

Global Online Safety Benchmark

2025

Prepared by



Foreword

The digital world offers children and young people unprecedented opportunities to learn, connect, and thrive. Yet, it also exposes them to new and evolving risks that demand urgent, coordinated, and evidence-based responses.

As the Internet Society Online Safety Special Interest Group (SIG), we recognize that protecting children online is not only a moral imperative but also a shared responsibility that transcends borders and cultures.

The Global Online Safety Benchmark was created to address the pressing need for localized, data-driven insights into child online protection systems. By focusing on **Indonesia, the Philippines, Ghana, Rwanda, and the Dominican Republic**, this report highlights both the diversity of online risks and the universal commitment to safeguarding children in the digital age.

Our goal is to provide actionable analysis that empowers policymakers, practitioners, and communities to build safer, more resilient digital environments for the next generation.

This benchmark is the result of collaboration between dedicated researchers, expert organizations, and passionate advocates. It reflects the values of the Online Safety SIG: inclusivity, evidence-based action, and a relentless pursuit of progress in online safety.

We invite you to explore the findings, reflect on the recommendations, and join us in advancing a safer, more inclusive internet for children everywhere. Together, we can ensure that the digital world remains a place of opportunity, growth, and protection for all.

Sincerely,

Godsway Kubi

Lead Facilitator

Internet Society Online Safety SIG



Acknowledgements

The Global Online Safety Benchmark is a pioneering initiative conceived and led by the Internet Society Online Safety Special Interest Group (SIG). This benchmark reflects the collective vision, expertise, and commitment of the Online Safety SIG to advance safer digital environments worldwide, particularly for children and vulnerable users.

About the Internet Society Online Safety SIG

The Internet Society Online Safety SIG is a dedicated community within the Internet Society focused on promoting best practices, policies, and frameworks that enhance online safety globally. The SIG serves as a collaborative platform for experts, advocates, and stakeholders to share knowledge, develop tools, and influence positive change in the digital ecosystem. Our work emphasizes a multi-stakeholder approach, recognizing that effective online safety requires coordinated efforts across governments, civil society, industry, and technical communities.

For more information about our work, please visit: <https://www.internetsociety.org/sigs/online-safety/>

Leadership Team

This benchmark was initiated and guided by the leadership of the Online Safety SIG, whose commitment and expertise have been instrumental throughout the project.

Lead Facilitator: Godsway Kubi

Vice Facilitator: Lavish Mawuena Mensah

Secretary: Charles Owiti

Board Members:

- Raymond Mamattah
- Muhammad Umair Ali
- Joy Uchechi Eziashi

Project Vision

The idea for the Global Online Safety Benchmark originated from the Online Safety SIG's recognition of the urgent need for localized, evidence-based analysis of child online protection systems. This report focuses on five countries: Indonesia, the Philippines, Ghana, Rwanda, and the Dominican Republic, each facing unique challenges but united by the shared goal of safeguarding children in the digital world. The benchmark aims to illuminate both progress and gaps, providing actionable insights for policymakers, practitioners, and advocates.

Collaborators and Contributors

This project would not have been possible without the invaluable contributions of our partners and expert collaborators. We extend our deepest gratitude to:

- Bullyid App – NMA Foundation

For their thorough research, coordination, and analysis, which formed the foundation of this benchmark. For more information on the work of Bullyid App and NMA Foundation, please visit bullyid.org

- Expert Contributors and Organizations:

- Andy Ardian, National Coordinator, ECPAT Indonesia
- Hiqmat Sungdeme Saani, Founder & Executive Director, Paahibu Space, Ghana
- Roland Angerer, Country Director of Plan International for the Dominican Republic
- Department of Education, Philippines
- National Child Development Agency, Rwanda
- UNICEF Rwanda

Their insights, data, and recommendations have enriched this report, ensuring that it reflects national priorities and context-specific strategies to enhance online child safety.

Protecting children in the digital age requires proactive collaboration, clarity, and courage from all sectors. Through this benchmark, we aspire to inspire meaningful, evidence-based action that is grounded in the voices and experiences of those on the frontlines of child online protection.

Thank you to everyone who contributed to this important initiative. Together, we can build a safer digital future for children everywhere.

Contact

For inquiries or further information about the Global Online Safety Benchmark or the Online Safety SIG, please contact us at: online-safety@isoccommunity.org





Executive Summary

The Global Online Safety Benchmark 2025 offers a critical assessment of the worldwide online safety environment, with a distinct focus on the vulnerabilities and protections for children and adolescents. It benchmarks prevailing online safety measures on prominent digital platforms—**YouTube, TikTok, Instagram, and Snapchat**—and examines the legislative and support infrastructures in five selected countries: **Indonesia, the Philippines, Ghana, Rwanda, and the Dominican Republic**.

As digital technologies become increasingly central to the lives of children and adolescents, the report underscores a corresponding escalation in their exposure to diverse online risks. Among the primary concerns are the pervasive threats of cyberbullying, encounters with inappropriate and harmful content including sexual abuse material and violence, violations of privacy, the dangers of online grooming, and significant mental health challenges that can be exacerbated by online interactions.

An examination of the major social media platforms reveals inconsistent levels of commitment and effectiveness in the implementation of their safety policies and features. Although these platforms have introduced various tools for content moderation, reporting mechanisms, and parental controls, significant shortcomings persist. These include the inconsistent enforcement of community guidelines, the potential for algorithmic amplification of harmful content, inadequate age verification processes, and a general lack of transparency concerning data usage and the specifics of content moderation practices.

Across the surveyed nations, there is a growing acknowledgment of the necessity for robust online safety laws, particularly for child protection. However, the journey from recognizing this need to effectively developing, implementing, and enforcing such laws is marked by considerable variation and challenges. These challenges range from keeping legal frameworks current with rapidly advancing technologies and addressing all forms of online harm, to securing adequate resources for enforcement agencies and fostering cross-border cooperation. Concurrently, victim support services for those affected by online harms are frequently found to be fragmented, under-resourced, and not easily accessible. This situation is compounded by often weak or ill-defined mechanisms for holding digital platforms accountable for harms occurring on their sites and for their responsiveness to user safety.

The benchmark concludes that despite rising awareness of online safety issues, current global efforts fall short of adequately protecting children and adolescents in the digital realm. The findings highlight the intricate relationship between technology, user behaviour, platform governance, and national regulatory capacities.

Moving forward, a comprehensive, multi-stakeholder approach is strongly advocated to foster a safer digital environment. Governments are urged to develop, enact, and rigorously enforce national online safety laws and policies, with a specific emphasis on child online protection and clear mandates for regulatory bodies. Investment in capacity building for law enforcement, the judiciary, and social services is crucial, alongside the promotion of digital literacy and online safety education for children, parents, and educators, and the fostering of international cooperation.



Table of Contents

01	Executive Summary	11	Digital Landscape for Children & Adolescents
02	Table of Contents	19 - 34	Platform Analysis: YouTube - TikTok - Instagram - Snapchat
03	Introduction	48 - 79	Legislation & Policy Framework: Indonesia - Philippines - Ghana - Rwanda - Dominican Rep.
07	Acronyms and abbreviations	88 - 102	Victim Support & Platform Accountability: Indonesia - Philippines - Ghana - Rwanda - Dominican Rep.
08	Glossary/ definitions	105	Insights and Recommendations
		111	References



Introduction

The pervasive integration of digital technologies into daily life has fundamentally reshaped childhood and adolescence. Social media and video-sharing platforms, in particular, stand as central arenas for learning, social interaction, creative expression, and entertainment for young people globally.

These digital environments offer unprecedented opportunities, fostering connections, broadening horizons, and igniting creativity. However, this immersion is accompanied by significant and evolving risks.

From social media platforms to live-streaming sites and messaging apps, children are more digitally connected than ever before. Yet this connectivity has a double edge. These platforms often become gateways for harmful behaviors, including cyberbullying, online grooming, child sexual exploitation and abuse (OCSEA), sextortion, the circulation of child sexual abuse material (CSAM), and exposure to age-inappropriate or harmful content.

The COVID-19 pandemic further intensified these risks—escalating screen time, reducing supervision, and accelerating children’s digital immersion in unregulated spaces.

This surge in unsupervised digital activity highlighted critical shortcomings in child online safety frameworks, particularly in low- and middle-income countries where regulatory structures, reporting mechanisms, and parental awareness tools remain underdeveloped.

Global statistics reflect a deeply worrying trend: CSAM is increasing at unprecedented rates, with victims becoming younger and more vulnerable. At the same time, cyberbullying and online harassment continue to affect the mental health, academic participation, and personal development of millions of children.

This **Global Online Safety Benchmark** responds to the urgent need for localized, evidence-based analysis of child online protection systems. The report focuses on five countries—**Indonesia, the Philippines, Ghana, Rwanda, and the Dominican Republic**—each facing diverse risks but united by a common goal: safeguarding children in the digital world.

Through this research, we examine each country’s legal definitions, policy responses, and digital governance tools aimed at protecting children online. We assess the strength and implementation of laws addressing key threats such as AI-generated child abuse content, live-streaming exploitation, grooming, and non-consensual image sharing. We also look at how platforms like YouTube, TikTok, Instagram, and Snapchat enforce community standards, remove harmful content, and report online sexual abuse.

This report is the product of extensive stakeholder engagement, drawing on insights from government agencies, law enforcement, tech platforms, civil society, and survivor support networks. It not only highlights protection gaps but also showcases innovative strategies, scalable models, and best practices for creating safer online environments.

Aims



Evaluate the effectiveness of national responses to online child sexual exploitation and abuse (OCSEA) in five selected developing countries: Indonesia, the Philippines, Ghana, Rwanda, and the Dominican Republic.



Establish a practical benchmarking framework that enables governments, policymakers, civil society, and tech platforms to assess and compare their current child online safety efforts.



Identify gaps in legislation and policy frameworks relating to child online protection and propose actionable legal reforms.



Assess the accessibility, quality, and coordination of victim support services, including helplines, psychosocial support, case referral systems, and trauma-informed care for child victims of online abuse.



Analyze the policies, community guidelines, and enforcement mechanisms of leading social media platforms (e.g., YouTube, TikTok, Instagram, Snapchat) in relation to child protection, takedown procedures, and reporting tools.



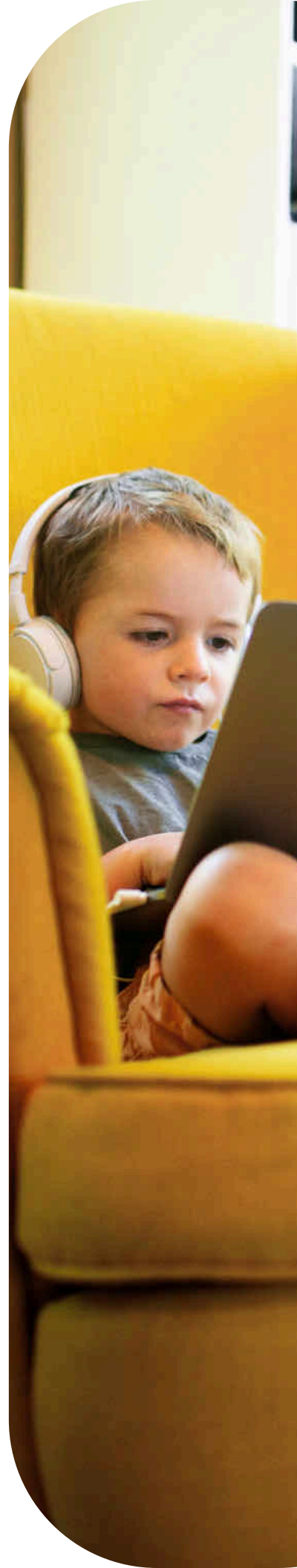
Methodology

This research analysis employed a comparative analysis of secondary data to investigate child online safety issues in **Indonesia, the Philippines, Ghana, Rwanda, and the Dominican Republic.**

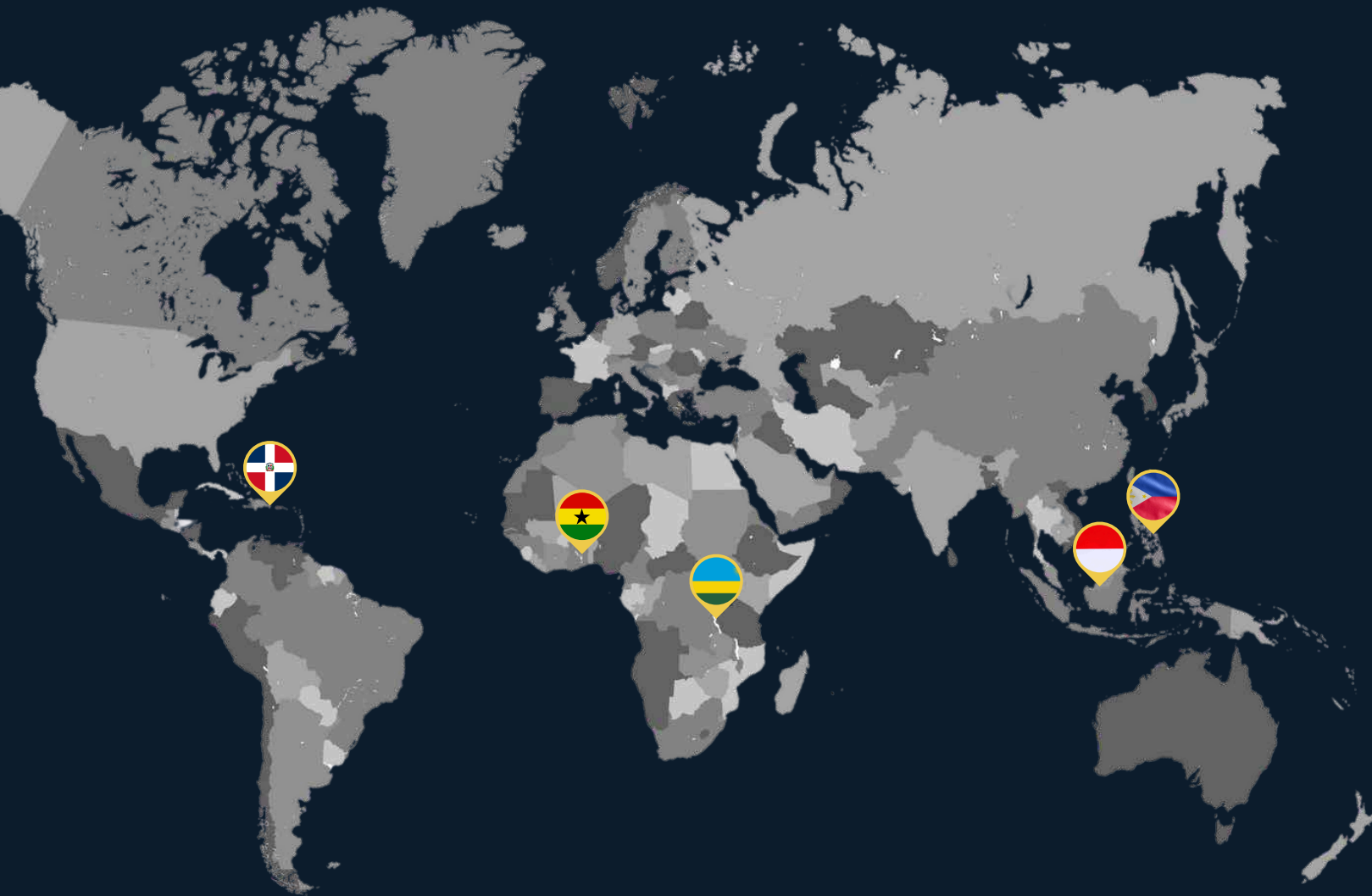
The methodology involved a comprehensive literature review encompassing:

- **Academic Papers and Research Studies:** Peer-reviewed articles and studies examining online risks, child development, digital behavior, and intervention effectiveness.
- **Reports from International Bodies:** Publications and data from organizations such as UNICEF, the International Telecommunication Union (ITU), the WeProtect Global Alliance, the World Health Organization (WHO), and the UN Office on Drugs and Crime (UNODC).
- **Reports from Reputable NGOs and Foundations:** Data and analyses from organizations focused on child protection, digital rights, and online safety, including ECPAT, INTERPOL (within specific projects), ChildFund Alliance, 5Rights Foundation, International Justice Mission (IJM), Internet Watch Foundation (IWF), National Center for Missing and Exploited Children (NCMEC), and others.
- **Government Publications and Legal Documents:** Official government reports, national statistics, policy documents, and legislation related to child protection, cybersecurity, and digital regulation from the focus countries
- **Industry Reports and News Articles:** Data and insights from digital analytics firms (e.g., Datareportal) and reputable news sources covering technology, policy, and social issues.

Data extracted from these sources were synthesized to understand the global context, analyze the specific situation in each target country (digital usage, risks, policies, initiatives), and conduct a comparative analysis. The focus was on identifying patterns, convergences, divergences, and specific challenges and successes within and across the five nations. Suggestions were formulated based on the synthesized evidence.



Limitations



While this report offers a broad analysis of child online safety across five countries, it is subject to several limitations due to reliance on secondary data.

Data availability and quality vary widely. Some countries have stronger systems than others, and sensitive issues like online child sexual exploitation and cyberbullying are often underreported due to stigma or lack of awareness, making comparisons difficult. The digital environment is rapidly evolving. Platform features and threats—such as AI-generated CSAM—change quickly, and policies may have shifted since data was collected.

Cultural factors also impact reporting behaviors and perceptions of risk, which may not be fully captured in generalized studies. Moreover, some reports may carry institutional or reporting biases, and many incidents go unreported. Most research focuses heavily on OCSEA and cyberbullying, potentially overlooking other harms like online hate speech or algorithmic risks. Additionally, findings from small or localized samples (e.g., school surveys) may not reflect national realities. These limitations were carefully considered during the interpretation of findings.



Dominican Republic



Indonesia



Ghana



The Philippines



Rwanda

Acronyms and abbreviations

AI

Artificial
Intelligence

API

Application
Programming
Interface

CSA

Child Sexual Abuse

CSAM

Child Sexual Abuse
Material

COP

Child Online
Protection

CSEA

Child Sexual
Exploitation and
Abuse

CSAI

Child Sexual
Abuse Imagery

GBV

Gender-Based
Violence

ISP

Internet Service
Provider

MLAT

Mutual Legal
Assistance Treaty

NGO

Non-Government
Organization

OCSEA

Online Child Sexual
Exploitation and Abuse

TFGBV

Technology-
Facilitated Gender
Based Violence

VPN

Virtual Private
Network



Glossary/ definitions



Child Sexual Abuse

The involvement of a child (anyone under 18) in sexual activity that they do not fully comprehend, are unable to give informed consent to, or for which the child is not developmentally prepared and cannot give consent.¹

Child Sexual Exploitation

A form of child sexual abuse that involves any actual or attempted abuse of a position of vulnerability, differential power, or trust. This includes, but is not limited to, profiting monetarily, socially, or politically from the sexual exploitation of another.² Individuals or groups of offenders can perpetrate this. The underlying notion of exchange present in exploitation distinguishes child sexual exploitation from child sexual abuse.³ There is significant overlap between the two concepts because exploitation is often a feature of abuse and vice versa.⁴ This report primarily uses the phrase 'child sexual exploitation and abuse' in recognition of the overlap and to be most inclusive across different jurisdictions with different definitions.

Child Sexual Exploitation and Abuse Online

Child sexual exploitation and abuse that is partly or entirely facilitated by technology, i.e. the internet or other wireless communications. This report uses online child sexual exploitation and abuse and technology-facilitated child sexual exploitation and abuse interchangeably with child sexual exploitation and abuse online.

Livestreaming Child Sexual Exploitation and Abuse

Transmitting child sexual abuse and exploitation in real-time over the internet.

1. World Health Organization, 'Guidelines for Medico-Legal Care for Victims of Sexual Violence: Child Sexual Abuse', 2003, <<https://apps.who.int/iris/handle/10665/42788>>, accessed 8 February 2025.

2. United Nations, Glossary on Sexual Exploitation and Abuse, 24 July 2017, <https://hr.un.org/sites/hr.un.org/files/SEA%20Glossary%20%20%5BSecond%20Edition%20-%202017%5D%20-%20English_0.pdf>, accessed 8 February 2025.

