



UNICEF

STUDY GUIDE

AGENDA

DIGITAL SAFETY AND PROTECTING MINORS ONLINE

CONTENTS

04. INTRODUCTION TO THE UN

05. COMMITTEE OVERVIEW

06. INTRODUCTION TO THE AGENDA

07. KEY DEFINITIONS

09. HISTORICAL CONTEXT

11. CURRENT SITUATION

12. ROOT CAUSES

CONTENTS

14. STAKEHOLDERS

16. EFFECTS / IMPACT

17. CASE STUDIES

21. KEY INTERNATIONAL BODIES

22. PAST SOLUTIONS AND FRAMEWORKS

24. QUESTIONS A RESOLUTION MUST ANSWER

26. BIBLIOGRAPHY

INTRODUCTION TO THE UN

The United Nations is an international organization founded in 1945. Currently made up of 193 Member States, the UN and its work are guided by the purposes and principles contained in its founding Charter. The UN has evolved over the years to keep pace with a rapidly changing world. But one thing has stayed the same: it remains the one place on Earth where all the world's nations can gather together, discuss common problems, and find shared solutions that benefit all of humanity.

The main purpose of the United Nations is to maintain international peace and security, develop friendly relations among nations, promote human rights, and encourage international cooperation in addressing global challenges. The organization serves as a global platform where countries can collaborate to address common challenges such as conflict, poverty, inequality, climate change, and humanitarian crises. It operates under the principle of sovereign equality, where every member state has equal representation in the General Assembly, regardless of its economic or political stature. Through its various organs, agencies, and offices located in New York, Geneva, Vienna, and Nairobi, the UN continues to play a central role in promoting peace, security, development, and human rights worldwide.

COMMITTEE OVERVIEW

UNICEF is the United Nations agency dedicated exclusively to children, from vaccines and nutrition to education, child protection, and, increasingly, children's rights in digital spaces. Its work is guided by a rolling Strategic Plan, currently organised around five goal areas, of which is children protection from violence, exploitation, and abuse. It supports governments in drafting child-friendly laws and policies, funds and runs protection programmes on the ground, produces research and data that other actors rely on, and brings together governments, industry, and civil society around shared standards.

UNICEF cannot pass binding international law, prosecute offenders, or compel a state to change its domestic legislation; its recommendations carry political and moral weight, not legal force. It depends entirely on voluntary contributions rather than assessed UN dues, so its programming is shaped by what donors choose to fund. It also works by invitation – respecting national sovereignty means UNICEF partners with governments rather than acting unilaterally inside their borders.

INTRODUCTION TO THE AGENDA

Roughly four in five young people worldwide are online, and that number keeps climbing as connectivity spreads and children start using devices at younger ages. The internet gives children access to education, creative expression, and connection, but it has also become a space where they can be groomed, exploited, bullied, and profiled, sometimes by strangers and sometimes by the very platforms designed to keep them engaged.

This agenda matters now because the pace of technological change has outrun the pace of regulation. Millions of reports of child sexual exploitation are filed every year, generative AI has opened entirely new categories of harm, and states are experimenting with very different solutions – from strict age limits to platform design rules – without any real consensus on what works.

KEY DEFINITIONS

Digital Environment: the internet, mobile devices, and digital services considered together – the space within which children's rights must be respected, protected, and fulfilled, per General Comment No. 25.

Child Sexual Abuse Material (CSAM): images, videos, or other content depicting the sexual abuse or exploitation of a child; the largest single category of harm reported to child-protection hotlines.

Online Child Sexual Exploitation and Abuse (OCSEA): an umbrella term covering CSAM, grooming, sextortion, and other technology-facilitated sexual crimes against children.

Grooming and Sextortion: grooming is the process of building a child's trust, typically online, in order to abuse or exploit them later; sextortion is a form of enticement in which a child is coerced into providing sexual images or acts, often under threat of exposure.

Age Verification / Age Assurance: technical or procedural methods used to confirm a user's age before granting access to a platform, ranging from self-declaration to ID checks and facial-age estimation.

