victims of exploitation or cyberbullying who are already marginalized, for instance, because of poverty, migration status, disability, or membership of a minority group can be confronted with additional barriers to reporting and accessing

justice. The risk of not being believed or supported can deter children from making known what occurred to them.

AI-Generated Exploitation and Deepfakes

The online world has become ever more complicated with the intervention of Artificial Intelligence, algorithms and automated decision-making systems. Deepfake technology is available that enables superimposing children's faces on abusive material, generating synthetic sexual images that look more and more real. These new types of abuse pose special difficulties to child protection services and law enforcement, as in them, no direct contact with the child might be involved but still, significant psychological and reputational damage is done. Software tools are used by some perpetrators to manipulate available photos or movies to produce new abusive material, such as simulations of non-existent victims. New technologies enable perpetrators to be anonymous and operate freely across boundaries. This introduces new challenges for investigation and prosecution. The form of AI-generated abuse defies established legal definitions of child sexual abuse material, resulting in regulatory uncertainty and differing enforcement across jurisdictions. Industry codes highlight the importance of proactive detection technology and effective content moderation to detect and eliminate synthetic abuse materials. Voluntary systems for industry self-regulation have been only minimally effective in countering abuse of AI for malicious means. There is a large gap between the speed of technological development and the generation of regulatory mechanisms. Children's rights are not sufficiently taken into account in the development of AI systems. AI tools that profess to identify grooming or recognize dangerous content are frequently not transparent and accountable, and there is limited data on their efficacy.

The application of predictive analytics in measuring children's behavior on the web presents serious ethical issues, particularly where it is based on incomplete or skewed data. There are jurisdictions with uncertain legislation concerning deepfake material concerning children, rendering it challenging to prosecute even where harm is clear. Detection is not the only challenge but also how to respond to harms that are unseen, like emotional trauma, reputational harm, or social exclusion by manipulated content. Children's images and information are routinely gathered without their consent or understanding, exposing them further to privacy threats and exploitation. With growing awareness, international collaboration to counter AI-generated child sex abuse is still patchy and inadequate. Technology-facilitated abuse progresses faster than the law, and loopholes are often taken advantage of by abusers who utilize encrypted websites and anonymizing services. Though there are some firms that have created AI classifiers to identify known abusive content, synthetic or manipulated material is still hard to flag or delete at scale.

INTERNATIONAL TREATIES AND CONVENTIONS

1. Convention on the Rights of the Child (CRC)

Adopted in 1989, the Convention on the Rights of the Child is the cornerstone of international legal instruments to protect children's rights. Though drafted before the rise of the internet, it offers a robust legal framework for addressing online violence and exploitation. Article 19 obligates states to protect children from all forms of violence, including psychological abuse and cyberbullying.

The Committee on the Rights of the Child, in its **General Comment No. 13 (2011)**, explicitly recognizes cyberbullying and calls for educational measures, accurate and age-appropriate information regarding self-protection, and children's empowerment. The Committee emphasized that responsibility to prevent and tackle cyberbullying ultimately rests with the State.

2. Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography (2000)

This protocol expands the obligations of states under the CRC by specifically addressing child sexual exploitation, including when facilitated through digital technologies. It obliges states to criminalize child pornography and prostitution, regardless of whether the acts occur offline or online. It reinforces the need for international cooperation and victim protection in addressing these crimes.

3. Council of Europe Convention on Cybercrime (Budapest Convention)

The **Budapest Convention** is the first international treaty on crimes committed via the Internet and other computer networks. It aims to harmonize national laws, improve investigative techniques, and increase international cooperation. It addresses the protection of children from exploitation online by mandating legal frameworks against offenses such as child pornography, grooming, and the production/distribution of illegal content.

4. Council of Europe Lanzarote Convention

The **Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)** obliges parties to criminalize all forms of sexual abuse of children, including acts committed online. It promotes preventive and protective measures, support for victims, and international collaboration in tackling online child sexual exploitation.

5. United Nations Guiding Principles on Business and Human Rights

Adopted by the UN Human Rights Council in 2011, these principles set out the duty of businesses to respect human rights, including children's rights. Companies are expected to avoid infringing on child rights and address adverse impacts, both online and offline. Businesses are encouraged to conduct due diligence and impact assessments with regard to their digital operations.

6. Children's Rights and Business Principles

Developed by UNICEF, **Save the Children**, and the **UN Global Compact**, these principles urge companies to respect and support children's rights throughout their business practices. The principles cover data protection, child safety in advertising, responsible digital platform design, and safeguarding against digital exploitation.