3. Interagency Working Group on Sexual Exploitation of Children, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, 2016, <www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf>, accessed 21 February 2025.

4. Ibid.

Child Sexual Abuse Material (CSAM)

Any visual or audio content of a sexual nature involving a person under 18 years old,⁵ whether real or not real.

Note on alternative terminology: Some organizations distinguish between ‘child sexual abuse material’ and ‘child sexual exploitation material’ (e.g., the Interagency Working Group on the Sexual Exploitation of Children define ‘child sexual exploitation material’ as a broader category that encompasses both ‘material depicting child sexual abuse and other sexualised content depicting children’). This report largely uses the phrase ‘child sexual abuse material’.

The phrase ‘child pornography’ is also used in some international, regional, and domestic legislation. The Committee on the Rights of the Child has recognised that this term is gradually being replaced for various reasons, including that it can undermine the gravity of the crimes.⁶ ‘Child sexual abuse material’ is considered to capture the heinous nature of sexual violence against children more accurately and protect the dignity of victims and survivors.

Some ‘self-generated’ sexual material would also constitute child sexual abuse material depending on the circumstances of its production.

Child Sexual Exploitation

Content of a sexual nature, including nude or partially nude images and video, produced by children of themselves. There are scenarios in which harm is caused, primarily:

- When a child or adolescent is coerced into producing ‘self-generated’ sexual material
- When voluntarily ‘self-generated’ sexual material is shared against an adolescent’s wishes.

Grooming children online for the purpose of sexual exploitation and abuse

An individual builds a relationship, trust, and emotional connection with a child or young person to manipulate, exploit and abuse them (facilitated, partly or entirely, by the internet or other wireless communications). There is not always an intent to meet in person.

Tradecraft

An ever-evolving host of ‘cloaking’ techniques and evasion strategies offenders use to avoid individual detection, and their methods and strategies for identifying and engaging children.

5. National Center for Missing & Exploited Children, ‘Child Sexual Abuse Material (CSAM)’, <www.missingkids.org/theissues/csam>, accessed 8 February 2025.

6. Committee on the Rights of the Child, Guidelines regarding the Implementation of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, CRC/C/156, 10 September 2019, <www.ohchr.org/Documents/HRBodies/CRC/CRC.C.156_OPSC%20Guidelines.pdf>, accessed 8 February 2025.

Glossary/ definitions

Online Child Sexual Exploitation and Abuse (OCSEA)

Refers to situations involving digital, internet and communication technologies at some point during the continuum of abuse or exploitation. OCSEA can occur fully online or through a mix of online and in-person interactions between offenders and children.

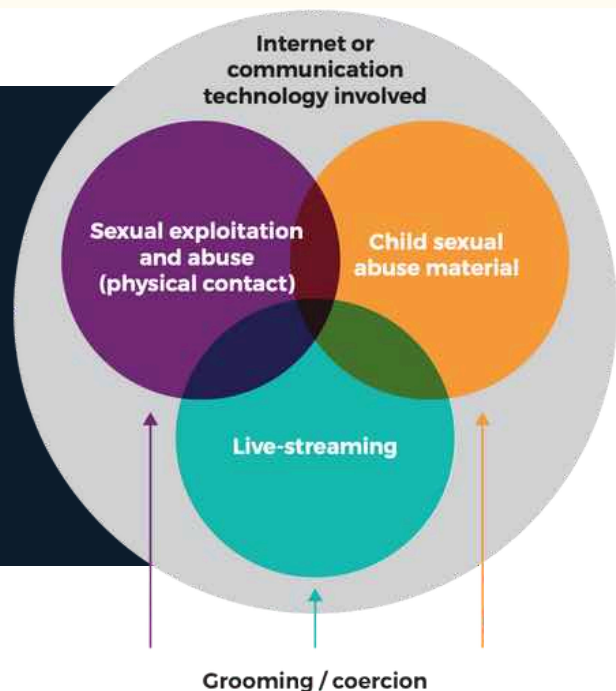
Sexual Extortion of Children

Refers to the use of blackmail or threats to extract sexual content or other benefits (e.g., money) from the child, often using sexual content of the child that has previously been obtained as leverage.

Unwanted Exposure of a Child to Sexual Content

Refers to other phenomena which can constitute or enable OCSEA in some instances. For example, offenders can deliberately expose children to sexual content as part of grooming to desensitise them to sexual acts.

Framing the
main forms of
online child
sexual
exploitation
and abuse.



Source: Disrupting Harm 2022

A close-up photograph of two young children with dark, curly hair looking intently at a laptop screen. The child on the right is resting their chin on their hand, and the child on the left is also looking closely at the screen. The background is dark and out of focus.

Digital Landscape for Children & Adolescents

Global Internet & Social Media Usage Trends

Children and adolescents represent a substantial and growing segment of the global online population. Estimates suggest that individuals under 18 constitute approximately one-third of all internet users worldwide.⁷ The influx of young users is rapid, with projections indicating that a new child goes online for the first time every half second globally.⁸ Data consistently shows that young people, particularly those aged 15-24, utilize the internet at higher rates than the general population, although this generational gap shows signs of narrowing.⁹ In 2023, approximately 77% of individuals aged 15-24 used the internet.¹⁰

Despite increasing global connectivity, significant disparities, often termed the "digital divide," persist. A 2020 joint report by UNICEF and the International Telecommunication Union (ITU) revealed that two-thirds of the world's school-age children, amounting to 1.3 billion individuals aged 3 to 17, lacked internet access at home.¹¹ This lack of connectivity disproportionately affects children from lower-income households and those residing in rural areas. Globally, only 16% of school-age children from the poorest households had home internet access, compared to 58% from the richest households.¹²

Similarly, less than 1 in 20 children in low-income countries had home internet, versus nearly 9 in 10 in high-income countries. Geographic disparities are stark, with approximately 75% of rural school-age children lacking home access compared to 60% in urban areas. Sub-Saharan Africa and South Asia exhibit the highest rates of unconnected children, with around 9 out of 10 lacking home internet access.¹³

Even where access is available, the mode of connection significantly influences the online experience and potential risks. In many developing nations, internet access, particularly for children, occurs primarily through mobile devices.¹⁴ While mobile technology expands reach, this mobile-first environment presents unique challenges. Access often occurs on shared devices and without adequate adult supervision or guidance. This is frequently coupled with lower levels of digital literacy among both children and their caregivers.¹⁵

Limited digital skills hinder the ability to navigate online environments safely, recognize risks, utilize privacy settings effectively, and report harmful content. The reliance on mobile interfaces, potentially differing from desktop experiences, might also affect exposure types and the ease of using safety features or reporting mechanisms. This confluence of factors—unsupervised mobile access and limited digital literacy—suggests that the way children connect, not just whether they connect, is a critical determinant of their vulnerability in many regions. Affordability of data and devices, alongside low digital skills, remain significant barriers to equitable and safe participation in the digital world.

7. Rapid Review of Online Safety Risks: Full Report - ChildFund Alliance, <<https://childfundalliance.org/wp-content/uploads/2022/03/Rapid-Review-of-Online-Safety-Risks-Full-Report-5.pdf>>, accessed 10 March 2025.

8. Protecting children online - UNICEF.org, <<https://www.unicef.org/protection/violence-against-children-online>>, accessed 10 March 2025.

9. Global Threat Assessment 2023 Data - WeProtect Global Alliance, <<https://www.weprotect.org/global-threat-assessment-23/data/>>, accessed 10 March 2025.

10. Child and Youth Safety Online - the United Nations, <<https://www.un.org/en/global-issues/child-and-youth-safety-online>>, accessed 10 March 2025.

11. Two thirds of the world's school-age children have no internet access at home, new UNICEF-ITU report says, <<https://www.unicef.org.uk/press-releases/two-thirds-of-the-worlds-school-age-children-have-no-internet-access-at-home-new-unicef-itu-report-says/>>, accessed 10 March 2025.

12. Ibid.

13. Ibid.

14. Rapid Review of Online Safety Risks: Executive Summary - ChildFund Alliance, <<https://childfundalliance.org/wp-content/uploads/2022/03/Rapid-Review-of-Online-Safety-Risks-Executive-Summary-5.pdf>>, accessed 10 March 2025.

15. ONLINE KNOWLEDGE AND PRACTICE OF PARENTS ... - Unicef, <<https://www.unicef.org/indonesia/media/23586/file/online-knowledge-practice-parents-and-children-indonesia-baseline-study-2023.pdf>>, accessed 10 March 2025

Common Online Activities

Children and adolescents engage in a diverse range of activities online, driven primarily by social, entertainment, and informational needs. Key activities include:

Socializing and Communication

Connecting with friends through instant messaging, social media platforms, and video/voice calls is a primary motivator for online engagement.¹⁶ Many teens report that using these platforms helps them feel closer to their friends.¹⁷

Entertainment

Consuming entertainment content, such as watching videos (especially on YouTube), streaming movies, and playing online games, is highly popular. Online gaming is a major activity, often serving as a social space for communication with friends, although it also involves interaction with strangers.¹⁸

Information Seeking and Learning

The internet is a vital resource for schoolwork, learning new things, and exploring hobbies and interests. Platforms like YouTube are frequently used for finding information on how to build or create things.¹⁹

Content Creation

A growing number of older children and adolescents actively participate by creating and sharing their own content, such as uploading videos, particularly on platforms like TikTok.²⁰

16. Children and Parents: Media Use and Attitudes Report - Ofcom, < <https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/children-media-use-and-attitudes-2024/childrens-media-literacy-report-2024.pdf?v=368229> >, accessed 11 March 2025.

17. Ibid.

18. Ibid.

19. What are your kids watching on YouTube? - Scott Guthrie, < <https://sabguthrie.info/kids-watching-youtube/> >, accessed 11 March 2025.

20. Ofcom (N 16)

Social Media Platform Trends



Globally, **YouTube consistently ranks as the most widely used platform among teenagers.**²¹ Following YouTube, TikTok, Instagram, and Snapchat command significant attention, with substantial proportions of teens using them daily. Usage often begins at young ages; platforms like TikTok and Instagram have seen notable increases in adoption among children as young as 5 to 7 years old.²² Conversely, Facebook's popularity among teenagers has markedly decreased over the last decade.²³ Adolescents dedicate considerable time to these platforms, with daily usage averaging between 3.5 and 5.4 hours according to various studies.²⁴ A significant portion, nearly half of U.S. teens, report being online "almost constantly," indicating deep integration into their daily lives.²⁵

Usage Patterns

YouTube's reach is extensive, dominating usage across various age groups, from young children (3-4 year olds) to teenagers.²⁶ Its daily engagement is high, with a notable percentage of teens reporting "almost constant" use. For many children aged 8-15, YouTube is preferred over traditional television programming, as the platform serves multiple functions, including entertainment, learning (both formal and informal), exploring hobbies, and seeking information.²⁷

Popular Content

Content consumed by children and teens on YouTube is diverse, including vlogs (video blogs), content related to video games (tutorials, walkthroughs), music videos, educational materials covering a wide range of topics, and videos depicting challenges or stunts.²⁸

Specific Risks

YouTube presents a high risk for cyberbullying; one study identified it as the platform where children were most likely to experience cyberbullying (79% likelihood).²⁹ Roughly six-in-ten parents say they are at least somewhat concerned about their child in this age range ever being the target of online predators (63%), accessing sexually explicit content (60%) and accessing violent content online (59%).³⁰ The platform's policies acknowledge the risk of minors imitating harmful or dangerous acts depicted in videos, such as dangerous challenges or substance use. Parents express concern about the types of videos recommended to their children by YouTube's algorithms. While less emphasized compared to platforms with stronger direct messaging features, the potential for predatory behavior exists within comment sections and community interactions.³¹

21. 2. Parental views about YouTube - Pew Research Center, <<https://www.pewresearch.org/internet/2020/07/28/parenting-approaches-and-concerns-related-to-digital-devices/>>, accessed 11 March 2025.

22. Children and Parents: Media Use and Attitudes Report - Ofcom, <<https://www.ofcom.org.uk/consult/condocs/media-literacy-research/children/children-media-use-and-attitudes-2024/children-media-literacy-report-2024.pdf?v=368229>>, accessed 11 March 2025.

23. Teens and social media: Key findings from Pew Research Center surveys, <<https://www.pewresearch.org/short-reads/2024/04/24/teens-and-social-media-key-findings-from-pew-research-center-surveys/>>, accessed 11 March 2025.

24. Ibid.

25. Teens, Social Media and Technology 2025 | Pew Research Center, <<https://www.pewresearch.org/internet/2024/12/11/teens-social-media-and-technology-2025>>, accessed 11 March 2025.

26. Ofcom (N 22)

27. Ofcom (N 21)

28. 4 reasons teens take part in social media challenges | Clemson News, <<https://news.clemson.edu/4-reasons-teens-take-part-in-social-media-challenges/>>, accessed 11 March 2025.

29. Cyberbullying: Twenty Crucial Statistics for 2025 | Security.org, <<https://www.security.org/resources/cyberbullying-20-statistics/>>, accessed 11 March 2025.

30. Ofcom (N 21)

31. Ibid.

Social Media Platform Trends



Usage Patterns

TikTok has experienced explosive growth, becoming exceptionally popular among teenagers (around 63-67% usage reported in recent surveys).³² Its reach extends to younger demographics as well, with significant usage reported among 5-7 year olds (30% in UK) and even children under 10 (50% in UK).³³ Daily usage is high, with 58% of teens using it daily and 16-17% reporting "almost constant" use. Usage patterns show demographic variations, with higher adoption among girls and Black and Hispanic teens in the U.S.³⁴

Popular Content

The platform is defined by its short-form video format. Popular content includes user-generated videos featuring dance trends, participation in viral challenges, comedy sketches, lip-syncing to audio clips, and short educational or informational segments.³⁵

Specific Risks

TikTok is associated with a high risk of cyberbullying (64% likelihood for children reported in one study).³⁶ The platform's trend-driven nature makes it a conduit for potentially harmful or dangerous challenges. Exposure to inappropriate content, including sexual or violent themes, is a concern. Data privacy practices have also drawn scrutiny.³⁷ The platform's features can be exploited for online grooming.³⁸ The highly engaging, algorithmically driven feed contributes to concerns about excessive screen time, potential addiction, and negative impacts on mental health, particularly body image.³⁹

32. Teens and social media: Key findings from Pew Research Center surveys, <<https://www.pewresearch.org/short-reads/2023/04/24/teens-and-social-media-key-findings-from-pew-research-center-surveys/>>, accessed 11 March 2025.

33. Children and Parents: Media Use and Attitudes Report - Ofcom, <<https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/children-media-use-and-attitudes-2024/children-media-literacy-report-2024.pdf?u=368229>>, accessed 11 March 2025.

34. Pew Research Center (N 57)

35. What to do about your teenager trying social media challenges or trends - Parent Talk, <<https://parents.actionforchildren.org.uk/home-family-life/technology/teenage-social-media-challenges-trends/>>, accessed 11 March 2025.

36. Cyberbullying: Twenty Crucial Statistics for 2025 | Security.org, <<https://www.security.org/resources/cyberbullying-facts-statistics/>>, accessed 11 March 2025.

37. Is Tik Tok Safe For Kids? - Healthy Young Minds, <<https://www.healthyyoungminds.com/is-tik-tok-safe-for-kids/>>, accessed 11 March 2025.

38. Social Media and Online Grooming <<https://socialmediavictims.org/sexual-violence/online-grooming/>>, accessed 11 March 2025.

39. Social Media and Youth Mental Health | HHS.gov, <<https://www.hhs.gov/surgeon-general/reports-and-publications/youth-mental-health/social-media/index.html>>, accessed 11 March 2025.

Social Media Platform Trends



Usage Patterns

Instagram remains highly popular among teenagers, with usage rates around 62%. It is particularly favored by teen girls and older adolescents (13-17), and the daily engagement is substantial, with about half of teens using it daily and a smaller but growing percentage (8-12%) reporting "almost constant" use.⁴⁰

Popular Content

The platform centers on visual content, including photo and video sharing through the main feed, ephemeral Stories, and short-form Reels. Influencer content is prominent, and direct messaging is a key feature for communication.

Specific Risks

Uploading objectified selfies to Instagram is a behavior that may increase the risk perception and perceived likelihood of being a victim of cyberbullying compared with uploading non-objectified selfies.⁴¹ Various research studies have shown that Instagram usage by girls is related to the increased visual surveillance of one's appearance, body image concerns, and self-objectification.⁴² Exposure to inappropriate or sensitive content is remain a risk, addressed partly by features like Sensitive Content Control.⁴³

The direct messaging features and discoverability create avenues for online grooming and sextortion.⁴⁴ Privacy concerns arise from data collection practices and the potential for public exposure if accounts are not set to private. A critical issue, highlighted by investigations from The Wall Street Journal and Stanford University, involves Instagram's recommendation algorithms potentially connecting and promoting vast networks dedicated to trading CSAM, effectively facilitating contact between predators and sellers of illicit material.⁴⁵ Despite Meta reporting high volumes of CSAM detection and removal⁴⁶, these investigations raise serious questions about the effectiveness of their systems in preventing the platform from being used as a marketplace and networking tool for child exploitation.⁴⁷

40. Cyberbullying on Instagram: How adolescents perceive risk in personal selfies?, <<https://cyberpsychology.eu/article/view/33546>>, accessed 11 March 2025.

41. Cyberbullying Statistics: Insights and Analysis | VebPurify, <<https://www.webpurify.com/blog/cyberbullying-statistics/>>, accessed 11 March 2025.

42. Cohen, R., Fardouly, J., T., & Slater, A. (2018). Selfie-objectification: The role of selfies in self-objectification and disordered eating in young women. Computers in Human Behavior, 79, 68–74. <<https://doi.org/10.1016/j.chb.2017.10.037>>

43. Meta says it fixed error after Instagram users report a flood of graphic and violent content, CNBC, <<https://www.cnbc.com/2025/02/27/meta-apologizes-after-instagram-users-see-graphic-and-violent-content.html>>, accessed 11 March 2025.

44. Instagram Targets Teen Sextortion Scammers With Nude Image Filter For Direct Messages, Forbes, <<https://www.forbes.com/sites/roberthart/2024/04/11/instagram-targets-teen-sextortion-scammers-with-nude-image-filter-for-direct-messages/>>, accessed 11 March 2025.

45. Instagram Connects Vast Pedophile Network, WSJ, <<https://www.wsj.com/tech/instagram-vast-pedophile-network-4ab7189>>, accessed 11 March 2025.

46. Chapter 5 - Technology and child exploitation - Parliament of Australia, <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/ChildExploitation47thInquiry_report/Chapter_5_-_Technology_and_child_exploitation>, accessed 11 March 2025.

47. Ofcom (N 45)

Social Media Platform Trends



Usage Patterns

Snapchat is a popular platform among teens, with usage rates between 55-59%. It shows higher usage among girls and older teens. Daily usage is high (51% daily), with 14-15% reporting "almost constant" engagement.⁴⁸

Popular Content

The platform is known for its ephemeral messaging (Snaps) using photos and videos, often augmented with filters and lenses. Stories, Chat, the Discover tab (featuring content from publishers and creators), and Snap Map (location sharing) are key features.

Specific Risks

Snapchat is associated with a very high risk of cyberbullying (69% likelihood for children reported in one study).⁴⁹ The platform's features, including the ease of connecting with strangers and the perceived ephemerality of messages (though screenshots are possible), create significant risks for online grooming and sextortion.⁵⁰ The Discover tab can expose users, including children who bypass age gates, to inappropriate or adult content.⁵¹ The Snap Map feature poses privacy and potential physical safety risks if location sharing settings are not carefully managed. The disappearing nature of Snaps may lower inhibitions and encourage riskier sharing behaviors, including sexting.⁵²

48. Teens and social media: Key findings from Pew Research Center surveys, <<https://www.pewresearch.org/short-reads/2023/04/24/teens-and-social-media-key-findings-from-pew-research-center-surveys/>>, accessed 11 March 2025.

49. Cyberbullying: Twenty Crucial Statistics for 2025 | Security.org, <<https://www.security.org/resources/cyberbullying-facts-statistics/>>, accessed 11 March 2025.

50. Social Media and Online Grooming, <<https://socialmediavictims.org/sexual-violence/online-grooming/>>, accessed 11 March 2025.