Duty of Care / Safety by Design: a regulatory approach requiring platforms to assess and mitigate risks to users, and to build safety into a product's design from the start rather than reacting to harm after it occurs.



HISTORICAL CONTEXT

1989 – Convention on the Rights of the Child: the foundational, near-universally ratified treaty establishing children's rights to privacy, protection from exploitation, and access to information.

2000/2002 – Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography (OPSC): adopted by the General Assembly in 2000 and in force from 2002, this was the first binding international instrument specifically requiring states to criminalise child sexual exploitation material and related offences, laying the legal foundation later extended online.

2012–2016 – Formation of WeProtect Global Alliance: two separate initiatives – the Global Alliance Against Child Sexual Abuse Online (2012) and WePROTECT (2014) – merged in 2016 into a single multi-stakeholder coalition coordinating the global response to online child sexual exploitation.

2021 – General Comment No. 25: the Committee on the Rights of the Child's landmark clarification that the Convention applies fully online, following consultation with over 700 children worldwide.

2022–2023 – First binding platform-regulation laws: several jurisdictions introduced statutory duties requiring major platforms to assess and mitigate risks to children, with significant financial penalties for non-compliance.

2024 – Expanded mandatory reporting duties: legislative changes in multiple countries broadened platforms' reporting obligations to include child sex trafficking and online enticement, not just CSAM, substantially increasing the volume of reports reaching hotlines.

2024–2026 – The minimum-age legislation wave: a growing number of states across several regions began adopting or proposing minimum-age requirements for social media accounts, with widely varying implementation timelines and enforcement models.



CURRENT SITUATION

Major reporting hotlines now receive over 20 million reports of suspected child exploitation annually, and reports linked to generative AI – including deepfake imagery and AI-assisted grooming – have grown from a few thousand to well over a million in just two years. Cyberbullying and peer-to-peer harassment remain widespread and are consistently linked, alongside online sexual abuse, to the clearest evidence of harm to children's mental health.

States are currently split between two broad regulatory philosophies: restricting who can access platforms through minimum-age laws, or regulating how platforms are designed and operated for everyone through duty-of-care and safety-by-design rules. Both approaches depend on reliable age verification, which remains technically imperfect and raises its own privacy and surveillance concerns.

Meanwhile, commercial data profiling, algorithmic content amplification, and the tension between end-to-end encryption and detection capability continue to complicate enforcement, and roughly a third of the world's children still lack meaningful internet access at all – meaning the risks and the protections discussed in this guide are distributed very unevenly around the world.

ROOT CAUSES

Technological change: consistently outpaced the legal and regulatory frameworks meant to govern it, leaving gaps that new harms, such as AI-generated exploitation material, can exploit before rules catch up.

Commercial, engagement-driven business models: reward design features – infinite scroll, algorithmic recommendation, streaks and notifications – that maximise time on platform, which can conflict with child-safety objectives.

Enforcement and regulatory capacity: highly uneven between states, so the same global platforms are policed far more consistently in some markets than others.

Lack of universality: there's no single harmonised international legal definition of key offences or a universal cross-border cooperation mechanism, which slows investigation and prosecution of crimes that routinely cross-national borders.

Digital literacy: digital literacy among children, parents, and educators has not kept pace with how quickly children adopt new platforms and technologies.

Privacy-orientation: privacy-preserving technologies: such as end-to-end encryption, while valuable for security and free expression, can also limit platforms' technical ability to detect and report abuse.



STAKEHOLDERS

Children and Minors: vulnerability varies significantly by age, and children are rarely consulted directly in the policies designed to protect them.

Parents and Caregivers: the frontline of supervision at home, but often lack the tools, technical knowledge, or time to monitor children's online activity effectively.

Governments and National Regulators: responsible for legislating and enforcing protections, balancing child safety against competing rights to privacy and free expression, and often constrained by limited technical and financial capacity.

Technology and Social Media Companies: control platform design, content moderation, and reporting practices; face growing legal obligations but also commercial incentives that can run counter to child-safety goals.

Educators and Schools: positioned to deliver digital literacy and early intervention, but frequently lack standardised curricula, training, or resources to do so effectively.