7. ITU Guidelines on Child Online Protection

The **International Telecommunication Union (ITU)**, in collaboration with UNICEF and other stakeholders, issued **Child Online Protection Guidelines** aimed at various sectors—industry, parents, educators, and governments. These guidelines promote a safe and secure digital environment through:

- Criminalization of child sexual abuse material online
- Support systems for victims
- Age-appropriate content filtering
- National policy frameworks
- Industry codes of conduct

The guidelines emphasize the importance of integrating digital safety into national education and cybersecurity strategies.

8. General Comment No. 25 on Children’s Rights in the Digital Environment

Issued by the **Committee on the Rights of the Child**, this comment elaborates on how children’s rights—such as the right to privacy, protection from violence, freedom of expression, and access to information—must be upheld in digital contexts. It was informed by consultations with 709 children across 28 countries.

It emphasizes:

- The indivisibility of children’s rights online and offline
- The need for age-appropriate policies
- Regular research to understand digital risks
- Inclusion of children’s voices in policy formation.

9. WePROTECT Global Alliance

Launched by the UK government, **WePROTECT** unites governments, tech companies, law enforcement, and civil society to combat online child sexual exploitation. Its **Model National Response** framework recommends:

- Victim identification and support
- Investigation and prosecution of offenders
- Preventive educational measures
- Industry cooperation for content takedown

WePROTECT emphasizes multi-stakeholder accountability and has been endorsed in summits held globally.

10. OECD Recommendation on the Protection of Children Online

Adopted in 2012, this recommendation focuses on policy coordination, evidence-based decision-making, and international cooperation. It emphasizes the challenges of balancing protection and empowerment in the digital environment. The OECD has also recognized newer threats like sexting, sextortion, and harmful online content.

11. Better Internet for Kids (BIK)

Supported by the **European Commission**, this platform aims to build a safer and empowering online experience for children and adolescents. BIK provides resources for:

- Positive digital content
- Online safety education
- Youth participation in digital policy
- Collaboration with national Safer Internet Centres across Europe.

12. African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)

Adopted in 2014, this convention addresses data protection and cybersecurity, including child safety online. It urges AU member states to adopt laws to criminalize online child exploitation and create regulatory authorities for enforcement and awareness.

NATIONAL POLICIES AND CYBER LAWS

Since more and more governments around the world recognize the need to build safe and enabling digital environments for children, national policies and cyber laws have evolved in recent years. New and emerging risks remain within the prism of international recommendations, such as the OECD Council Recommendation on the Protection of Children Online and the UN Convention on the Rights of the Child. The following is a comprehensive and strictly sourced account of these national policy and legal developments.

- **Legislative Approaches**

All participating countries in the OECD survey reported having a legislative and policy response of some kind to manage risks to children in the digital world. These included specific legislation to target child protection online up to more general digital strategies that include child safety as an element. The legislative regimes generally cover three major areas: criminality (for example, sexual abuse and harassment), content regulation, and protection of privacy. Most of the legislation is generic in character but has been modified to include online threats. Others have sought to

transpose offline laws into the online environment. Cyberbullying, sexting, sextortion, grooming, and child sexual exploitation are some of the threats that have seen legislation being put in place. For instance, Australia's Enhancing Online Safety Act 2015 established the Office of the e-Safety Commissioner with authority to take down offensive content and apply sanctions. New Zealand's Harmful Digital Communications Act 2015 establishes comparable regulatory provisions.

- **National Oversight Bodies**

Several nations have established statutory oversight institutions to track and respond to children's online safety. They include:

- Australia: Office of the e-Safety Commissioner (Enhancing Online Safety Act 2015)
- Costa Rica: National Online Security Commission (Decree N° 36274, 2010)
- Israel: National Network for the Prevention of Violence and Network Crime against Children and Teenagers (Government Decision, 2016)
- Japan: Headquarters for the Promotion and Development and Support for Children and Young People
- Italy: Permanent Observatory to Protect Children and Fundamental Rights of People on the Internet
- New Zealand: Netsafe (Harmful Digital Communications Act 2015).

These bodies look into complaint administration, raising awareness, coordination of national policies, and interacting with educational and legal institutions.