51. Behind the Filters: The risks Snapchat poses to children, <<https://www.childrenssociety.org.uk/what-we-do/blogs/the-risks-snapchat-poses-to-children>>, accessed 11 March 2025.



Social Media Platform Trends

The design choices inherent in these platforms, aimed at maximizing user engagement, connection, and content discovery, simultaneously create vulnerabilities.

Features like ephemeral messaging on Snapchat, powerful algorithmic content recommendations on Instagram, TikTok, and YouTube, direct messaging capabilities across platforms, location sharing on Snapchat, and features encouraging interaction with unknown users (e.g., TikTok's For You feed, Instagram's Explore page, Snapchat's Discover tab, open gaming chats) are consistently implicated in facilitating risks such as grooming, cyberbullying, and exposure to harmful content.

Safety features, while present, often function as reactive layers rather than being integrated into the core design logic that prioritizes engagement.

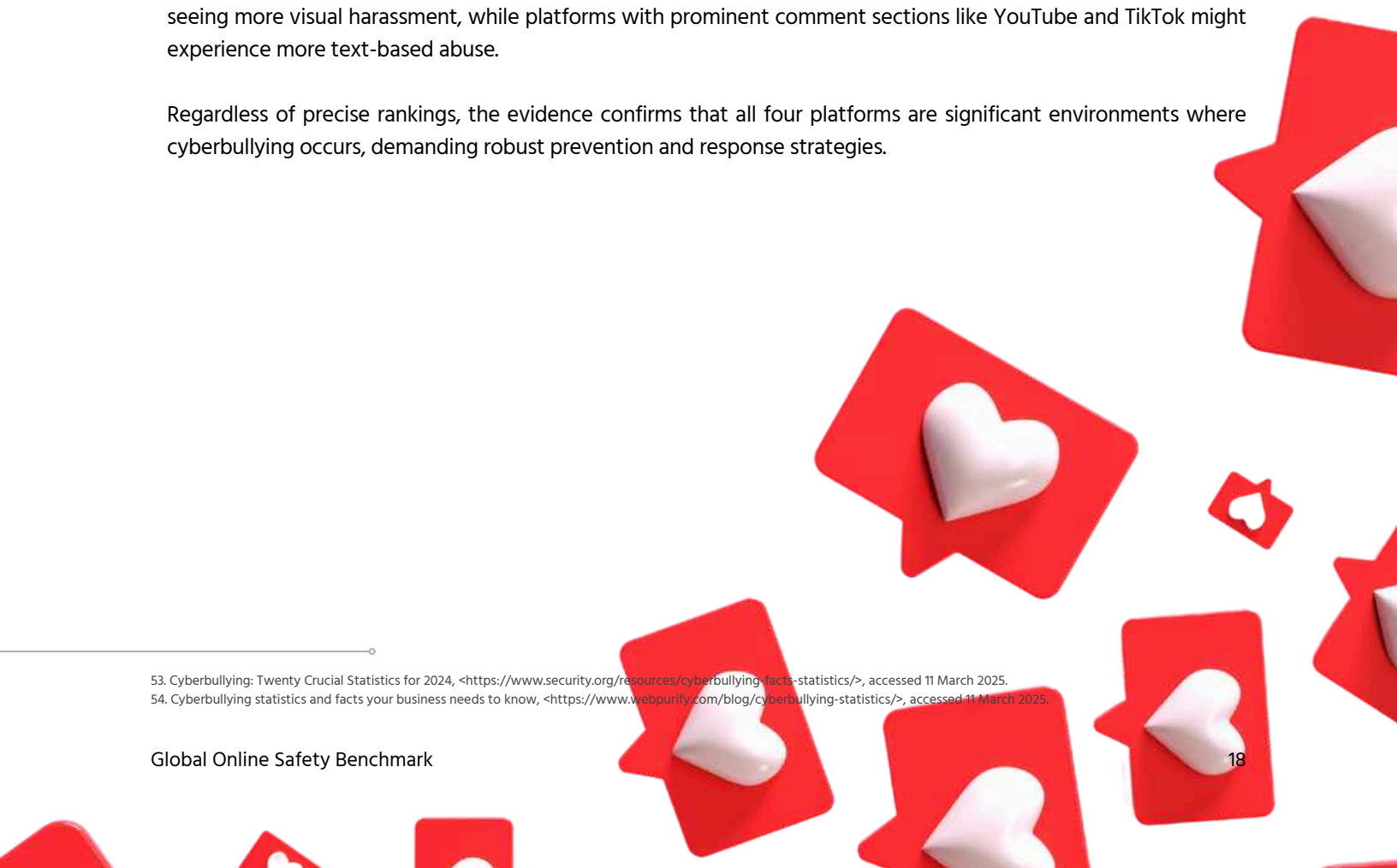
While cyberbullying is a pervasive threat across all four platforms, the available data suggests potential variations in risk levels.

Some studies indicate YouTube and Snapchat might pose a particularly high likelihood of cyberbullying for children⁵³, while others rank Instagram and Facebook highly.⁵⁴ These discrepancies may stem from differing research methodologies, definitions of cyberbullying, or the specific age groups studied. It is plausible that the nature of cyberbullying varies by platform, with image-centric platforms like Instagram and Snapchat potentially seeing more visual harassment, while platforms with prominent comment sections like YouTube and TikTok might experience more text-based abuse.

Regardless of precise rankings, the evidence confirms that all four platforms are significant environments where cyberbullying occurs, demanding robust prevention and response strategies.

53. Cyberbullying: Twenty Crucial Statistics for 2024, <<https://www.security.org/resources/cyberbullying-facts-statistics/>>, accessed 11 March 2025.

54. Cyberbullying statistics and facts your business needs to know, <<https://www.webpurify.com/blog/cyberbullying-statistics/>>, accessed 11 March 2025.



Platform Analysis: YouTube

Policies & Guidelines

YouTube, a Google service, maintains strict policies focused on child safety. The platform prohibits content that endangers the emotional or physical well-being of minors (defined as under 18). This includes specific bans on unwanted sexualization, abuse, and harmful or dangerous acts involving minors. YouTube explicitly forbids CSAM, grooming, and sextortion. A key policy prohibits content that targets young minors and families but contains mature themes such as sexual content, violence, or obscenity. Cyberbullying and harassment involving minors are also disallowed.

YouTube employs a tiered age structure. The main platform requires users to be 13 or older (or the applicable age of consent in their region) to create a standard account. For children under 13, YouTube offers the separate **YouTube Kids app**, which features curated content, stricter filters, and dedicated parental controls. For pre-teens and younger teens transitioning from YouTube Kids but not yet ready for the full platform, YouTube provides **"Supervised Experiences."** This allows parents to create a supervised Google Account for their child (managed via Google Family Link) and select from tiered content settings (Explore 9+, Explore More 13+, Most of YouTube) that filter the main YouTube platform. Age verification is tied to the Google Account system.

Enforcement of these policies involves removing violating content. YouTube uses a system of warnings and strikes for Community Guideline violations; accumulating three strikes within 90 days typically results in channel termination. Severe abuse cases or channels dedicated to violations can lead to immediate termination. YouTube reports illegal CSAM (referred to as CSAI - Child Sexual Abuse Imagery - for videos) to NCMEC and assists law enforcement when a child is believed to be in danger.

YouTube provides transparency through its regular Community Guidelines Enforcement Reports and a dedicated Google-wide CSAM Transparency Report. This specific report details NCMEC reporting numbers, Google Account disables for CSAM, CSAM removals from Google Search, and the number of CSAM hashes Google contributes to the shared industry database.

The platform's distinct, multi-layered approach to age-appropriateness (YouTube Kids, Supervised Experiences with defined content levels, and standard YouTube with additional filters like Restricted Mode) represents a structured attempt to cater to different developmental stages. This system offers potentially more granular control than a single age gate but places a significant onus on parents to understand the different tiers, select the appropriate level for their child, and actively manage the associated Google Account and Family Link settings. The effectiveness hinges on parental engagement and the accuracy of the underlying Google Account age information.



Platform Analysis: YouTube

Technical Safety Measures

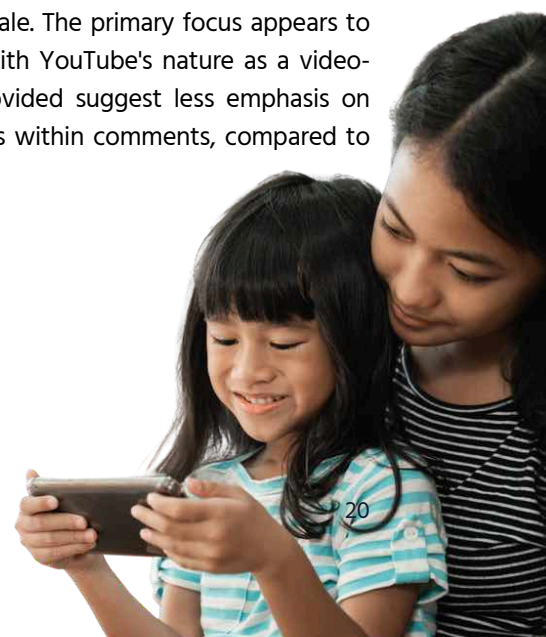
YouTube leverages Google's significant technological resources for child safety enforcement. Machine learning (ML) systems are employed extensively to proactively detect policy violations across videos, playlists, thumbnails, and comments. These automated systems analyze various signals, including video titles, descriptions, metadata, and language used. Content flagged by ML systems may be automatically removed if confidence is high, or escalated to human review teams for verification. ML also identifies videos that, while not strictly violating policies, may pose risks to minors; these videos may have features restricted (like comments or recommendations) or be age-gated. Google/YouTube actively works on discovering never-before-seen CSAM using ML classifiers, which are then confirmed by specialist human reviewers.

Hash-matching technology is a critical component, particularly YouTube's proprietary CSAI Match system for detecting known illegal videos. Content matching known CSAM hashes is automatically removed and reported to NCMEC. Google is a major contributor of unique CSAM hashes discovered on its platforms to the central NCMEC database, aiding industry-wide detection efforts.

Text analysis is used in various ways. Video metadata (titles, descriptions, tags) and language are analyzed by detection systems. Comments are also scanned for violations. Google Search employs algorithms to identify CSAM-seeking queries, filtering explicit results and displaying warnings or links to support organizations in many regions. Regarding specific risks, YouTube takes steps to detect child abuse in livestreams and restricts live features (like chat) on content deemed potentially risky for minors. While policies prohibit grooming, and one external report suggests YouTube uses technology for grooming detection, the platform's public-facing technical descriptions emphasize the detection of exploitative content (sexualization, CSAM) more explicitly than the detection of grooming conversations within interactive features like comments.

A notable aspect of Google/YouTube's approach is the sharing of its safety technology. Both CSAI Match and the Content Safety API (which uses classifiers to prioritize potentially abusive content for review) are made available free of charge to qualifying external organizations, including other platforms and NGOs, to aid their own child safety efforts.


YouTube's technical measures demonstrate significant strength in detecting known CSAM through hashing (CSAI Match) and leveraging Google's ML capabilities for analyzing video content at scale. The primary focus appears to be on the analysis and classification of uploaded video content, which aligns with YouTube's nature as a video-sharing platform. While comment moderation exists, the technical details provided suggest less emphasis on proactively detecting risky interpersonal interactions, such as grooming attempts within comments, compared to the robust systems described for video content analysis.



Platform Analysis: YouTube

Design Features for Safety

YouTube offers several design features and settings to manage content exposure and user interaction, operating across its different access tiers (Kids, Supervised, Standard).



Restricted Mode is an optional filter available on the standard YouTube platform. It aims to screen out potentially mature content identified through automated signals (metadata, title, language) and human-applied age restrictions. When enabled, Restricted Mode also hides all video comments. It can be turned on by individual users or enforced by network administrators (e.g., in schools, libraries) or parents via Google Family Link for supervised accounts. While helpful, YouTube acknowledges that this mode is not infallible and relies on automated systems that can make mistakes. **Age-Restricted Content** is a separate classification applied by human review teams to videos deemed inappropriate for users under 18, based on factors like vulgar language, violence, nudity/sexual suggestiveness, or portrayal of harmful activities. Such content is not accessible to users who are logged out, under 18, or have Restricted Mode enabled. This includes content deceptively packaged as family-friendly but containing adult themes.

The YouTube Kids app provides a distinct, highly curated environment with its own interface, stricter content filters based on age categories (Preschool, Younger, Older), and specific parental controls like timers, channel/video approval, and the ability to disable search. **Supervised Experiences**, managed through a supervised Google Account and Family Link, allow parents to choose one of three content levels (Explore 9+, Explore More 13+, Most of YouTube) that filter the main YouTube platform. Importantly, certain features are disabled in supervised mode, including the ability for the child to create content (upload videos, create channels, post comments), participate in live chat, or make purchases.

Reporting tools allow users to flag specific videos, comments, or entire channels that violate Community Guidelines. A specific flag for "Child Abuse" is available. YouTube also operates a "Trusted Flagger" program, granting prioritized review status to reports from vetted individuals and organizations. **Comment sections**, often identified as a source of risk, are subject to several controls. As mentioned, they are hidden in Restricted Mode and disabled for most content designated as "Made for Kids" under COPPA regulations. Comments may also be automatically disabled by YouTube on videos featuring minors that are deemed potentially risky. Creators also possess tools to moderate comments on their own channels.

Digital Wellbeing features include optional "Take a Break" and "Bedtime" reminders, which are turned on by default for users under 18. The autoplay feature (automatically playing the next video) is also turned off by default for users under 18. Additionally, YouTube limits repeated recommendations of certain sensitive topics (e.g., related to body image, social aggression) for teen viewers.

The array of safety controls offered by YouTube (Restricted Mode, Age Restrictions, Supervised Experiences, YouTube Kids) provides parents with multiple options for tailoring access. However, this layered system introduces complexity. Parents need to understand the distinctions between these modes—for example, that Restricted Mode is a filter on standard YouTube, while Supervised Experiences operate through a specific account type with different content levels and feature limitations, and YouTube Kids is a separate app entirely. Effective use requires careful selection of the appropriate tier and active management, often through the linked Google Family Link account.

Platform Analysis: YouTube

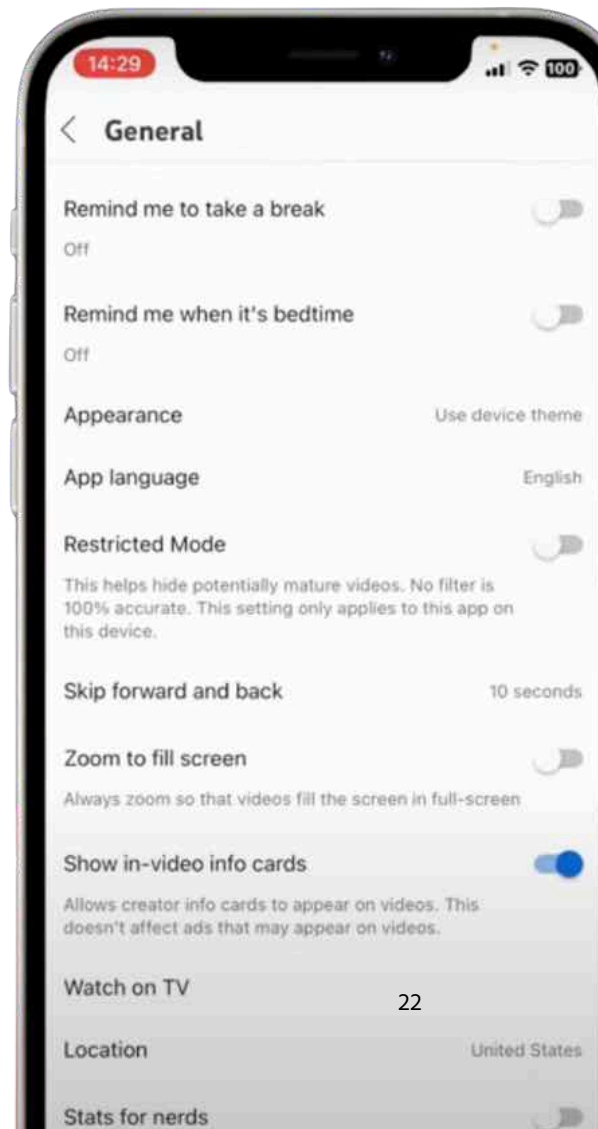
Parental Controls

YouTube's primary parental controls for the main platform are delivered through Supervised Experiences, which are intrinsically linked to Google Family Link. This system is designed for parents whose children (typically pre-teens under 13, or older if the account was set up before they reached the age of consent) are deemed ready to move beyond the YouTube Kids app but still require oversight. It requires the child to have a Google Account managed by the parent through Family Link.

Key features managed via Family Link for the YouTube supervised experience include:

- **Content Level Settings:** Parents choose one of three predefined content levels that filter the main YouTube platform: "Explore" (generally suitable for ages 9+), "Explore More" (generally suitable for ages 13+), or "Most of YouTube" (includes nearly all content except age-restricted videos). Parents can adjust this setting as the child matures.
- **Feature Restrictions:** Supervised accounts automatically have certain YouTube features disabled. Children using a supervised account cannot upload videos, create channels or posts, comment publicly, participate in live chat, or make purchases. Live streams are generally available only in the "Explore More" and "Most of YouTube" settings (excluding Premieres).
- **History Management:** Parents can view their child's watch and search history through Family Link or on the child's device. They can also choose to pause or clear the watch and search history for the supervised account.
- **Blocking:** Parents can block specific channels directly within YouTube when signed in with their linked parent account, preventing those channels from appearing in their child's supervised experience. Parents can also unblock videos previously blocked via YouTube Kids.
- **General Family Link Controls:** Beyond YouTube-specific settings, Google Family Link offers broader device and account management features, such as setting overall screen time limits for devices, approving or blocking app downloads, managing location sharing (for Android devices), and filtering content on Google Search (SafeSearch is on by default for supervised accounts).

The YouTube Supervised Experience, integrated with Google Family Link, provides a structured pathway for graduated access to the main platform with significant parental oversight regarding content levels and feature availability. **The automatic disabling of interactive features like commenting and content creation within the supervised mode is a key differentiator, significantly reducing avenues for potential harassment or risky interactions compared to standard accounts.**



Platform Analysis: YouTube

Report Handling Process

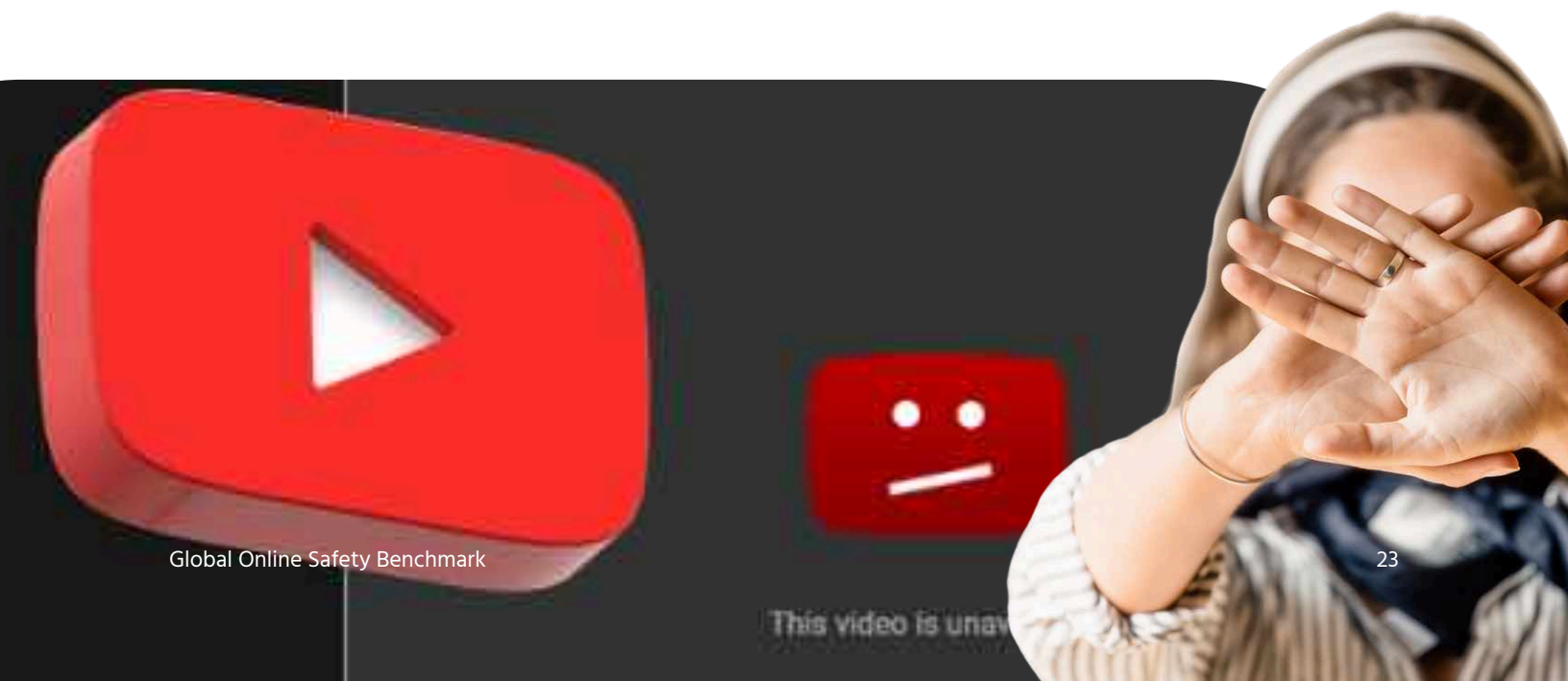
YouTube's process for handling reports of child safety violations, including grooming and exploitation, involves user flagging, automated detection, human review, and escalation to NCMEC and law enforcement. Users can report content they believe violates the Child Safety Policy or other Community Guidelines by flagging individual videos, comments, or entire channels using the platform's reporting tools. A specific "Child Abuse" flagging reason is available. For more complex situations involving multiple pieces of content, a more detailed complaint can be filed via a dedicated reporting tool. Reports from members of the Trusted Flagger program receive prioritized review.