Law Enforcement and International Cooperation Bodies: investigate and prosecute offences that often cross borders, but depend on platform cooperation, cross-jurisdictional legal tools, and resourcing that varies widely by country.

Civil Society and NGOs: operate hotlines, provide victim support, and advocate for stronger protections, often serving as the main source of independent data and accountability.



EFFECTS / IMPACT

Psychological and emotional harm: exposure to sexual abuse, exploitation, or bullying is consistently linked to anxiety, depression, and other mental-health consequences for affected children.

Safety and physical risk: online grooming and enticement can escalate into offline abuse, trafficking, or other physical harm.

Long-term privacy and digital footprint risk: data collected from children can be retained, shared, or exploited commercially long after it was first gathered.

Educational and developmental effects: both excessive exposure to harmful content and overly restrictive access can disrupt learning, socialisation, and skill development.

Economic and institutional costs: compliance obligations affect platform operating costs, while investigation and victim support place a growing burden on law-enforcement and social-service budgets.

Erosion of trust: repeated exposure to abuse or exploitation online can undermine children's and families' trust in digital tools that also offer reliable educational and social value.

CASE STUDIES

United Kingdom: The Age Appropriate Design Code

(Children's Code): Enforced under the Data Protection Act 2018, the UK Information Commissioner's Office (ICO) introduced a landmark statutory code forcing tech platforms to design services with child safety embedded by default. The code mandates strict privacy settings, bans dark patterns that trick children into sharing data, disables location tracking by default, and limits profiling for behavioral advertising. Major tech companies adjusted their global features to comply, such as YouTube making default uploads private for teens and Instagram disabling direct messaging between adults and unrelated minors. The UK model shifted regulatory policy from passive content moderation to proactive "safety by design."

United States: FTC Regulations & COPPA Enforcement

Against Major Tech: The Federal Trade Commission (FTC) enforces the Children's Online Privacy Protection Act (COPPA), targeting tech platforms that illegally harvest data from children under 13 without verifiable parental consent. High-profile enforcement actions—including multi-hundred million dollar fines and mandatory privacy restructuring against major social platforms and gaming companies—highlighted systemic abuses in algorithmic profiling and micro-targeted advertising aimed at youth. These enforcement actions established precedent for corporate liability and forced platforms to segregate child-directed content, disable personalized tracking on minor-centric hubs, and implement strict age-gating mechanisms.

Australia: eSafety Commissioner & Age-Verification Mandate:

Australia created the world's first dedicated independent government regulator for online safety, the eSafety Commissioner, empowered by the Online Safety Act 2021. The agency holds broad powers to compel platforms to remove severe cyberbullying, non-consensual intimate images, and explicit content within strict timeframes, leveraging heavy civil penalties for non-compliance. Australia has also led trials into mandatory age-verification technologies (such as facial estimation and digital ID verification) to restrict minors' access to explicit content and social media platforms.

United States: FTC Regulations & COPPA Enforcement

Against Major Tech: The Federal Trade Commission (FTC) enforces the Children's Online Privacy Protection Act (COPPA), targeting tech platforms that illegally harvest data from children under 13 without verifiable parental consent. High-profile enforcement actions—including multi-hundred million dollar fines and mandatory privacy restructuring against major social platforms and gaming companies—highlighted systemic abuses in algorithmic profiling and micro-targeted advertising aimed at youth. These enforcement actions established precedent for corporate liability and forced platforms to segregate child-directed content, disable personalized tracking on minor-centric hubs, and implement strict age-gating mechanisms.

Australia: eSafety Commissioner & Age-Verification Mandate:

Australia created the world's first dedicated independent government regulator for online safety, the eSafety Commissioner, empowered by the Online Safety Act 2021. The agency holds broad powers to compel platforms to remove severe cyberbullying, non-consensual intimate images, and explicit content within strict timeframes, leveraging heavy civil penalties for non-compliance. Australia has also led trials into mandatory age-verification technologies (such as facial estimation and digital ID verification) to restrict minors' access to explicit content and social media platforms.