- **Fragmentation and Challenges**

Even with these efforts, the legislative and policy responses are somewhat fragmented. Countries tend to extend existing frameworks rather than have a single, coherent child-specific strategy. Responses are mostly reactive and triggered by high-profile incidents rather than by systematic, evidence-based planning. For example, anti-cyberbullying legislation in Italy and Austria was enacted after reported suicides resulting from online bullying. This demonstrates a pattern where policies get initiated through a response to the media instead of being planned as a part of long-term strategy. Furthermore, the duty is also often compartmentalized between ministries of justice, education, and health, even though the risks online like sexting and cyberbullying are cross-disciplinary in nature.

- **Policy Frameworks and Complementary Action**

Nations supplement legal responses with policy initiatives addressing education, digital literacy, industrial involvement, and raising awareness. Policy responses typically form part of an overall digital agenda and are executed through collaborations between government departments and civil society.

Examples of national policy mixes and regulatory bodies are:

- Belgium: "Je décide" campaign for online privacy, led by the Data Protection Authority and Child Focus.
- Canada: Canadian Centre for Cyber Security and Innovation and Skills Plan.

- Chile: ENLACES (educational resource integration) and collaboration with mobile phone industry bodies.
- Colombia: Law Against Commercial Sexual Exploitation, National Digital Security Policy (CONPES No. 3854).
- France: Digital Education Unit, Educnum, and E-enfance association.
- Hungary: Digital Child Protection Strategy based on awareness raising, digital literacy, and protection.

- **Cybercrime Task Forces and Law Enforcement**

Most nations have established cybercrime sections in their police departments. Australia's Cybercrime Protocol, for example, gives power to its cyber taskforce to deal with grooming, child pornography, and cyberbullying. Israel, Greece, and Norway have similar departments. There are also provisions for increasing penalties in cases of cybercrimes against children in some nations, for example, Spain, Belgium, and Colombia. Interpol coordinates investigations of child exploitation on the internet at the international level and closely cooperates with national organizations.

- **National Digital Strategies**

Certain nations have taken on national digital strategies with child protection components:

- Poland: Cyberspace Protection Policy (2013), with a focus on national cybersecurity.
- Mexico: National Digital Strategy (2013), with child safety as part of its public safety goals.
- Austria: Digital Roadmap (2017), taking a whole-of-government approach to digital dangers and opportunities for children.

- **Multi-Sectoral Coordination**

In the United Kingdom, the UK Council for Internet Safety (UKCIS) brings together more than 200 stakeholders from government, industry, and civil society. Comparable programs are found in Australia (Online Safety Consultative Working Group) and Costa Rica (National Council of Childhood and Adolescence). The European Union's Better Internet for Children (BIK) Strategy is also a critical one. It funds national Safer Internet Centres (SICs) in member states as well as partner countries such as Norway and Russia. They offer helplines, hotlines, and awareness material, and are crucial for the launch of national-level BIK actions.

- **International Cooperation**

At the global level, bodies such as UNICEF and the International Telecommunication Union (ITU) have been working together on guidelines for child protection. The ITU's Child Online Protection (COP) program works towards safety through legal, technical, and educational approaches. UNICEF and ITU co-created industry guidelines to provide children with online safety.

UNICEF GLOBAL INITIATIVES AND PROGRAMS

UNICEF focuses on the protection of children from violence, exploitation and abuse. The UNICEF Innocenti Research Centre, has prepared a number of reports on the safety on children online, and has launched the Global Kids Online Research Initiative in partnership with the London School of Economics and Political Science and EU Kids Online. Separately, UNICEF partnered with ITU to develop guidelines for industry on online child protection.

Global Kids Online, is a collaborative initiative between the UNICEF Office of Research-Innocenti, the London School of Economics and Political Science, and the EU Kids Online Network. This research seeks to fill a knowledge gap which had existed with regards to comparable evidence from lower and middle income countries across different continents on topics such as skills digital literacy and civic engagement, as well as risk and hurtful behaviour. It aims to provide tools and guidelines to national researchers and comparative analysis of country specific research findings. A comprehensive research synthesis covering 2015–2016 has been completed, and overall, the projects aim to create a researcher's toolkit, which can enable longitudinal and cross-national comparisons so as to create a global knowledge base around children's use of the internet and its associated risks.

The Guidelines for Industry on Child Online Protection are aimed at establishing the foundation for safer and more secure use of Internet-based services and associated technologies for today's children and future generations. In response to substantial advances in technology and convergence, ITU, UNICEF and the COP partners have developed and updated the Guidelines for the broad range of companies that develop, provide or make use of telecommunications or related activities in the delivery of their products and services.