Flagged content, along with content proactively identified by automated systems (ML classifiers, hash matching), is reviewed by human moderators. These reviewers verify whether the content violates policies and take appropriate action. Their decisions also help train the automated systems.

If content is found to violate the Child Safety policy, it is removed, and the uploader receives an email notification. Depending on the severity and frequency of violations, this can lead to warnings, Community Guideline strikes (which can result in temporary feature restrictions), or channel/account termination. YouTube states a zero-tolerance policy for predatory behavior.

A critical step for illegal content, specifically CSAM/CSAI, is escalation to NCMEC. When YouTube identifies videos containing CSAI or users soliciting such material (e.g., via comments), the content is removed, hashed (given a unique digital fingerprint), and reported to NCMEC's CyberTipline. NCMEC then liaises with relevant global law enforcement agencies. Google provides data on these NCMEC reports in its CSAM Transparency Report.

Direct escalation to law enforcement occurs if YouTube believes a child is in immediate danger based on reported content. Users who believe a child is in immediate danger are also encouraged to contact local law enforcement directly. The process relies heavily on YouTube's technical capacity for detection (especially CSAI Match for known videos) and its human review teams. The established pathway through NCMEC is the primary mechanism for reporting illegal material to authorities, consistent with US law and industry practice. The effectiveness hinges on both the platform's internal processes and the subsequent actions taken by NCMEC and law enforcement.



Platform Analysis: TikTok

Policies & Guidelines

TikTok's Community Guidelines explicitly forbid a wide range of activities related to child endangerment. The platform states a zero-tolerance policy for Child Sexual Exploitation and Abuse (CSEA), encompassing Child Sexual Abuse Material (CSAM) – including AI-generated depictions – grooming, pedophilia, sextortion, sexual solicitation, and the sexual harassment of individuals under 18. This zero-tolerance stance extends specifically to predatory or grooming behavior. Beyond direct exploitation, policies also prohibit content that might facilitate harm, such as encouraging minors to move conversations off-platform where risks are higher, or displaying semi-nudity of young people due to the potential for unintended sexualization.

The platform mandates a minimum user age of 13 years. In the United States, a distinct, more restricted "TikTok for Younger Users" experience is offered for those under 13, featuring curated content and enhanced safety protections in partnership with Common Sense Networks. While an age gate requiring a full birthdate is used during sign-up, users can potentially falsify this information. TikTok states it uses various methods, including moderator training and analysis of keywords and user reports, to identify and suspend or ban suspected underage accounts.

Enforcement actions for policy violations, particularly severe offenses like CSEA or repeated infractions, include content removal and permanent account bans. Notably, TikTok considers off-platform activities related to violence, hate, and CSEA when making decisions about account bans. The platform commits to transparency through its Community Guidelines Enforcement Reports, which provide data on content and account removals, including those related to underage use, and through specific communications regarding its CSEA efforts.

While TikTok's Community Guidelines present a comprehensive stance against CSEA, explicitly prohibiting grooming and exploitation, the practical effectiveness of these policies faces scrutiny. Reports suggest challenges in enforcing against nuanced behaviors compared to overt CSAM, coupled with the inherent difficulties in accurately identifying underage users who misrepresent their age. The reliance on self-attested age gates and detection of "signs" of underage use creates vulnerabilities, potentially leading to a gap between the breadth of the stated policy and the depth of its real-world enforcement, as evidenced by user observations of grooming normalization on the platform.



Platform Analysis: TikTok

Technical Safety Measures

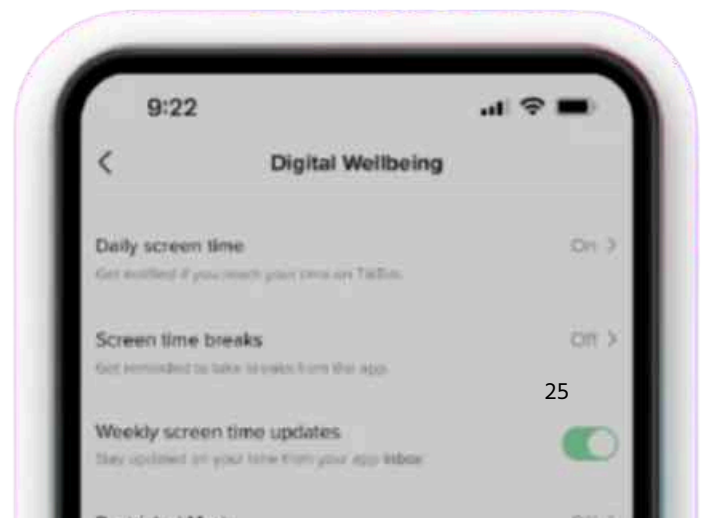
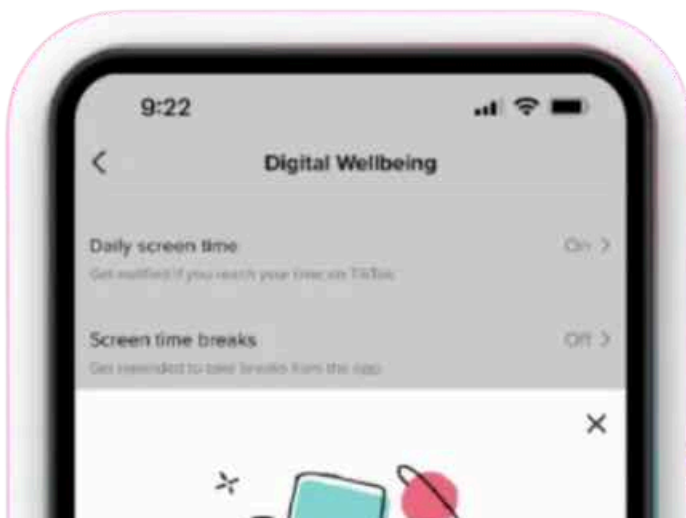
TikTok employs a multi-layered technological approach to detect and prevent harmful content. Automated systems, utilizing machine learning, review uploaded content by analyzing signals such as keywords, images, captions, and audio. If a potential violation is detected with high confidence, the system may automatically remove the content; otherwise, it is flagged for human review by safety teams. TikTok reports high proactive removal rates, suggesting these systems catch a significant volume of violating content before user reports. Automation is particularly focused on categories like minor safety, where the platform claims high accuracy.

To combat known CSAM, TikTok utilizes industry-standard hash-matching technology. This involves comparing the unique digital fingerprints (hashes) of uploaded images and videos against extensive databases compiled by NCMEC and the Internet Watch Foundation (IWF). Matches prevent the re-upload and circulation of previously identified illegal material. TikTok also leverages external technologies, including Google's Content Safety API, YouTube's CSAI Match, and Microsoft's PhotoDNA, to bolster its internal detection systems.

Keyword filtering is another key technical measure. TikTok maintains and applies databases of keywords and phrases associated with CSEA and behaviors indicative of grooming. This includes filtering "red-flag language" identified through industry collaboration and internal analysis. Users are also given tools to filter specific keywords from their own feeds. Furthermore, the platform uses the IWF's URL database to block known links leading to CSAM, and removes links posted in violation of its rules.

For problematic searches, TikTok blocks queries associated with CSEA/CSAM and deploys in-app interventions that warn users about the potential illegality of such searches, directing them towards offender deterrence resources. In the context of live streaming, which requires users to be 18 or older to host, TikTok reportedly uses technology to detect child abuse.


This heavy investment in diverse technologies illustrates a commitment to technical safety solutions. However, the digital landscape presents continuous challenges. The emergence of sophisticated AI-generated CSAM necessitates the development of new detection paradigms beyond traditional hashing. The sheer volume of content uploaded daily means that even highly accurate automated systems will have limitations, including false positives and negatives, underscoring the ongoing need for robust human moderation and constant adaptation of technical tools. Some external comparisons have also suggested potential gaps in TikTok's detection capabilities in specific areas relative to peers.



Platform Analysis: TikTok

Design Features for Safety

TikTok incorporates numerous safety considerations into its platform design, particularly for younger users. **Accounts belonging to users aged 13-15 are set to private by default upon creation.** This default setting significantly restricts visibility and interaction: only approved followers can view their videos, read their bio, or interact with their content. Furthermore, content from these accounts cannot be downloaded and is ineligible for recommendation in the main "For You" feed, limiting its reach.



Direct Messaging (DM) features have stringent age-based restrictions. For users aged 13-15, DMs are entirely disabled. For those aged 16-17, DMs default to "No One," meaning the user cannot receive messages unless they proactively change this setting to allow messages from "Suggested friends" or "Friends" (mutual followers). These settings can be managed by parents through the Family Pairing feature. A critical design choice is the prohibition of sending images or videos within TikTok's direct messages. The platform explicitly links this decision to studies showing the role of image/video messaging in CSAM proliferation.

Interaction features like Duet and Stitch are also age-restricted. These features are disabled for users under 16. For 16- and 17-year-olds with public accounts, the default setting is "Friends only". Commenting abilities are similarly tiered: users aged 13-15 default to "Friends only" and can only change this to "No one". Users aged 16-17 with public accounts default to "Everyone" but retain options to restrict comments.

Content filtering options provide additional layers of control. A "Restricted Mode" can be enabled (optionally, or via Family Pairing) to limit exposure to content identified as potentially mature or complex. Users can also manually filter specific keywords or hashtags from their "For You" and "Following" feeds. TikTok also employs internal "content levels" to automatically restrict overtly mature content from being shown to users under 18.

Reporting mechanisms are integrated throughout the app. Users can report specific videos, comments, accounts, or hashtags directly. A dedicated reporting category exists for "Exploitation and abuse of people under 18", and reports concerning potential CSEA receive priority handling. Teens using Family Pairing have the option to notify a linked parent when they submit a report. Other safety-oriented design features include the 18+ age requirement for hosting LIVE sessions and sending virtual gifts during LIVEs, and automatic nighttime restrictions on push notifications for teen accounts.

The platform's approach demonstrates strong "safety by default" principles for its youngest teen users (13-15), implementing significant restrictions on interaction and visibility automatically. This contrasts with the greater autonomy granted to older teens (16-17), who can modify settings like DMs and comment permissions more freely. This difference highlights the importance of parental involvement through Family Pairing or vigilant personal safety practices for this older teen cohort. The platform-wide ban on sending images or videos in DMs stands out as a fundamental design choice aimed squarely at mitigating a known vector for CSAM distribution and grooming attempts.

Platform Analysis: TikTok

Parental Controls

TikTok's primary parental control suite is "Family Pairing," which requires both the parent/guardian and the teen to have TikTok accounts and mutually agree to link them, typically via scanning a QR code or using an invite link. Once linked, parents gain access to a range of controls and insights accessible through their own account settings.

A core component is Screen Time Management. Parents can set daily time limits for their teen's TikTok usage (with a default of 60 minutes for all users under 18). These limits can be customized for different days of the week. Parents receive a usage dashboard summarizing daily time spent and app opens over the previous weeks. They can also schedule specific "time away" periods when the app is inaccessible to the teen and can choose to provide a passcode to allow temporary access beyond the set limits.

Family Pairing provides significant control over Content and Privacy Settings. Parents can remotely enable or disable "Restricted Mode" to filter potentially mature content. They can manage the teen's search functionality, restricting the ability to search for videos, hashtags, or LIVEs. Parents can switch the teen's account between private and public (though teens under 16 default to private). Keyword filtering allows parents to add specific words or hashtags they wish to exclude from the teen's feeds. Control over the STEM feed's visibility is also provided, as is the ability to prevent the teen's account from being suggested to others.

Interaction Management is another key area. Parents can manage Direct Message settings for teens aged 16 and older, restricting senders or disabling DMs entirely. They can control who is allowed to comment on the teen's videos and who can view the teen's liked videos. Depending on the region, parents may also be able to view their teen's following and follower lists, as well as accounts the teen has blocked.

Parents can also manage Notifications, setting schedules to mute push notifications beyond the platform's default nighttime restrictions, and can opt to receive alerts about activity related to the linked accounts, such as if the pairing is unlinked.

The Family Pairing feature set is arguably one of the most comprehensive available among major platforms, offering granular control over time, content, privacy, and interactions. However, its utility depends entirely on parental awareness that it exists, the willingness of both parent and teen to set it up, and the parent's ongoing engagement in managing the settings and discussing them with their teen. It is important to note that Family Pairing does not grant parents the ability to read the content of their teen's direct messages (where applicable for 16+), thus maintaining a boundary of conversational privacy.



Platform Analysis: TikTok

Report Handling Process

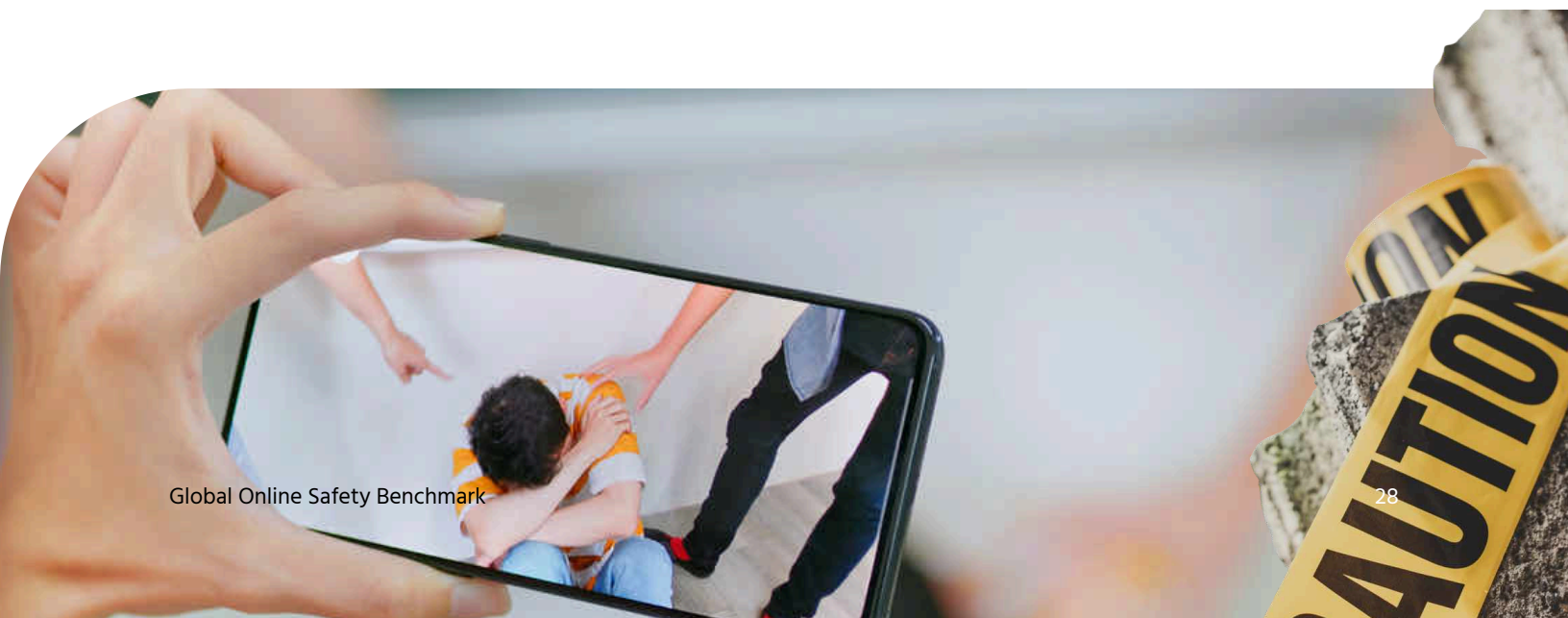
TikTok's process for handling reports of grooming and exploitation involves several stages, combining automated systems and human oversight. Reports are initiated by users through in-app or online reporting tools, including a specific category for "Exploitation and abuse of people under 18". Proactive detection systems also flag potentially violating content or behavior.

Once flagged or reported, content undergoes review by a combination of automated technology and human moderation teams. TikTok states that its dedicated Child Safety Team prioritizes reports indicating immediate risk, such as active grooming, sextortion, or ongoing abuse situations. If a violation is confirmed, TikTok takes enforcement action, which can range from removing the specific content to permanently banning the user's account. For severe violations like CSEA, this can include banning the user's device to prevent re-registration and banning any other accounts associated with the offender. The platform also actively filters language indicative of grooming and shares relevant information about such situations with NCMEC.

Escalation to external bodies is a critical part of the process. TikTok reports all suspected CSEA, along with supporting evidence, to NCMEC via their CyberTipline. NCMEC then assesses these reports and coordinates with relevant law enforcement agencies globally. In cases where TikTok believes there is a specific, credible, and imminent threat to a young person's life or of serious physical injury, the platform may bypass the standard NCMEC route and report directly to the relevant law enforcement authorities.

Communication back to the person who filed the report is not explicitly detailed for grooming/exploitation cases in the provided materials, beyond standard notifications about content removal or account actions.

The platform's stated prioritization of immediate risks like grooming and its reliance on the NCMEC reporting pathway for CSEA align with U.S. legal requirements and broader industry practices. The effectiveness of this system depends not only on the quality and timeliness of TikTok's internal detection and reporting but also on the capacity and prioritization of NCMEC and downstream law enforcement agencies to act on the information received. Some historical reports have noted lower NCMEC reporting volumes from TikTok compared to platforms like Meta, although platform practices and reporting capabilities evolve over time.