European Union: The Digital Services Act (DSA) & Systemic Risk Audits: Under the EU's Digital Services Act, Very Large Online Platforms (VLOPs) are legally required to assess and mitigate systemic risks to minors, including mental health impacts, addiction loops, and exposure to harmful content. The DSA strictly prohibits targeted advertising to minors based on profiling or sensitive personal data. Regulators enforce these obligations through mandatory independent audits and fines reaching up to 6% of a firm's global annual turnover. EU enforcement shifts focus toward algorithmic accountability, compelling platforms to overhaul recommendation engines that push dangerous content rabbit holes to young users.

South Korea: Anti-Addiction Measures & Real-Name Verification Systems: The government introduced the "Shutdown Law" (Youth Protection Act amendment), which restricted minors under 16 from accessing online gaming platforms during overnight hours. While the law was later phased out in favor of a flexible "Choice System" allowing parents to set limits, South Korea maintains strict real-name identification verification (using mobile phone numbers or resident registration numbers) across online platforms. This framework minimizes underage access to restricted services and combats anonymous online harassment.

KEY INTERNATIONAL BODIES

UN Committee on the Rights of the Child: the treaty body that monitors state compliance with the Convention and its Optional Protocols, and issued General Comment No. 25 on the digital environment.

International Telecommunication Union (ITU): publishes the Guidelines on Child Online Protection and coordinates a multi-stakeholder network of governments, industry, and civil society on child online safety standards.

WeProtect Global Alliance: a multi-stakeholder coalition coordinating national and international responses to online child sexual exploitation through its Model National Response framework.

INTERPOL: supports cross-border law-enforcement cooperation on crimes against children, including through its International Child Sexual Exploitation database, which helps investigators identify victims and offenders across jurisdictions.

UNESCO: promotes digital literacy and media education, and coordinates the International Day against Violence and Bullying at School, Including Cyberbullying.

PAST SOLUTIONS AND FRAMEWORKS

Convention on the Rights of the Child (1989) and its Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography (2000/2002) – the core binding legal foundation for child protection, later extended to digital contexts.

General Comment No. 25 (2021) – authoritative guidance confirming that all rights in the Convention apply fully in the digital environment, and directing states on implementation.

ITU Guidelines on Child Online Protection – a periodically updated, multi-stakeholder framework offering practical recommendations for governments, industry, and educators.

WeProtect Global Alliance Model National Response – a voluntary framework supporting states in building coordinated policy, criminal-justice, and victim-support responses to online exploitation.