The new Guidelines for Industry on Child Online Protection are the result of consultations with members of the COP Initiative, as well as a wider open consultation that invited members of civil society, business, academia, governments, media, international organizations and young people to provide feedback on the Guidelines. The Guidelines apply to the safety of children when using information and communication technologies (ICTs). They provide advice on how industry can work to help ensure children's safety when using the Internet or any of the associated technologies or devices that can connect to it, including mobile phones and game consoles.

The purpose of this document is to:

- Establish a common reference point and guidance to the ICT and online industries and relevant stakeholders.
- Provide guidance to companies on identifying, preventing and mitigating any adverse impacts of their products and services on children's rights.

The UNICEF Strategic Framework was developed through a participatory process with input and feedback from colleagues across UNICEF. The key authoritative source for this brief is the Committee on the Rights of the Child General comment No. 25 on children's rights in relation to the digital environment. Notably, General comment No. 25 was informed by consultations with 709 children and

young people in 28 countries around the world. These brief highlights four key priority areas and strategic actions for governments to respect, protect and fulfil children's rights to freedom from all forms of violence, abuse, and exploitation in relation to the digital environment.

Protecting children from:

- bullying and harassment
- harmful content
- economic exploitation
- sexual abuse and exploitation.

The digital environment has the potential to offer children incredible opportunities. The UN Committee on the Rights of the Child has affirmed that meaningful access to digital technologies can support children to realise the full range of their rights. Children use the internet to learn, connect with others, and express themselves in ways previous generations could only imagine. Digital technology is an integral part of many children's daily lives. However, the internet and many digital technologies were not designed with children and their rights in mind. While recognising the potential positive opportunities, there are serious risks of harm that need mitigation. The need to protect children online will only increase as countries become more connected and technology development accelerates.

UNICEF has noted that children's rights are largely absent from Internet governance and notably the Council of Europe ('COE') and the Committee on the Rights of the Child ('the CRC Committee') have taken steps to seek to ensure that children's rights are appropriately protected and upheld in any legislative or policy response. Whilst to date, policy measures focus to a large extent on the need to protect children, this emphasis has been noted as contributing to a diminishment of children in their role as individual rights holders. It neglects the fact that they themselves are creators of digital content, have a right to participate in matters that affect them, have a right to provision of information, and a right to a freedom of expression.

The CRC Committee held a general day of discussion in 2014 on Digital Media and Children's Rights. The recommendations from that day included, inter alia, that:

- States should recognise the importance of children's access to, and use of, digital media and information and communication technologies in the promotion of their rights.
- States should undertake on-going research, data collection, and analysis to better understand how children access and use digital and social media, and how it impacts on their lives.
- States should carry out awareness raising activities, and support digital and social literacy skills for children.
- Children's right to privacy in relation to digital media and information needs to be effectively safeguarded.
- States need to address risks posed by digital media and information and communications technologies to the safety of children, including online harassment, access to violent and sexual content, and self-generated sexual content.
- States should provide effective remedies for child victims of online harm.

- States should implement policies to ensure accessibility of online content to children with disabilities.

The Convention on the Rights of the Child, which is the most widely ratified international human rights treaty, sets out the civil, political, economic, social, and cultural rights of children. It establishes that all children have a right to education; to leisure, play and culture; to obtain appropriate information; to freedom of thought and expression; to privacy and to express their views on matters that affect them in accordance with their evolving capacities.

These new Guidelines for Industry on Child Online Protection provide a framework for the increasingly broad range of companies that develop, provide or make use of information and communication technologies in the delivery of their products and services. Such companies are especially well positioned to drive innovative solutions, creating digital platforms that can expand educational opportunities and enable children and young people both to engage in the civic life of their communities to become truly global citizens. Local and national initiatives are critical, and we look forward to collaborating on complementary guidelines for governments that address the formulation, implementation, management and monitoring of Country Action Plans to strengthen child online protection.

SUGGESTED READINGS

- <https://learning.nspcc.org.uk/online-safety/preventing-online-abuse-and-harm>
- <https://www.unicefusa.org/what-unicef-does/parenting/protect-children-cyberbullying>
- [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2025\)769570](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)769570)
- [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769570/EPRS_BRI\(2025\)769570_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769570/EPRS_BRI(2025)769570_EN.pdf)
- https://www.wvi.org/sites/default/files/2023-06/Policy%20Brief%20on%20Children%27s%20Rights%20in%20the%20Digital%20Environment_0.pdf
- <https://www.humanium.org/en/the-risks-for-children-surfing-the-internet/>
- <https://beauftragte-missbrauch.de/en/themen/recht/online-legal-issues>