Platform Analysis: Instagram

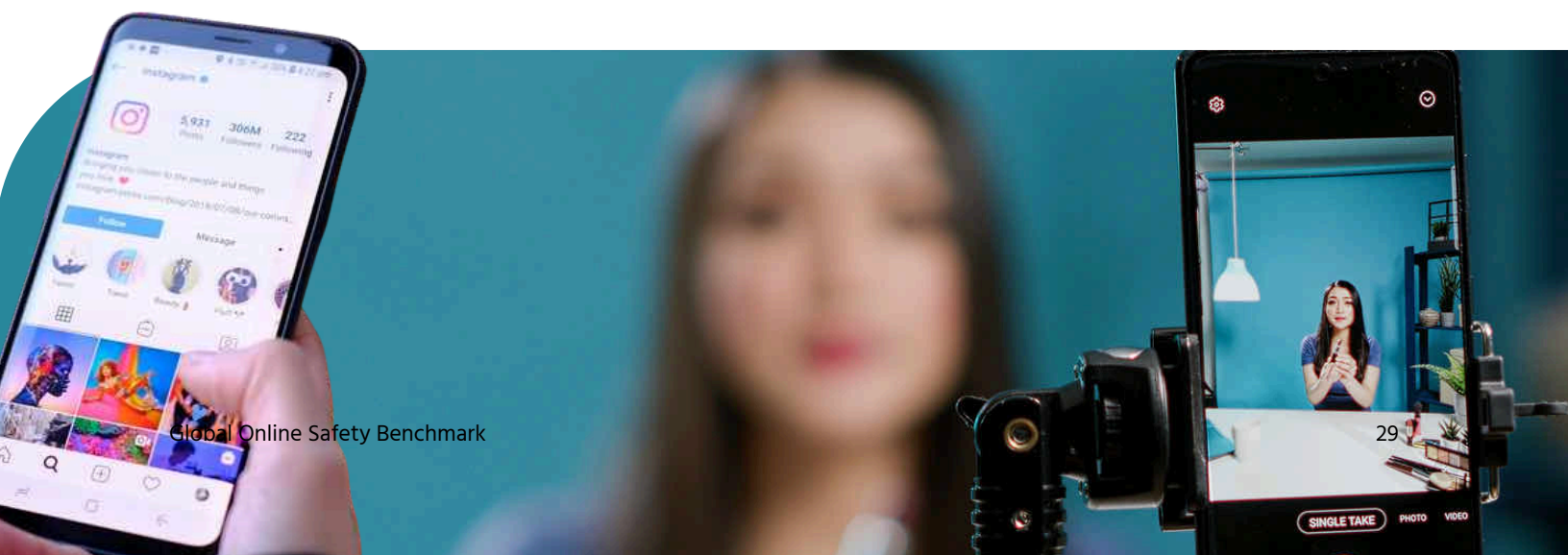
Policies & Guidelines

Instagram, owned by Meta, enforces comprehensive policies aimed at protecting minors. The platform explicitly prohibits content that endangers children, covering child nudity, physical abuse, and all forms of sexual exploitation. This ban extends to CSAM (including AI-generated), grooming behaviors, sextortion, inappropriate interactions initiated by adults towards teens, and both explicit and implicit sexualization of minors. Meta emphasizes a zero-tolerance policy and takes action against accounts dedicated to sharing even seemingly innocent images of children if they are accompanied by inappropriate or sexualizing comments or captions. Broader Community Standards also forbid bullying, harassment, hate speech, the glorification of self-injury (including eating disorders), and the offering of sexual services.

The minimum age requirement for Instagram is 13 years old. Meta employs various methods for age verification, including user-provided birthdays, requests for photo identification, and video selfie analysis technology. Sign-ups indicating an age below 13 are blocked. The platform investigates reports of suspected underage users and disables accounts where reliable evidence confirms the user is under 13, offering an age verification appeal process.

Enforcement actions for violations include content removal and account disablement, particularly for severe or repeated offenses involving child safety. Meta actively reports apparent child exploitation, primarily CSAM, to NCMEC, fulfilling its legal obligations as a US-based company. The company also cooperates with law enforcement agencies when there are perceived risks of physical harm or threats to public safety. Meta publishes regular Community Standards Enforcement Reports detailing actions taken against violating content and accounts across various categories, including child endangerment, and provides additional transparency on NCMEC reporting.

Meta's policies demonstrate a broad scope, attempting to address not only illegal CSAM but also more nuanced forms of potential harm like implicit sexualization and suggestive commentary around minors' content. This reflects an awareness of the diverse ways exploitation can manifest online. However, the effectiveness and consistency of enforcing these broad policies have been significantly challenged by external investigations and reports. Notably, research by the Wall Street Journal and Stanford University found that Instagram's own recommendation algorithms were actively connecting and promoting vast networks dedicated to trading CSAM, suggesting a fundamental conflict between platform mechanics designed for engagement and stated safety goals. Reports also indicate failures in timely responses to user reports of child abuse material.



Platform Analysis: Instagram

Technical Safety Measures

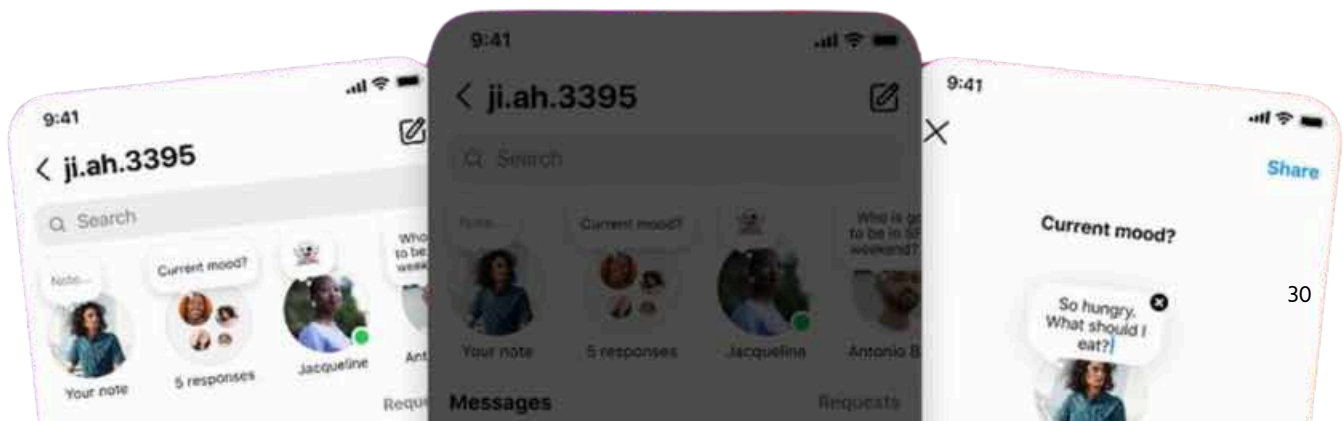
Meta employs extensive technological infrastructure for safety enforcement on Instagram, relying heavily on AI and machine learning for proactive detection. **These systems analyze content (images, videos, text) to identify violations of Community Standards, including CSEA.** Meta reports high proactive detection rates, indicating that a large volume of violating content, particularly CSAM, is found and removed before user reports. Specialized technology is used to identify adult accounts exhibiting potentially suspicious behavior towards minors, such as patterns of being blocked or reported by young users. The platform also utilizes Google's Content Safety API to aid in prioritizing potentially harmful content for review.

Hash-matching technology is a cornerstone of CSAM detection. Instagram uses databases of known CSAM hashes, including those from NCMEC and likely incorporating technologies like PhotoDNA through Meta's partnerships. This allows for the rapid identification and removal of previously reported illegal images and videos. Instagram also participates in NCMEC's "Take It Down" program, which uses hashes generated by victims themselves to remove non-consensually shared intimate images created when they were minors.

Text analysis plays a role through the "Hidden Words" feature, which allows users (and is applied by default in some cases) to filter out comments and DM requests containing offensive keywords, phrases, or emojis. AI systems also analyze text accompanying images (captions, comments) to assess the risk of sexualization, even if the image itself is benign.

Meta actively works to detect and dismantle coordinated networks engaged in violating activities, including child exploitation. This involves identifying interconnected accounts and taking action against the network as a whole, aiming to prevent offenders from simply creating new accounts. Task forces have been established internally to address findings related to CSEA networks operating on the platform. While policies explicitly ban AI-generated CSAM, detecting novel, AI-created abusive content poses a significant technical challenge, as it won't match existing hash databases. Current methods rely on classifiers and potentially biometric analysis of image proportions, but this remains an evolving area.

Meta operates safety systems at an immense scale, reflected in the high volume of proactive CSEA detections reported. The development of tools to identify suspicious adult accounts and disrupt harmful networks demonstrates sophisticated approaches to safety. However, a critical tension exists: the platform's core engagement-driven recommendation algorithms have been shown to inadvertently amplify and connect CSEA networks. This suggests that the platform's own architecture can undermine its safety efforts, creating situations where detection systems may be insufficient to counteract the risks generated by recommendation systems optimized for user engagement.



Platform Analysis: Instagram

Design Features for Safety

Instagram has implemented a suite of design features and default settings aimed at creating a safer environment for minors. A key measure is defaulting new users under 16 (or under 18 in certain regions) into Private Accounts. This means only approved followers can see their posts, Stories, and Reels, and comment on their content. Existing accounts are prompted to switch, and supervised teens under 16 require parental approval to make their account public.

Direct Messaging (DM) capabilities for teens are significantly restricted. Adults over 18 (or 19) are prevented from initiating private chats with teens who do not follow them. Message requests from non-followers are limited to a single text-only message. Furthermore, a recent default setting change means teens under 16/18 generally cannot receive DMs or be added to group chats by anyone they do not follow or are not already connected to, including other teens. Changing this restrictive default requires parental approval for supervised teens. Instagram also deploys safety notices within DMs to warn teens interacting with adults exhibiting potentially suspicious behavior patterns. A planned feature aims to automatically blur images containing suspected nudity in DMs, with parental permission required for teens under 16 to disable this blurring.

Other Interaction Controls provide further safeguards. By default, accounts that teens do not follow cannot tag or mention them, nor use their content in Reels Remixes or Guides. Comprehensive comment controls allow users to filter offensive language ("Hidden Words"), block specific users, restrict comments to followers, or turn them off entirely. Comments from potentially suspicious adult accounts are automatically hidden on teens' public posts.

Content Filtering is managed through the "**Sensitive Content Control**" feature. Teens under 16/18 are defaulted into the "Less" setting, which limits their exposure to potentially sensitive content (that doesn't necessarily violate guidelines but may be inappropriate) in discovery surfaces like Explore, Reels, Search, and recommendations. Parental approval via Supervision is needed for teens under 16 to change this setting to "Standard". Additionally, for teens under 16, Instagram hides certain sensitive content categories (e.g., related to self-harm, eating disorders, borderline adult nudity) even if shared by people they follow. Visibility of content related to restricted goods (alcohol, tobacco, etc.) is also limited for all users under 18. An "Alternate Topic Nudge" prompts teens who dwell on a single content type in Explore to discover something new.

Standard Reporting and Blocking tools are readily available. Users can report posts, comments, DMs, profiles, or Stories that violate guidelines. Reporting is anonymous. Blocking prevents all interaction and visibility. **The "Restrict"** feature offers a less confrontational way to limit interactions from specific accounts, while the "Limits" feature can temporarily hide comments and DMs from new followers or non-followers during periods of unwanted attention. Additional features include requiring parental permission via Supervision for teens under 16 to host Instagram Live sessions, an Activity Dashboard for self-monitoring time, Quiet Mode/Sleep Mode features, and the option to hide like counts.

Instagram's safety design demonstrates a layered and evolving approach, particularly strengthening default protections for younger teens (under 16). The shift towards requiring parental approval via Supervision for loosening key defaults like account privacy, DM restrictions, and sensitive content filtering marks a significant move towards shared control. These increasingly stringent defaults aim to create a more age-appropriate and protected environment from the outset, addressing concerns about unwanted contact and exposure to harmful content.

Platform Analysis: Instagram

Parental Controls

Instagram's parental controls are accessed through the Meta Family Center and operate under the "Supervision" feature set. Setting up Supervision requires mutual consent between the parent/guardian and the teen (aged 13-17) and is initiated via an invitation link. Either party can choose to remove Supervision at any time. Supervision automatically ends when the teen turns 18.

Supervision provides parents with significant Monitoring and Visibility into their teen's account activity and settings. Parents can see the total amount of time their teen spends on Instagram (including time on Threads if used) on a daily and weekly average basis. They can view the teen's list of followers and the accounts the teen is following, as well as a list of accounts the teen has blocked. Parents can also view their teen's key safety and privacy settings, including account privacy status, DM controls, sensitive content filter level, and tag/mention permissions. If a teen makes a report on Instagram and chooses to share this information, the parent receives a notification including the report type and the reported account's name.

Time Management tools allow parents to set daily time limits for Instagram/Threads usage, ranging from 15 minutes to 2 hours, or set no limit. Once the limit is reached, the app becomes unavailable (unless the teen requests and receives an extension, which the parent can approve/deny). Parents can also schedule specific break times or "sleep mode" periods (e.g., during school hours or overnight) when the app is blocked.

A significant aspect of Supervision, particularly for teens under 16, is the Setting Approvals mechanism. Parents receive a notification and must approve or deny any request made by their supervised teen (under 16) to change certain default safety and privacy settings to a less restrictive state. This includes attempts to switch from a private to a public account, change the Sensitive Content Control from "Less" to "Standard," or alter DM settings to allow messages from non-followers. Parental approval is also required for supervised teens under 16 to host an Instagram Live session or to disable the planned automatic blurring of potentially nude images in DMs.

Instagram's Supervision tools have evolved significantly from their initial launch. The introduction of parental approval requirements for key safety setting changes for younger teens represents a shift towards a model of shared control, granting parents more direct power to maintain protective defaults compared to systems based solely on notifications. This approach offers more intervention capability than Snapchat's Family Center but, like other platforms, still necessitates teen consent for the initial setup and does not provide parents with access to the content of their teen's messages, balancing oversight with a degree of privacy.



In April 2025, Meta has launched the #CerdasDigital2025 initiative in Indonesia to empower parents in guiding teens through the digital world. In partnership with key ministries and the Indonesian Child Protection Commission, the campaign introduces **"Teen Accounts"** on Instagram with critical safety features.

These include default private profiles, strict content controls, limited nighttime notifications, usage break reminders, and message restrictions to only connected users.

These features aim to create a safer, age-appropriate digital experience for youth.

Platform Analysis: Instagram

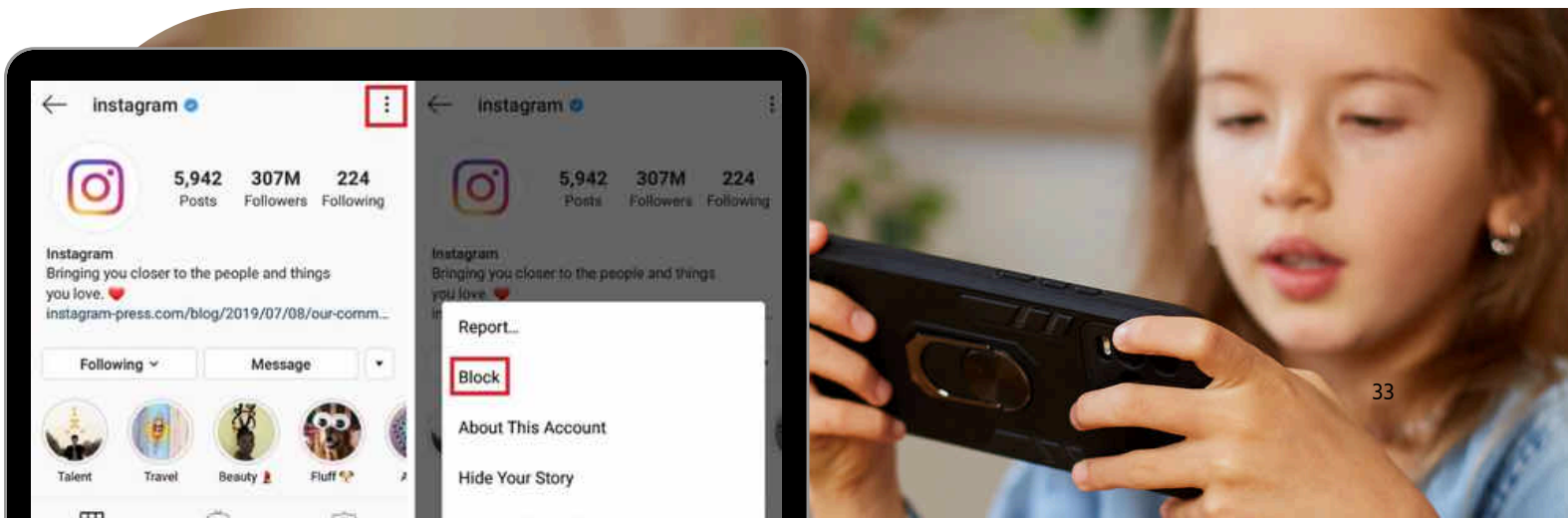
Report Handling Process

Instagram's process for addressing reports related to grooming and exploitation leverages user reporting, proactive detection, and established escalation pathways. Users can flag content (posts, comments, DMs, Stories) or profiles that violate Community Standards using built-in reporting tools. To prioritize child safety issues, a specific option to report content that "involves a child" was added under the "Nudity & Sexual Activity" category. Proactive systems, including AI/ML classifiers and hash matching, also constantly scan for and flag potential CSEA and other violations. Supervised teens can optionally notify their parents when they make a report.

Reports are reviewed by Meta's global content moderation teams, which operate 24/7. This review involves both automated systems and human reviewers. Reports concerning child safety are given priority. Meta utilizes a taxonomy developed with experts to assess the apparent intent behind sharing child exploitative content, distinguishing between potentially malicious sharing and non-malicious sharing (e.g., raising awareness, memes). Confirmed violations lead to enforcement actions, primarily content removal and, for more severe or repeated offenses, account disablement. For users identified as sharing viral or meme-based CSAM without apparent malicious intent, Meta may send safety alerts explaining the harm and policy violation, in addition to removing the content and reporting it to NCMEC. Users generally have the right to appeal decisions, unless there are extreme safety concerns associated with the content or account.

The primary escalation path for CSEA is reporting to NCMEC. Meta is documented as the largest single reporter of CSAM to NCMEC's CyberTipline. NCMEC then coordinates with global law enforcement. Instagram also works directly with law enforcement agencies when there is a perceived threat of physical harm or risk to public safety, and provides user information in response to valid legal requests like subpoenas or warrants.

While reporting is anonymous to the reported user, the system's communication back to the reporter regarding grooming or exploitation cases isn't explicitly detailed beyond potential notifications of enforcement actions taken (e.g., content removed). The option for supervised teens to notify parents adds a layer of potential communication. However, external reports and investigations have raised significant concerns about the platform's responsiveness and effectiveness in handling user reports, citing instances where reports of CSAM or exploitative networks were allegedly ignored or met with automated rejections, sometimes attributed to software glitches or inadequate moderator enforcement. This discrepancy between the high volume of NCMEC reports generated by Meta's systems and the reported user experience suggests potential gaps in effectively addressing all types of reported harms, particularly those beyond easily identifiable CSAM.



Platform Analysis: Snapchat

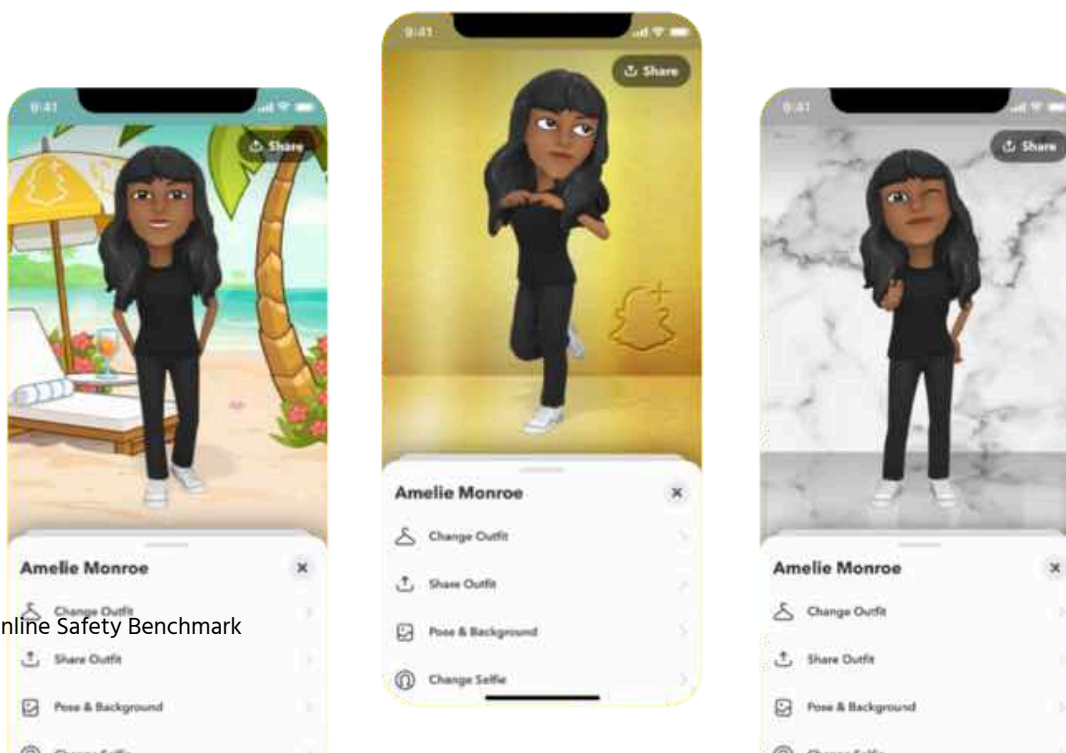
Policies & Guidelines

Snapchat's Community Guidelines articulate a strict stance against the sexual exploitation and abuse of minors. The platform explicitly prohibits sharing CSAM, grooming, sextortion (sexual extortion), and any sexualization of children. This includes a ban on posting, saving, sending, forwarding, distributing, or soliciting nude or sexually explicit content involving anyone under 18, even if self-generated. Snapchat states it has zero tolerance for severe harms, particularly CSEA, and will disable accounts engaging in such behavior. The guidelines also forbid harassment and bullying of any kind, specifically including sexual harassment like sending unwanted explicit images, as well as threats and violence. Promoting or facilitating illegal activities, including human trafficking, is also banned.