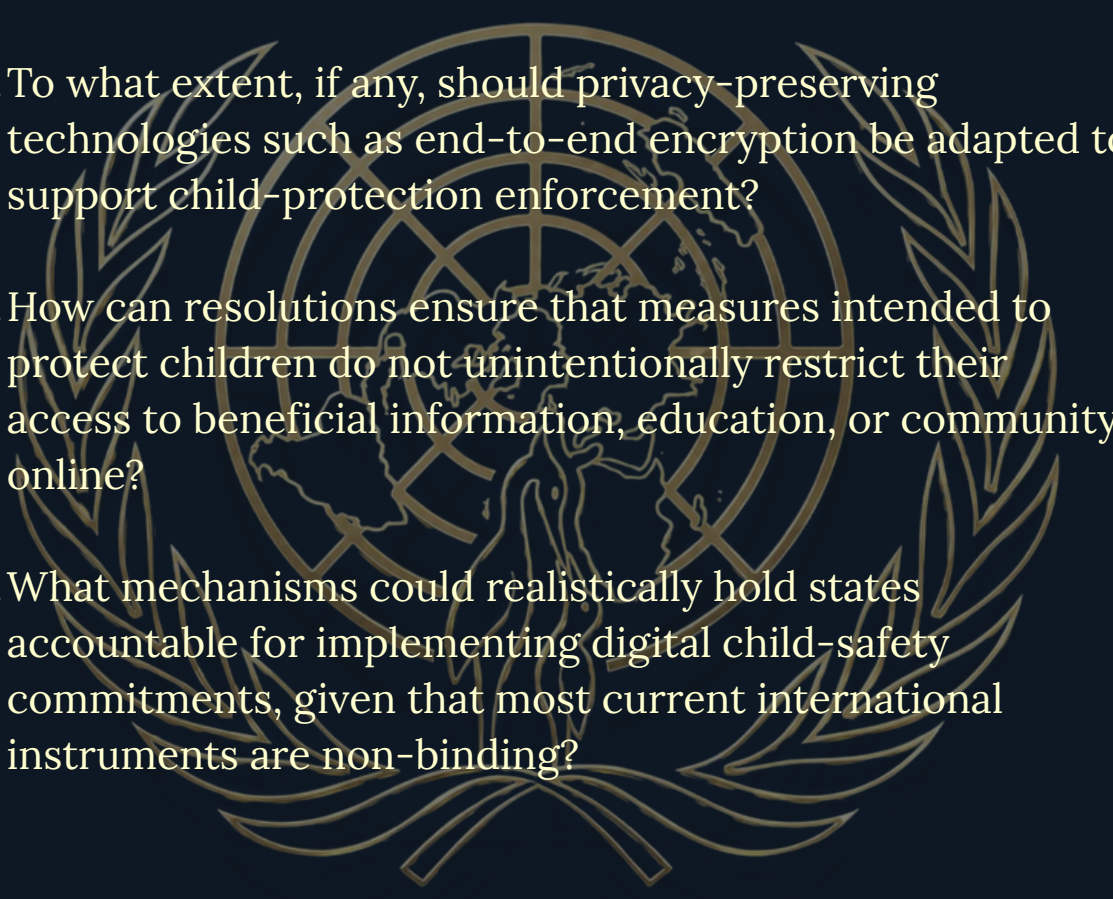
National regulatory experiments – including duty-of-care platform legislation, mandatory-reporting laws, and minimum-age requirements – which, while not internationally coordinated, offer a growing evidence base on what different regulatory models achieve in practice.

UNICEF-industry partnerships and safety-by-design toolkits
– voluntary technical guidance encouraging platforms to build child-safety considerations into products from the design stage.



QUESTIONS A RESOLUTION MUST ANSWER

- 
1. How should the international community balance children's right to protection online with their rights to privacy, freedom of expression, and access to information?
 2. What responsibilities should technology companies bear for harms occurring on their platforms, and how should accountability be balanced against innovation and the practical limits of enforcement?
 3. Should international policy favour age-restriction models, platform design and duty-of-care models, or some combination?
 4. How can the international community narrow the gap in enforcement capacity between well-resourced and under-resourced states without compromising national sovereignty?
 5. What role should children, parents, and educators play in shaping digital-safety policy, and how can their perspectives be meaningfully incorporated into international frameworks?

- 
6. How should international frameworks address harms created by emerging and future technologies, such as generative AI, given that today's solutions may not anticipate tomorrow's risks?
 7. To what extent, if any, should privacy-preserving technologies such as end-to-end encryption be adapted to support child-protection enforcement?
 8. How can resolutions ensure that measures intended to protect children do not unintentionally restrict their access to beneficial information, education, or community online?
 9. What mechanisms could realistically hold states accountable for implementing digital child-safety commitments, given that most current international instruments are non-binding?

BIBLIOGRAPHY

United Nations – Child and Youth Safety Online

UNICEF – Child Online Protection

UNICEF Innocenti – Childhood in a Digital World (2025)

UNICEF – Keeping Children Safe Online: Platform Regulation Policy Brief

UNICEF – Strengthening the Convention on the Rights of the Child: Optional Protocols

OHCHR – General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment

OHCHR – Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography

National Center for Missing & Exploited Children – 2024 CyberTipline Data

National Center for Missing & Exploited Children – 2025 CyberTipline Data

Thorn – Analysis of the 2024 NCMEC CyberTipline Report

WeProtect Global Alliance – History and Timeline

WeProtect Global Alliance – About the Alliance and Model National Response

Online Age Verification Laws by Country – Comparative Overview

eSafety Commissioner – Social Media Age Restrictions: Regulatory Guidance