The minimum age to create a Snapchat account is 13 years old. The platform employs an age gate during registration and blocks users who indicate they are under 13. If Snapchat becomes aware of an underage account, it is terminated, and the user's data is deleted. As a safeguard against circumvention, users aged 13-17 are prevented from changing their registered birth year to 18 or older.

Enforcement measures for guideline violations include content removal and limitations on account visibility or termination. For severe offenses like CSEA, Snapchat implements immediate account disabling and takes steps to prevent the user from rejoining the platform. The platform reports identified instances of child sexual exploitation to authorities (implicitly including NCMEC, as per standard US practice) and refers information to law enforcement when activity poses an imminent threat to human life. Snapchat publishes Transparency Reports twice a year, providing data on enforcement actions, CSEA reports made to NCMEC, and governmental requests for user data.

Snapchat's stringent policies reflect industry standards, but their implementation occurs within the context of a platform known for its ephemeral messaging features. This ephemerality, while offering perceived privacy benefits to users, presents inherent challenges for detecting and investigating policy violations like grooming or harassment, as evidence may disappear by default. This dynamic may make the platform attractive to individuals seeking to evade oversight, despite Snapchat's stated policies and enforcement efforts. The platform acknowledges this tension by stating its policy of retaining data specifically for the duration of investigations when harmful content is reported, overriding the default deletion.



Platform Analysis: Snapchat

Technical Safety Measures

Snapchat utilizes a combination of automated technologies and human review to enforce its safety policies. Proactive detection relies on tools including abusive language detection systems (monitoring keywords and emojis) and multi-modal artificial intelligence/machine learning (AI/ML) classifiers. Specific safeguards are also implemented for generative AI features, such as the "My AI" chatbot, to align generated content with Community Guidelines.

For combating known CSAM, **Snapchat employs industry-standard hash-matching technologies like PhotoDNA (for images) and Google's CSAI Match (for videos)**. These tools compare uploaded content against databases of known illegal material. Snapchat also utilizes hashes from NCMEC's "Take It Down" program, which allows minors to proactively hash their own sensitive images to prevent their spread.

Beyond content matching, Snapchat uses behavioral signals to identify potentially harmful activity or accounts. Analysis of user reports, particularly concerning trends like sextortion, informs the development of these signals and subsequent enforcement actions, such as locking accounts exhibiting specific characteristics. This behavioral analysis is also used to identify potentially suspicious adult accounts that might attempt to interact with minors.

Moderation efforts are particularly focused on public content areas like Stories and Spotlight, where additional review processes are applied to prevent violating content from reaching a wide audience. However, there are conflicting reports regarding the extent of technical monitoring within private communications. One external report from Australia's eSafety Commissioner claimed Snapchat does not use technology to detect grooming and only applies tools to public content, not direct messages. Snapchat's own statements assert the use of automated tools, including AI/ML and language detection, and policies prohibit grooming, but the specific application within ephemeral, private chats remains less clear compared to their public content moderation.

The platform demonstrably leverages standard industry tools for known CSAM detection and is increasingly incorporating behavioral analysis, often triggered by user reports, into its safety systems. Nonetheless, the conflicting external assessment regarding proactive grooming detection combined with the inherent technical difficulty of scanning ephemeral private messages suggests potential vulnerabilities in proactively identifying grooming or CSEA initiation within direct chats, relying more heavily on user reporting in that context.



Platform Analysis: Snapchat

Design Features for Safety

Snapchat's design incorporates several features aimed at enhancing minor safety, primarily by limiting contact from unknown individuals. A fundamental aspect is that friend lists are private for all users by default, preventing easy discovery of a user's social circle. For direct communication (chat, snaps) to occur, users must mutually accept each other as friends, or one must have the other in their phone contacts.

Default settings for teenagers are configured for heightened privacy. **Contact settings for teens default to "Friends and Phone Contacts" only, and this cannot be broadened to allow contact from anyone on the platform.** Location sharing via Snap Map is turned off by default for all users, requiring an active opt-in. Furthermore, teens under 18 are not permitted to create Public Profiles, which allow content visibility beyond approved friends.

Discoverability of teen accounts by strangers is intentionally limited. It is difficult for a teen to appear in search results or friend suggestions for another user unless they share mutual friends or are already in the user's phone contacts. Snapchat employs enhanced friending protections to block certain suspicious friend requests targeting teens. If a teen accepts a friend request from someone potentially unknown (especially without mutual friends), the platform sends an in-app warning prompt, encouraging caution and reminding them to communicate only with trusted individuals. Additional restrictions limit contact from adult users, generally requiring mutual friends before an adult can add a teen.

Direct messages on Snapchat are ephemeral by default, disappearing after being viewed, although users have the option to save chats. As noted, communication requires mutual friendship or prior contact.

Location sharing, when enabled, offers granular controls. Users can only share their location with existing Snapchat friends; broadcasting to the wider community is not an option. "Ghost Mode" completely disables location sharing. The platform provides reminders about active location sharing settings and a centralized place to manage these preferences.

Reporting and blocking tools are designed to be easily accessible. Users can report inappropriate content (Snaps, Stories, Chats) or accounts directly within the app, and reporting is confidential. An online reporting form is also available for non-users. Blocking a user prevents all further contact and visibility. Specific reporting options exist for issues like sextortion, using language relatable to teens. Content controls, manageable via Family Center, allow parents to limit exposure to potentially sensitive material in public feeds like Stories and Spotlight.

The platform's design philosophy strongly emphasizes preventing unwanted contact, particularly for minors, through robust default privacy settings and friend-gating mechanisms. This approach seeks to create a safer space mirroring real-world friendships. However, the effectiveness of these measures is contingent upon users providing accurate age information during sign-up, and they do not inherently eliminate risks arising from interactions within established friend groups or from sophisticated actors who manage to bypass initial friending barriers.

Platform Analysis: Snapchat

Parental Controls

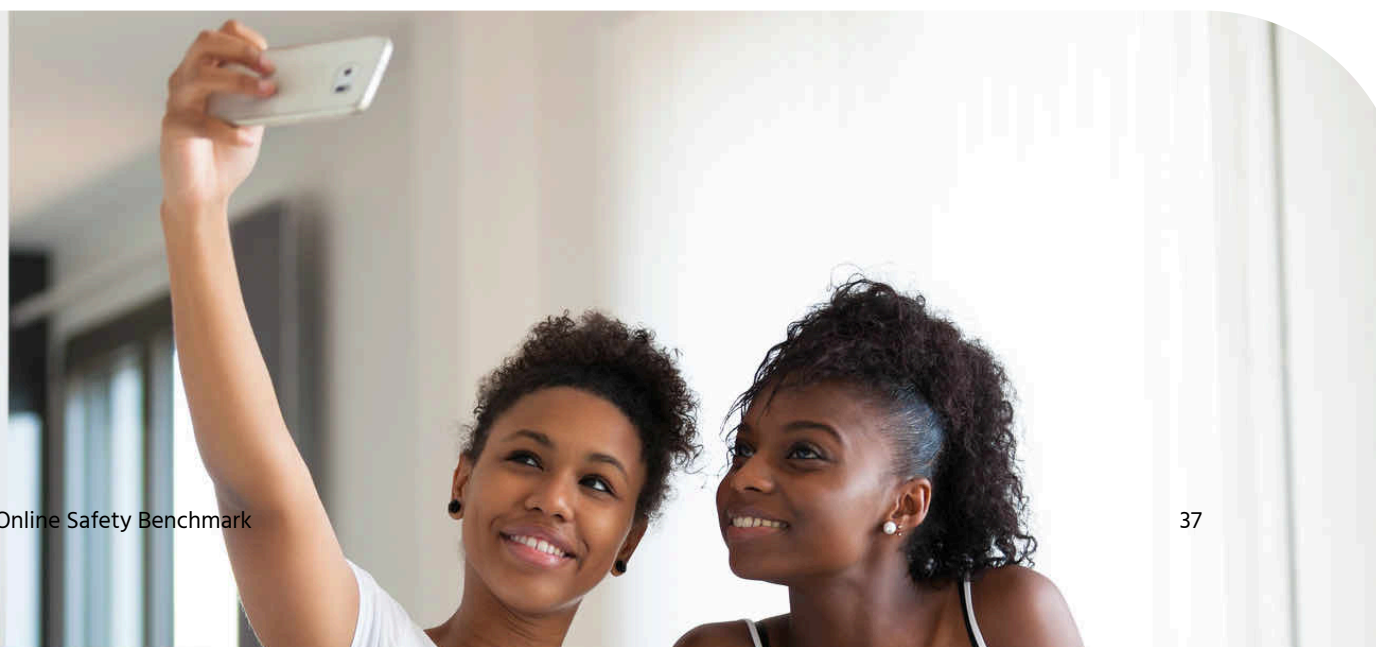
Snapchat's parental supervision tool is called "Family Center." It requires the parent (who must be over 25) and the teen (aged 13-17) to both have Snapchat accounts and mutually agree to link them through an invitation process.

The core functionality of Family Center focuses on providing parents with visibility into their teen's connections rather than direct control over all aspects of their usage. Parents can view their teen's complete friend list and see the names of accounts (individuals or groups) the teen has communicated with within the past seven days. Critically, parents cannot see the actual content of the Snaps or messages exchanged, preserving conversational privacy. Family Center also allows parents to view the teen's current privacy and safety settings and their birthday settings.

In terms of content controls, parents using Family Center can enable restrictions to filter potentially sensitive or suggestive content from appearing in the public Stories and Spotlight tabs for their teen. They can also manage parental controls related to the "My AI" chatbot, including potentially disabling its ability to respond to the teen.

Family Center includes an integrated, confidential reporting mechanism, allowing parents to easily report any accounts they find concerning directly to Snapchat's Trust & Safety team.

Unlike some other platforms' parental controls, the provided information does not indicate that Snapchat's Family Center allows parents to set specific screen time limits directly within the tool, although device-level screen time controls can be used. Similarly, while parents can view location sharing settings, direct location tracking of the teen by the parent within Family Center is not mentioned as a feature. Snapchat's approach with Family Center reflects a philosophy centered on fostering parent-teen dialogue by providing insights into social connections while deliberately respecting the privacy of conversations. It offers less direct intervention capability (like setting time limits or blocking specific users remotely) compared to TikTok's Family Pairing or Instagram's Supervision, positioning itself more as an awareness tool to facilitate offline conversations about online safety.



Platform Analysis: Snapchat


Report Handling Process

Snapchat provides multiple channels for reporting abuse, grooming, exploitation, or other safety concerns. Users can report content (Snaps, Stories, Chat messages) or profiles directly within the app using press-and-hold menus or dedicated report buttons. Non-users can submit reports via a web form. Parents linked through Family Center also have a direct reporting channel. Snapchat has implemented specific reporting options tailored for issues like sextortion, using language designed to be relatable for teens. Proactive detection systems also flag potential violations.

Reports are directed to Snapchat's global Trust & Safety team, which operates 24/7 to investigate potential violations of the Community Guidelines. The platform aims to review and take action on reports quickly, stating a goal of acting within an hour in most cases, although median turnaround times reported in transparency data may vary (~24 minutes in H1 2024).

Based on the review, **Snapchat may take various enforcement actions, including issuing warnings to users, removing the offending content, limiting the visibility of an account, or permanently banning the account.** For severe violations, particularly those involving CSEA or imminent threats, Snapchat enforces a zero-tolerance policy, leading to immediate account disabling and measures to prevent the user from creating new accounts.

Crucially, despite the default ephemeral nature of content, Snapchat explicitly states that it retains data related to reported incidents during the review process. This retention allows for investigation and is essential for cooperation with law enforcement.



Escalation to external authorities follows established protocols. Identified CSEA is reported to NCMEC. If the platform believes there is an imminent threat to human life, information is referred directly to law enforcement. Snapchat cooperates with law enforcement investigations and can provide user data when presented with valid legal process (subpoenas, court orders, search warrants under the U.S. Stored Communications Act for domestic requests; typically MLAT or letters rogatory for international requests). Data may be retained for longer periods specifically to support these investigations.

Reporting is confidential, meaning the reported user is not informed of the reporter's identity. The available information does not specify the level of feedback provided to reporters regarding the outcome of investigations into grooming or exploitation, beyond the visible enforcement actions like content removal or account disappearance.

The platform's emphasis on a rapid response team and its policy of retaining data for investigations are key operational elements designed to counteract the challenges posed by ephemeral content. The effectiveness of this process relies on users reporting incidents promptly and the platform's ability to preserve relevant data before potential automatic deletion, enabling meaningful review and potential law enforcement action.

Comparison of Platform Prohibited Content Policies

Platforms maintain extensive Community Guidelines or Standards outlining prohibited content, with specific sections often dedicated to child safety.

YouTube	TikTok	Instagram (Meta)	Snapchat
<p>Policies explicitly forbid content endangering the physical or emotional well-being of minors (defined as under 18). This includes CSAM, sexual exploitation, content depicting minors in harmful or dangerous acts (e.g., stunts, substance use, unsupervised firearm use), infliction of maltreatment or neglect (physical, sexual, or emotional), cyberbullying, and "misleading family content" (content targeting families but containing inappropriate themes like violence, sex, or horror).</p> <p>YouTube states it reports CSAM to the National Center for Missing and Exploited Children (NCMEC).</p>	<p>Adopts a zero-tolerance stance towards CSEA and CSAM, explicitly including AI-generated material.</p> <p>Policies also prohibit grooming, pedophilia, sextortion, sexual harassment of minors, and content depicting minor semi-nudity or encouraging minors to move off-platform.</p> <p>Broader guidelines cover violent behavior, hate speech, promotion of self-harm or eating disorders, dangerous challenges, and regulated goods.</p>	<p>Community Standards prohibit CSAM, sexual exploitation of minors, bullying and harassment, hate speech, graphic violence, and the glorification or encouragement of self-injury (with exceptions for awareness/support content). Offering sexual services and selling illegal items like firearms and drugs are also banned.</p> <p>Nudity is generally disallowed, with specific exceptions (e.g., breastfeeding, post-mastectomy scarring, art).</p> <p>The policy mentioned Instagram reports all apparent child pornography to the National Center for Missing and Exploited Children.</p>	<p>Community Guidelines prohibit any activity involving CSEA/CSAM, grooming, sextortion, or the sexualization of children. Sharing nude or sexually explicit content involving anyone under 18 (including self-generated images) is strictly forbidden.</p> <p>Policies also cover threats, violence (including animal abuse), hate speech, harassment, bullying, and illegal activities like selling drugs or weapons, or facilitating trafficking.</p> <p>Snapchat confirms reporting identified CSAM to authorities.</p>

Comparison of Platform Child Online Safety Measures

Synthesizing the evaluations of policies, takedown procedures, and reporting mechanisms allows for a comparative benchmarking of YouTube, TikTok, Instagram, and Snapchat across key child safety dimensions. This comparison highlights relative strengths and persistent weaknesses.

Criteria for Comparison

- **Policy Clarity & Comprehensiveness:** Assessment of how clearly, accessibly, and thoroughly the platform's rules address child safety risks (age limits, prohibited content like CSEA/grooming/bullying, harmful acts, privacy).
- **Age Verification:** Evaluation of the methods used to enforce minimum age requirements and their practical effectiveness in preventing underage access.
- **Proactive CSAM/CSEA Detection:** Assessment of the platform's investment in and use of technology (hashing, AI) to identify and remove CSEA/CSAM before user exposure or reports, including transparency around these efforts.
- **Grooming/Exploitation Prevention:** Evaluation of specific policies and technical features designed to disrupt grooming attempts and limit opportunities for exploitation, beyond general content removal.
- **Minor Privacy Controls:** Assessment of default privacy settings for minors, the granularity of user controls, data collection/use policies specific to minors, and the availability/robustness of parental supervision tools.
- **Reporting Mechanism Effectiveness:** Evaluation of the accessibility and usability of reporting tools (especially for children), platform responsiveness to reports, clarity of the reporting process, and integration with law enforcement/NCMEC.
- **Transparency:** Assessment of the availability, detail, consistency, and verifiability of public reporting regarding child safety policies, enforcement actions, takedown data, and algorithm impacts.

Feature/Policy Area	YouTube	TikTok	Instagram	Snapchat
Policy Clarity & Comp.	Clear policies on child safety, detailed examples provided.	Detailed, well-organized guidelines covering numerous risks.	Policies exist but can be fragmented across different documents (Terms, Standards).	Clear, concise guidelines covering key CSEA and minor safety issues.

Comparison of Platform Child Online Safety Measures

Feature/Policy Area	YouTube	TikTok	Instagram	Snapchat
Proactive CSAM/CSEA Detection	Employs hashing (CSAI Match) & AI; emphasizes proactive removal. Reports to NCMEC.	Employs automated systems & AI; emphasizes proactive detection. Reports to NCMEC.	Employs hashing & AI; reports vast volume to NCMEC. Effectiveness questioned by investigations into network facilitation.	Employs hashing (PhotoDNA/CSAI Match) & AI; reports proactive detection rates. Reports to NCMEC.
Grooming/Exploit. Prevention	Advises creators; may disable features on minor content. Less focus on interaction controls.	Default private accounts, DM restrictions for U16/U18. Policy explicitly prohibits grooming.	DM restrictions for unconnected adults/teens; suspicious adult detection. Algorithms criticized for potentially facilitating connections.	Emphasizes friending known people. Policy prohibits grooming/ sextortion. Ephemerality/ Discover pose risks.
Minor Privacy Controls	Google Family Link provides parental controls. Advises against sharing personal info.	Default private accounts U18; DM restrictions; Family Pairing offers significant parental controls.	Default private U16; Sensitive Content Control default; Supervision tools available. ¹⁰¹ Data use concerns remain.	Location sharing controls (Ghost Mode); Family Center offers parental insights/controls. Data use concerns remain.

Comparison of Platform Child Online Safety Measures

Feature/Policy Area	YouTube	TikTok	Instagram	Snapchat
Reporting Effectiveness	Standard reporting tools available. Responsiveness at scale is a challenge.	Standard tools with specific CSEA category. Responsiveness at scale is a challenge.	Standard tools; allows teen notification to parent. Responsiveness questioned (e.g., ignored reports).	In-app & webform reporting. Claims fast response for some reports, but reactive CSAM slower.
Transparency	Publishes reports including CSAM data. Detail/consistency can vary.	Publishes reports including CSEA data. Detail/consistency can vary.	Publishes reports, but faces criticism for lack of detail, consistency, and algorithmic transparency.	Publishes regular reports with enforcement data by category, including CSAM.
Age Verification	Relies mainly on self-attestation; ineffective in preventing underage use.	Relies mainly on self-attestation; US U13 curated experience exists. Stronger default settings for teens. ¹	Relies mainly on self-attestation; some verification attempts (ID/selfie) but effectiveness unclear.	Relies mainly on self-attestation; ineffective in preventing underage use.

Comparison of Platform Child Online Safety Measures

Overall Assessment

No single platform emerges as unequivocally superior across all dimensions of child safety.

- **TikTok** demonstrates relatively strong proactive measures in terms of default settings for minors (private accounts, DM restrictions) and offers robust parental controls through Family Pairing. Its guidelines are also notably detailed. However, it faces significant challenges related to harmful trends/challenges, addictive design, and content moderation at scale.
- **YouTube**, as the largest video platform, faces immense scale challenges but emphasizes technological solutions for proactive removal. Its policies are relatively clear, but age verification remains weak, and risks associated with recommended content and misleading family content persist.
- **Instagram** has implemented some positive changes (default private for younger teens, DM restrictions), but faces severe criticism regarding its algorithmic amplification of harmful content and networks, raising fundamental questions about its design priorities. Its high volume of CSAM reports to NCMEC contrasts with investigative findings about facilitation.
- **Snapchat** provides clear policies and utilizes proactive detection technology. Its Family Center offers parental tools. However, risks associated with its core features (ephemerality, Discover, Snap Map) and high reported rates of cyberbullying remain significant concerns. Transparency data suggests potential delays in responding to user-reported CSAM compared to proactively detected material.

All platforms struggle with effective age verification, the nuances of content moderation at scale (balancing accuracy, speed, and context), ensuring transparency, and adapting to new threats like generative AI and risks within encrypted environments. The gap between stated policies and practical enforcement or user experience remains a critical issue across the board.

"Digital technology is promising. It can bring rapid progress to humanity, but if it is not well-monitored and well-managed, it can also cause harm to all aspects of social life, especially it can destroy morality, psychology, and character of our children."

Prabowo Subianto, President of the Republic of Indonesia

President Prabowo Subianto issues the Government Regulation on Governance for Electronic System Providers in Child Protection, during an event held at the Merdeka Palace, Jakarta, Friday (03/28).



Internet Users by Country

early
2025



Indonesia

212 million



**The
Philippines**

97.5 million



Ghana

24.3 million



Rwanda

4.93 million



**Dominican
Republic**

10.2 million

Source: DATAREPORTAL, 2025

Digital Landscape

Country Overview

Indonesia, an expansive archipelago with a burgeoning youth population, has witnessed a significant surge in internet adoption among its younger citizens. As of early 2025, the nation recorded 212 million internet users, representing an internet penetration rate of 74.6%. Notably, a 2024 survey revealed that 48% of children under the age of 12 access the internet, with usage among Gen Z (ages 12–27) reaching a staggering 87%.⁵⁵ This digital immersion, while fostering connectivity and learning, has inadvertently exposed children to a spectrum of online vulnerabilities.

In 2024, Indonesia reported 15,914 cases of violence against children, with over 9,000 instances involving sexual violence.⁵⁶ The proliferation of social media platforms has further complicated the landscape, with a significant number of children engaging actively online. Recognizing these challenges, the Indonesian Ministry of Women's Empowerment and Child Protection announced plans to establish a specialized team dedicated to addressing digital child exploitation and abuse.⁵⁷

The Philippines stands out with its deep-rooted engagement in the digital sphere. As of early 2025, the nation boasted 97.5 million internet users, accounting for 83.8% of its population.⁵⁸ This extensive connectivity, while advantageous, has also rendered Filipino children susceptible to online sexual abuse and exploitation. A distressing report from 2021 highlighted that approximately two million children were subjected to such exploitation, encompassing grooming and coercion into explicit activities.

In response to these alarming trends, collaborative efforts between the Australian Federal Police and the Philippine National Police have been instrumental in rescuing victims and apprehending perpetrators. Notably, operations in 2024 led to the rescue of children as young as two from exploitative situations.⁵⁹ Furthermore, organizations like SaferKidsPH have been at the forefront, advocating for robust systemic measures to combat online child exploitation.

Ghana's digital evolution has been marked by a commendable increase in internet accessibility among its youth. Studies reveal that 90.5% of Ghanaian children aged 8 to 17 have ventured online, leveraging the internet for educational and social pursuits.⁶⁰ However, this digital enthusiasm is tempered by challenges such as cyberbullying, online grooming, and exposure to inappropriate content.

To address these concerns, UNICEF Ghana has been proactive in formulating a National Plan of Action aimed at curbing online child sexual exploitation and abuse. This initiative emphasizes collaboration with the National Cybersecurity Crime Centre to seamlessly integrate child protection protocols into the broader national cybersecurity framework.

55. Data Reportal Indonesia <<https://datareportal.com/reports/digital-2024-global-overview-report/indonesia>>, accessed 1 March 2025.

56. Ministry of Women's Empowerment and Child Protection, <<https://kekerasan.kemenpppa.go.id/>>, accessed 1 March 2025.

57. Peta Jalan Perlindungan Anak Indonesia di Internet, Ministry of Communication and Information Technology of the Republic of Indonesia, Indonesian Child Protection Commission, UNICEF Indonesia, Center for Communication Studies, University of Indonesia, Indonesia Child Online Protection and Indonesia Internet Governance Forum, <<https://lms.onnocenter.or.id/pustaka/docs/ICT4VILLAGES/InternetSehat/peta%20jalan%20perlindungan%20anak%20di%20internet%20indonesia.pdf>>, accessed 3 February 2025.

58. Philippine Institute for Development Studies, <<https://www.pids.gov.ph/details/news/in-the-news/accessibility-a-big-part-of-customer-strategy>>, accessed 10 January 2025.

59. Australian Federal Police, <<https://www.afp.gov.au/news-centre/media-release/international-cooperation-leads-92-children-removed-harm-2023>>, accessed 10 January 2025.

60. Child abuse and the internet, Janet Stanley, <https://www.researchgate.net/publication/242085433_Child_Abuse_and_the_Internet>, accessed 1 March 2025. 13. UNICEF Ghana, <<https://safeonline.global/unicef-ghana/>>, accessed 1 March 2025.

Digital Landscape

Country Overview

Rwanda's commitment to technological advancement is evident in its increasing internet penetration, which stood at 34.2% in early 2025.⁶¹ While this growth heralds numerous opportunities, it also necessitates a focus on digital literacy and safety, especially for the younger demographic.

The Rwanda Education Board's 2023 report highlighted that over 70% of urban households possess digital devices. However, only 45% of parents actively engage in their children's online educational activities, underscoring a gap in digital supervision.⁶² In response, the Rwandan government, in collaboration with organizations like 5Rights Foundation, has been instrumental in developing and implementing Child Online Protection policies.

The **Dominican Republic**, with its vibrant culture and growing economy, has seen a steady rise in internet adoption. As of early 2025, there were 10.2 million internet users, representing an internet penetration rate of 88.6%.⁶³ This digital expansion, while promising, brings to the fore concerns about online safety for children.

Collaborative endeavors between UNICEF Dominican Republic and Plan International have culminated in the establishment of a national response board.⁶⁴ This body is tasked with orchestrating initiatives aimed at preventing and addressing online sexual exploitation and abuse, reflecting a national commitment to safeguarding its younger citizens in the digital realm.

In Indonesia, the rapid digital uptake among children—often through mobile-first access—has outpaced both parental literacy and institutional safeguards. This digital enthusiasm is a powerful force for education and empowerment, but without adequate protection, it leaves children vulnerable to exploitation and harm.

At Bullyid App, we've witnessed firsthand the growing need for responsive support systems, particularly in urban centers where online grooming, sextortion, and non-consensual content sharing are increasingly reported.

Agita Pasaribu, Executive Director at Bullyid App



61. Data Reportal Rwanda, <https://datareportal.com/reports/digital-2024-uganda>, accessed 10 February 2025

62. Rwanda Basic Education Board, <https://www.reb.gov.rw/publications>, accessed 10 February 2025.

63. Data Reportal Dominican Republic, <https://datareportal.com/digital-in-the-dominican-republic>, accessed 15 February 2025.

64. Safe Online, <https://safeonline.global/unicef-dominican-republic-plan-international-dominican-republic/>, accessed 15 February 2025.

Legislation & Policy Frameworks



Indonesia

Legal Definitions of ‘Child’ in Indonesia

In the context of Indonesia’s evolving digital landscape, one of the foundational components in safeguarding children from online risks is the legal definition of who a “child” is. This may appear to be a straightforward issue; however, Indonesia’s complex statutory framework reveals inconsistencies and overlapping interpretations of age thresholds across various sectors of law.

The definition of a “child” is pivotal because it determines the scope of legal protections, the jurisdiction of juvenile justice systems, and the eligibility of rights and remedies within child protection mechanisms—including those that apply in the digital world.

Indonesia does not adopt a single, uniform definition of a child across all its legislation. Instead, different laws and codes define the term in varying ways, sometimes with overlapping or conflicting thresholds. This legal fragmentation creates potential gaps in protection, enforcement, and clarity, particularly when it comes to issues of online child sexual exploitation and abuse (OCSEA), digital consent, grooming, and exposure to harmful content.

Implications for Online Child Protection

The lack of a unified legal definition of “child” has practical implications. It introduces legal uncertainty in determining:

- When children can lawfully consent to digital terms of service,
- Whether adolescents between 17 and 21 receive child-specific protections,
- How digital grooming or exploitation should be prosecuted when different age benchmarks are involved.

These inconsistencies create interpretative challenges in prosecuting online offenses, particularly when dealing with cross-border cases or platforms requiring clarity about the legal status of a user. The reliance on general provisions such as sexual exploitation or electronic-based harassment can be problematic in practice, especially when law enforcement lacks sufficient digital forensic expertise or legal literacy regarding evolving online harms. Without explicit recognition, many acts of sextortion risk being misclassified under lesser offenses, thereby failing to capture the full extent of trauma inflicted on the child victim.

The future of online child safety depends not solely on the punitive framework, but on the clarity, accessibility, and adaptability of the law to address threats that are increasingly complex, cross-jurisdictional, and technologically sophisticated.

Indonesia

Age-Based Definitions Across National Laws

Law / Regulation	Article	Definition of Child	Age Limit	Notes
Law No. 4 of 1979 on Child Welfare	Art. 1(2)	A person who has not reached the age of 21 and has never married	21	Applies only if unmarried; earliest statutory reference
Law No. 39 of 1999 on Human Rights	Art. 1(5)	Any human under 18 years and unmarried; includes unborn children if in their best interest	18	Recognizes child in womb when in their best interest
Law No. 23 of 2002 on Child Protection (as amended by Law No. 35/2014, No. 17/2016)	Art. 1(1)	A person who hasn't reached 18, including unborn children	18	Core child protection legislation
Law No. 44 of 2008 on Pornography	Art. 1(4)	A person who has not reached 18 years	18	Used for defining child pornography/CSAM
Law No. 11 of 2012 on Juvenile Justice System (SPPA Law)	Art. 1(3), (4), (5)	Child in conflict with law: 12–18 years Child victim/witness: Under 18	12-18	Introduces role-based differentiation (e.g., victim, witness)
Law No. 12 of 2022 on Sexual Violence Crimes (UU TPKS)	Art. 1(5)	A person who hasn't reached 18, including unborn children	18	Covers children in sexual violence cases, aligns with Child Protection Law

Indonesia

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses

Building on the foundational definition of a “child” within Indonesia’s statutory framework, it is essential to explore how the Indonesian legal system recognizes, defines, and penalizes behaviors that fall under child sexual exploitation (CSE) and sexually explicit conduct, particularly in relation to online safety. These categories include acts such as grooming, sextortion, and the production or dissemination of child sexual abuse material (CSAM).

Indonesia’s criminal legal framework does not yet provide detailed provisions specifically addressing the protection of children from online sexual crimes. Neither the Child Protection Law, the Pornography Law, nor the Electronic Information and Transactions Law contains explicit clauses that criminalize or sanction online sexual offenses involving minors. This absence creates a normative vacuum or ambiguity, opening legal loopholes in prosecuting increasingly complex and technology-driven offenses.

As online sexual crimes evolve rapidly in the digital age, relying solely on traditional interpretations of existing laws may no longer be sufficient. While general criminal provisions offer some protective scope, proactive legal reform is critical. Updating and strengthening Indonesia’s criminal legislation to clearly define and address online sexual exploitation of children is essential—not only to close legal gaps but to ensure that justice is accessible and enforceable. Strengthened legal language would also prevent perpetrators from exploiting the principle of legality to evade accountability due to technicalities or legislative silence.



In Indonesia, the offenses outlined in **Law No. 35 of 2014 on Child Protection include sexual violence against children (Article 76C)**, violence or the threat of violence that forces a child to engage in sexual intercourse (Article 76D), violence or the threat of violence, coercion, deception, manipulation, or persuasion of a child to engage in or tolerate indecent acts (Article 76E), and the economic or sexual exploitation of children (Article 76I).



Indonesia’s legislation on online sexual exploitation of children comprises only two articles under Law No. 19 of 2016 in conjunction with Law No. 11 of 2008 on Electronic Information and Transactions. Article 27 paragraph (1) criminalizes the distribution, transmission, and provision of access to electronic information that violates morality, while Article 52 paragraph (1) specifically stipulates that the penalty is increased by one-third if the offense under Article 27 paragraph (1) is committed against a child. Moreover, the pornography law in Indonesia has overly broad provisions and lacks specific regulations for cases involving children as its victim.

The offenses contained in the Indonesian Pornography Law are still too broad, as there are no specific offenses for sexual crimes against children, and no provision for online sexual crimes against children.

In March 2025, the Indonesian government introduced **Peraturan Pemerintah (PP) Nomor 17 Tahun 2025**

a landmark regulation that for the first time explicitly addresses child online protection at the national level.

Commonly referred to as **PP Tunas**, the regulation outlines legal obligations for Electronic Service Providers (ESPs) to safeguard children’s data, privacy, and well-being in the digital space. It introduces a seven-tier risk classification framework for ESPs, based on self-assessed criteria, and imposes specific prohibitions and duties aimed at preventing online sexual exploitation of children.

Indonesia

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses

Child Sexual Exploitation (CSE)



Indonesia's Child Protection Law (Law No. 23 of 2002, as amended) provides a key statutory basis for addressing sexual exploitation. According to Article 66, child sexual exploitation is defined as: "Any form of exploitation of a child's sexual or other organs for profit, including but not limited to prostitution and sexual abuse."

This language links exploitation directly to transactional intent—emphasizing acts where a child's sexual integrity is violated in return for money, benefits, or coercive gains. However, it is important to note that this definition does not always capture non-commercial sexual abuse, grooming, or digital coercion. Nevertheless, Article 76I criminalizes sexual exploitation and Article 88 provides punishment up to 10 years in prison and/or IDR 200 million in fines.

The Sexual Violence Crimes Law (Law No. 12 of 2022) further extends the protection. It includes acts such as forced sexual exploitation, forced prostitution, and electronic-based sexual violence (see: Articles 4(1)–(2)). It reframes CSE from being merely transactional to including abuse through deception, coercion, or manipulation—essential in a digital age where such acts may occur online without money exchanged.

Sexually Explicit Conduct

While Indonesia's statutes do not contain a standalone legal definition for "sexually explicit conduct," related concepts are articulated primarily through the **Pornography Law (Law No. 44 of 2008)** and certain provisions in the Indonesian Penal Code (KUHP).



The Pornography Law defines pornography broadly under Article 1 as: "Images, sketches, illustrations, photos, texts, sounds, videos, animations, cartoons, conversations, gestures, or other forms of messages via communication media and/or public performance, which contain obscenity or sexual exploitation that violate public decency norms."

"PP Tunas marks an important first step by the Indonesian government, but the process lacked transparency and meaningful civil society involvement.

While it regulates crucial issues like data privacy and ESP obligations, it doesn't explicitly mention children involved in online child sexual offenses.
The regulation's reliance solely on ESPs for child protection is insufficient.

A more coordinated response involving multiple ministries and clear implementation guidelines is needed. We urge the government to swiftly follow up with a Presidential Regulation on the Child Online Protection Roadmap to ensure effective, multi-stakeholder enforcement."

Andy Ardian, National Coordinator of ECPAT Indonesia



Indonesia

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses

The **Sexual Violence Crimes Law** provides a detailed list of acts that qualify as sexual violence. **Article 4(1)** lists:

- Non-physical and physical sexual harassment,
- Forced contraception and sterilization,
- Sexual slavery and exploitation,
- Electronic-based sexual violence,
- Child marriage and abuse.



In addition, Article 4(2) includes rape, lewd acts, and sexual intercourse or obscene acts against children.

Furthermore, Article 76I and 76J of the **Child Protection Law**, along with Article 81 and 82, address offenses related to coercion or trickery used to obtain sexual access to a child, with imprisonment up to 15 years depending on aggravating factors.

Child Sexual Abuse Material (CSAM)

Indonesia defines CSAM under **Article 4(1)(f) of the Pornography Law** as:



“Any form of pornography involving children or involving adults who act or behave like children.”

This inclusion of “adults who act or behave like children” potentially allows for the prosecution of digitally morphed or role-play CSAM, though enforcement remains rare. There are also aggravating penalties if CSAM is distributed, with sentences reaching up to 12 years and fines of IDR 6 billion, with 1/3 added if children are involved.

Computer-Generated CSAM / AI-Based Abuse

While no law explicitly refers to AI-generated or computer-simulated CSAM, the **EIT Law (Law No. 11 of 2008) and its 2024 amendment** are relevant. According to:



- Article 1(1): “Electronic Information” includes text, images, maps, audio, etc.
- Article 1(4): “Electronic Document” includes digital, electromagnetic, optical formats that may be seen or heard through electronic systems.

These definitions are broad enough to encompass deepfake and AI-generated abuse material, even if the term “AI” is not directly mentioned.

Indonesia

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses

Grooming and Enticement

Grooming or online enticement of children is not yet explicitly codified under a single offense. However, several overlapping articles provide prosecutorial pathways:



- **Article 76E of the Child Protection Law** prohibits forcing or inducing a child into obscene acts.
- **Article 417 of the New Criminal Code (Law No. 1 of 2023), effective January 2026⁶⁵**, criminalizes offering gifts or abuse of power to mislead a child into committing or allowing obscene acts (punishable by 9 years).
- **Article 422** addresses those who move, bring, or deliver a child to another person to engage in obscenity or prostitution (9–10 years imprisonment depending on circumstances).

Sextortion

Sextortion, as codified in international legal standards such as the U.S. Missing Children's Assistance Act of 2023⁶⁶, is not specifically articulated in Indonesian law. Yet, the phenomenon is increasingly prevalent, as minors face coercion from predators leveraging recorded images, screenshots, or conversations for material or sexual gain.

Despite its omission in nomenclature, Sextortion is prosecutable under the umbrella of:

- Sexual exploitation,
- Sexual violence through digital means, and
- Economic exploitation of children, if aligned with threats or coercion.

The clearest pathway to prosecuting sextortion lies in **Article 14 of Law No. 12/2022**, which directly criminalizes electronic-based sexual violence. It provides the following stipulations:

Article 14(1)

Any person who, without right:



- (a) Records or takes screenshots of sexual content against the subject's will or without their consent;
- (b) Transmits electronic information (photos, messages, videos) that are sexually charged and go against the recipient's will;
- (c) Tracks or stalks individuals using electronic means for the purpose of sexual exploitation; shall be punished with a maximum of 4 years' imprisonment and/or a fine up to IDR 200 million.

65. International Parental Child Abduction, <<https://travel.state.gov/content/travel/en/International-Parental-Child-Abduction/International-Parental-Child-Abduction-Country-Information/Indonesia.html>>, accessed 10 February 2025

66. Missing Children's Assistance Reauthorization Act of 2023, <<https://www.congress.gov/bills/118th-congress/senate-bill/2051#:~:text=Missing%20Children's%20Assistance%20Reauthorization%20Act%20of%202023,-This%20act%20reauthorizes&text=Specifically%2C%20the%20act%20revises%20certain,with%20child%20sexual%20abuse%20material.>>>, accessed 10 February 2025

Indonesia

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses



Article 14(2) escalates the punishment if such actions are carried out:



- (a) To commit extortion, threat, or force; or
- (b) To mislead, deceive, or manipulate a person into acting or refraining from acting; such offenses carry a maximum sentence of 6 years and/or a fine of IDR 300 million.

These provisions implicitly cover sextortion, particularly when a child is manipulated into creating or sharing sexually explicit material through psychological coercion or threats of exposure.

Further supporting interpretation is **Article 66 of the Child Protection Law**, which identifies economically exploited children as those who are victims of extortion, slavery, oppression, or the use of their power or body for the gain of others. This broad language enables prosecutors and legal advocates to classify sextortion—particularly when money, cryptocurrency, gifts, or sexual favors are demanded under threat—as part of broader sexual or economic exploitation.

In this context, Article 76I of the same law reinforces that:



“Every person is prohibited from placing, allowing, committing, ordering to commit, or participating in the economic and/or sexual exploitation of children.”

This reflects a legal acknowledgment that **manipulation for gain (economic or otherwise) through sexual threats constitutes a criminal offense, even when the law does not name the act “sextortion.”**

Indonesia’s legal framework provides substantial, if indirect, coverage of sextortion-related acts, particularly through the combination of the Sexual Violence Crimes Law, Child Protection Law, and electronic surveillance provisions under the EIT Law. However, the country is yet to enact a targeted definition or charge for sextortion—an omission that may result in underreporting and inconsistent prosecution. As the digital lives of children continue to expand, the formal recognition and legal categorization of sextortion will be vital to shielding young users from exploitative digital coercion.



Philippines

Legal Definitions of ‘Child’ in the Philippines

In the Philippines, the legal protection of children is rooted in a deep commitment to human rights, bolstered by comprehensive statutory instruments that have evolved alongside international standards. The Philippines was the first country in Asia to ratify the United Nations Convention on the Rights of the Child (UNCRC) in 1990 and has since developed a layered, child-sensitive legal framework. This commitment is reflected not only in traditional welfare legislation but also in progressive measures addressing technology-facilitated exploitation and abuse.

In the Philippines, the term “child” is generally defined as a person below the age of eighteen (18) years.

This age threshold is used consistently across major laws, including the Family Code, Special Protection of Children Against Abuse, Exploitation and Discrimination Act (Republic Act No. 7610), the Anti-Child Pornography Act of 2009 (Republic Act No. 9775), and the most recent Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Child Sexual Abuse or Exploitation Materials (CSAEM) Act of 2022 (Republic Act No. 11930). These consistent definitions provide clarity in jurisprudence and implementation—especially in digital crimes, where verifying a victim’s age is essential to qualify an offense as involving a child.

Yet despite this coherence in statutory language, practical gaps remain. For example, while the age of majority is universally set at 18, certain digital platforms permit access at younger ages—allowing children to navigate environments where legal protections may be weakened or enforcement is unclear. Further complicating the issue is the increased use of synthetic images, online anonymity, and AI-generated CSAM, which makes identifying the victim’s age—let alone verifying consent—especially complex in digital crimes.

Equally important is the intersection between age of consent and child victimhood. **In 2022, the Philippines passed Republic Act No. 11648, raising the age of sexual consent from 12 to 16.** This shift was monumental—it closed a long-standing legal loophole that allowed abusers to evade conviction by claiming the child’s “consent.” In online spaces where grooming, sextortion, and manipulation often blur traditional boundaries of consent, the new age threshold strengthens prosecutorial reach. Under this reform, any sexual activity involving children under 16 is presumed coercive and therefore illegal, with additional protections for those aged 16 to 18 when power differentials or deception are involved.

The legal recognition of a child as a person below 18 is thus more than a categorical label. It is the legal key that unlocks protections under specialized courts, access to child-sensitive reporting procedures, eligibility for psychosocial support, and the ability to classify digital content as child sexual abuse material (CSAM).

Therefore, in the Philippines, the definition of “child” operates not only as a threshold of protection but as a gatekeeper for justice. As the digital environment continues to evolve—with increasing risks tied to real-time streaming, online grooming, and AI-based image manipulation—the legal system’s ability to uphold the rights of children will depend, fundamentally, on maintaining clarity, consistency, and adaptability in how the term “child” is understood, applied, and enforced across all digital domains.



Philippines

Age-Based Definitions Across National Laws



Law / Regulation	Article	Definition of Child	Age Limit	Notes
Republic Act No. 7610 - Special Protection of Children Against Abuse, Exploitation and Discrimination Act (1992)	Sec. 3(a)	A person below 18 years of age, or one over 18 who is unable to fully care for or protect themselves due to disability	18	Core child protection statute; includes vulnerable over-18s with disabilities
Republic Act 2 No. 9775 - Anti-Child Pornography Act of 2009	Sec. 3(a)	A person below 18 years of age	18	Definition used to prosecute CSAM and related digital crimes
Republic Act No. 9344 - Juvenile Justice and Welfare Act of 2006 (as amended by R.A. No. 10630)	Sec. 3	A child is a person under 18 years of age	18	Also defines children in conflict with the law and children at risk
Republic Act No. 11930 - Anti-OSAEC and CSAEM Act of 2022	Sec. 3(a)	Refers to a person below 18 years of age	18	Republic Act No. 11930 - Section 3(a) defines "child" as "a person below eighteen (18) years of age."
Republic Act No. 11648 - An Act Raising the Age of Sexual Consent (2022)	Sec. 1	Raises age of consent to 16; persons under 16 are presumed incapable of consent to sexual activity	16-18	Republic Act No. 11648 - Section 1 amends Article 263-A of the Revised Penal Code, effectively raising the age of sexual consent to 16.

Philippines

Age-Based Definitions Across National Laws

Law / Regulation	Article	Definition of Child	Age Limit	Notes
Family Code of the Philippines (Executive Order No. 209, s. 1987)	Art. 234	Parental authority applies until 18 years of age	18	Family Code of the Philippines - Article 234 states "Parental authority over the persons and property of unemancipated children shall belong to the parents." Emancipation typically occurs at 18.
Republic Act No. 11188 - Special Protection of Children in Situations of Armed Conflict (2018)	Sec. 5	Defines child as a person under 18 years of age	18	Republic Act No. 11188 - Section 5 defines child as a person below 18 years old or a person above that age but unable to fully take care or protect one's self due to physical or mental disability.

"We must continue working together to address the many challenges affecting children in the digital era, including online sexual abuse and teenage pregnancies. Our joint efforts are crucial in ensuring the protection, development and welfare of our children.roy morality, psychology, and character of our children."

Undersecretary Angelo M. Tapales, Executive DirectorCouncil for the Welfare of Children (CWC)

2025 Safer Internet Day Philippines, Manila



Philippines

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses



In Southeast Asia, the Philippines is an active partner of UNICEF and ASEAN in preventing online sexual crimes against minors. The Philippines has developed a comprehensive law to address sexual crimes against minors committed both online and offline. The Philippines has met the standards of the Child Pornography Law. The Anti-Child Pornography Act of 2009, which was recently revised to become REPUBLIC ACT NO. 11930, July 30, 2022, includes definitions of grooming, online grooming (luring), further regulations on the prohibition of internet and website use for child pornography, criminal sanctions for grooming and online grooming offenders, online broadcasting offenders, child pornography syndicates, and others.

The Philippines also specifically regulates witness protection in Republic Act No. 6981, "The Witness Protection, Security and Benefit Act," and compensation for child victims of pornography in Section 3(d) of Republic Act No. 7309, "An Act Creating a Board of Claims under the Department of Justice for Victims of Unjust Imprisonment or Detention and Victims of Violent Crimes and for Other Purposes." These efforts are in alignment with international commitments, including the UN CRC Optional Protocol on the Sale of Children, Child Prostitution, and Child Pornography.⁶⁷

- Republic Act No. 7610: **Special Protection of Children Against Abuse, Exploitation, and Discrimination Act**
- Republic Act No. 9775: **Anti-Child Pornography Act of 2009**
- Republic Act No. 11930: **Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act of 2022**
- Republic Act No. 10175: **Cybercrime Prevention Act of 2012**
- Republic Act No. 9995: **Anti-Photo and Video Voyeurism Act of 2009**

Child Sexual Exploitation (CSE)

Child sexual exploitation is addressed under several provisions, with **Republic Act No. 7610** providing foundational definitions. Under Article IV, Section 5(a):



"Children... who for money, profit, or any other consideration or due to the coercion or influence of any adult... indulge in sexual intercourse or lascivious conduct are deemed to be children exploited in prostitution and other sexual abuse."

The law also targets exploitative content creation and dissemination. Section 9(a) criminalizes:



"Any person who shall employ, use, persuade, induce, or coerce a child to perform in obscene exhibitions and indecent shows... or to sell or distribute the said materials."

67. Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, <<https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child>>, accessed 10 February 2025.

Philippines

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses



These provisions are strengthened under **RA 11930, particularly Section 3(d)**, refers to any of the following acts even if consent appears to have been granted by the child:

- (1) Child sexual abuse with consideration whether monetary or nonmonetary consideration, favor, or benefit in exchange for the opportunity to perform such abusive or exploitative act
- (2) Actual sexual intercourse with a child or children with or without consideration;
- (3) Employing fraud, machination, undue influence, intimidation, threat or deception by any person to commit sexual abuse of or sexual intercourse with a child or children; or
- (4) Any other similar or analogous acts related to child abuse, cruelty or exploitation or to be responsible for other conditions prejudicial to the development of the child;

The criminal law policy in the Philippines towards online sexual crimes against children includes:⁶⁸



Responsible for coordinating, monitoring, and overseeing the implementation of the Anti-Child Pornography Act of 2009, the Inter-Agency Council Against Child Pornography has been established in the Philippines. In addition to the development of UNICEF-supported National Response Plan to Address Online Sexual Exploitation and Abuse 20162022-, **the council generates a yearly report outlining the actions undertaken to enforce the Anti-Child Pornography Act.**



National Representatives in the Philippines are required to formulate an action plan based on research. The National Response Plan incorporated three studies that investigated various aspects of violence against children and the children's online experiences, including online child sexual exploitation and abuse. The findings from these studies were implemented and utilized by the Philippine government in the formulation of the National Response Plan aimed at mitigating cases of Online Child Exploitation and Abuse of Children.

68. United Nations Children's Fund (2021) Ending online child sexual exploitation and abuse: Lessons learned and promising practices in low- and middle-income countries, UNICEF, New York.

Philippines

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses



Sexually Explicit Conduct



The concept of sexually explicit conduct, particularly concerning children, is primarily defined within **Republic Act No. 9775 (Anti-Child Pornography Act of 2009)**. **Section 3(c)** of this Act defines it as an act that includes actual or simulated;

(1) As to form:

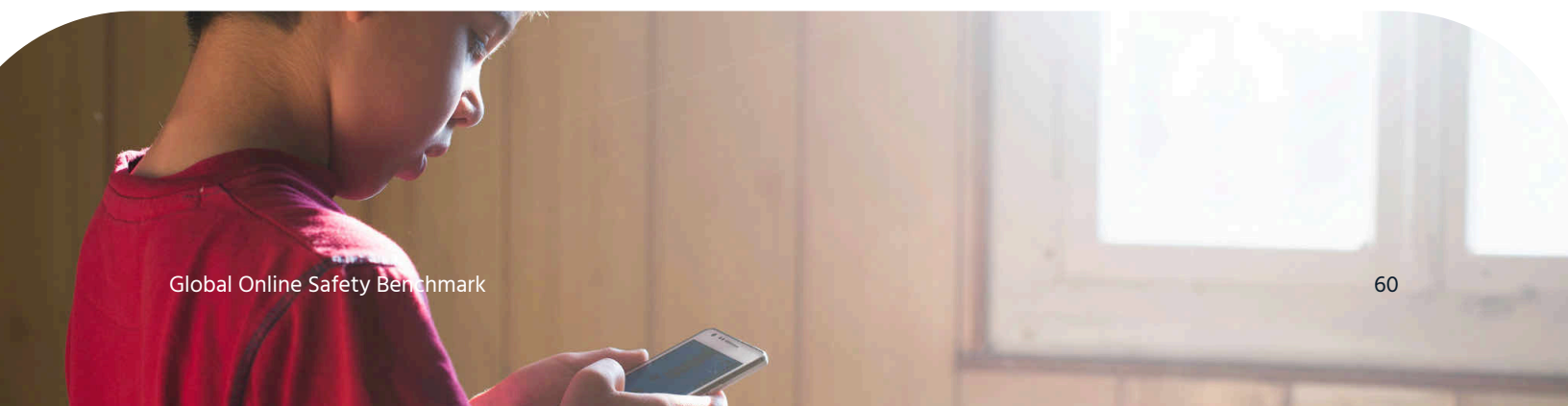
- (i) sexual intercourse or lascivious act including, but not limited to, contact involving genital to genital, oral to genital, anal to genital, or oral to anal, whether between persons of the same or opposite sex;
- (2) bestiality;
- (3) masturbation;
- (4) sadistic or masochistic abuse;
- (5) lascivious exhibition of the genitals, buttocks, breasts, pubic area and/or anus; or
- (6) use of any object or instrument for lascivious acts

This definition, while foundational, has been expanded and clarified by subsequent legislation, most notably Republic Act No. 11930 (Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Child Sexual Abuse or Exploitation Materials (CSAEM) Act of 2022). **R.A. 11930 significantly expands the scope of "sexually explicit conduct" to include digitally created and manipulated content, recognizing the dangers of AI-generated CSAM and other forms of online exploitation.**



R. A. 11930 Section 4 emphasizes regardless of the consent of the child, it shall be unlawful for any person to commit the following acts through online or offline means or a combination of both:

- (a) To hire, employ, use, persuade, induce, extort, engage, or coerce a child to perform or participate in whatever way in the creation or production of any form of OSAEC and CSAEM;
- (b) To produce, direct, manufacture, facilitate, or create any form of CSAEM, or participate in the production, direction, manufacture, facilitation or creation of the same;
- (c) To offer, sell, distribute, advertise, promote, export, or import, by any means, any form of CSAEM;
- (d) To knowingly publish, transmit and broadcast, by any means, any form of CSAEM;



Philippines

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses



Child Sexual Abuse Material (CSAM)/Computer-Generated

The Philippines has taken significant steps to address the issue of Child Sexual Abuse Material (CSAM). **Republic Act No. 9775 (Anti-Child Pornography Act of 2009), Section 3(b)**, defines **child pornography, which is a key component of CSAM**, as:



"Any representation, whether moving or still, live or recorded, or any reproduction, copy, imitation, or simulation thereof, of a child engaged in or involved in real or simulated explicit sexual activities."

This includes:

- **Digitally manipulated images, including cartoons or deepfakes,**
- **Computer-generated depictions where a person is made to appear as a child.**

Republic Act No. 10175 – Cybercrime Prevention Act of 2012, also define Child Pornography as the unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, committed through a computer system: Provided, That the penalty to be imposed shall be (1) one degree higher than that provided for in Republic Act No. 9775.

The Cybercrime Prevention Act also include **Cybersex** definition as:



"The willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration."

Republic Act No. 11930 (Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Child Sexual Abuse or Exploitation Materials (CSAEM) Act of 2022), Section 3(f), introduces and defines the term CSAEM, aligning with international terminology, and expands the scope to include:



"Any representation, whether moving or still, live or recorded, or any reproduction, copy, imitation, or simulation thereof, of a child, including digitally altered or generated images, engaged in or involved in real or simulated explicit sexual activities."



Philippines

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses



Grooming and Enticement

Grooming and enticement are comprehensively addressed in **Republic Act No. 9775**, and expanded upon in RA 11930, focusing on online luring and preparatory acts.



RA 9775 – Section 3(h):

“Grooming refers to the act of preparing a child or someone who the offender believes to be a child for sexual activity or sexual relationship by communicating any form of child pornography. It includes online enticement or enticement through any other means”



RA 11930 – Section 3(i) broadens the scope:

“Grooming refers to predatory conduct, act, or pattern of acts, of establishing a relationship of trust, or emotional connection by another, with a child or someone who is believed to be a child, and/or the family, guardian, and/or caregivers, whether in person or via electronic and other similar devices, for the purpose of perpetrating sexual abuse or exploitation or the production of any form of CSAEM.”



RA 11930 also criminalizes:

- To sexualize children by presenting them as objects of sexual fantasy, or making them conversational subjects of sexual fantasies, in any online or digital platform;
- Act of communicating, by means of a computer system, with a child or someone who the offender believes to be a child for the purpose of facilitating the commission of sexual activity or production of any form of CSAEM.



A survey of 950 children aged 12–17 found that 13% had **their sexual images shared without consent**, mostly by strangers (56%).

The findings reveal the widespread nature of online exploitation in the Philippines.

Source: Disrupting Harm 2022

Philippines

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses

Sextortion

Sextortion, a form of blackmail involving sexual materials or situations, is an increasingly common cybercrime. In the Philippines, laws and regulations have been enacted to criminalize such activities, chiefly among them being Republic Act No. 10175 or the "Cybercrime Prevention Act of 2012," and Republic Act No. 9995, known as the "Anti-Photo and Video Voyeurism Act of 2009."

Sextortion generally involves the use or threat of sharing explicit images, videos, or information about a person without their consent, typically with the aim of coercing money, favors, or further explicit content from the victim. Under Philippine law, this can be categorized as unauthorized access, data interference, and/or unlawful or prohibited conduct.

- **Republic Act No. 9995 (Anti-Photo and Video Voyeurism Act of 2009):** Prohibits the distribution or publication of explicit photos or videos without the consent of the individual depicted.
- **Republic Act No. 10175 (Cybercrime Prevention Act of 2012):** Defines cybercrime offenses, including online sextortion, and imposes penalties one degree higher than those provided for by the Revised Penal Code for similar offenses committed offline.
- **Article 282 of the Revised Penal Code:** Criminalizes grave threats, which can encompass sextortion even if no money is ultimately paid. Convicted offenders can face substantial prison time.

95% of children aged 12–17 in the Philippines access the internet using **mobile phones**, making it the most popular device.

In comparison, 20% use computers and 7% use tablets, reflecting the dominant role of mobile technology in young people's online lives.

Source: Disrupting Harm 2022



Ghana

Legal Definitions of ‘Child’ in Ghana

In Ghana, the legal definition of a “child” is both foundational and far-reaching, framing the country’s child protection obligations in both physical and digital environments.

According to Article 28(5) of the 1992 Constitution of the Republic of Ghana, a child is defined as “**a person below the age of eighteen years.**” This definition is reinforced by Section 1 of the Children’s Act, 1998 (Act 560), which likewise defines a child as “a person below the age of eighteen.” Together, these laws form the legal cornerstone of Ghana’s child protection framework, underpinning a rights-based approach that extends from education and healthcare to the digital protection of minors.

Further aligned with international obligations, **Ghana has ratified the United Nations Convention on the Rights of the Child (UNCRC)**, which defines a child similarly and strengthens Ghana’s global commitment to protect children across all domains. The minimum legal age for light work is set at 13, with broader employment protections applying from age 15 under Ghanaian labour standards, demonstrating the country’s recognition of the evolving capacities of children.

While the age of 18 remains consistent across most protections, the application of this definition in digital contexts presents growing challenges. As internet usage and social media penetration rise, children in Ghana increasingly face risks of online grooming, sextortion, cyberbullying, and exposure to child sexual abuse material (CSAM), including deepfakes and AI-generated content. These emerging threats have exposed gaps in digital enforcement and case adjudication, especially where perpetrators exploit technological tools to mask identities and simulate underage imagery.

Yet, Ghana’s legal ecosystem is evolving. The Cybersecurity Act, 2020 (Act 1038) represents a significant stride forward, introducing cyber-specific offenses involving children, such as child pornography, grooming, and unauthorized image sharing. Complemented by the National Child Online Protection (COP) Framework, which emphasizes digital literacy, stakeholder coordination, and law enforcement training, Ghana is taking a proactive stance in adapting child protection to the realities of a networked world.

The classification of a person under 18 as a “child” is not only symbolic—it is the legal trigger for specialized reporting mechanisms, judicial protections, and psychosocial support. As digital harms become more nuanced, Ghana’s ability to maintain a unified, consistent definition of “child” across its legal instruments is essential. This consistency allows prosecutors to pursue offenders of online grooming, CSAM possession, or sextortion under age-based protections, even when digital evidence complicates identity verification or consent.

In today’s digital era, the definition of “child” is not static—it is a legal compass. It must be responsive, resilient, and respected across emerging technologies to uphold the dignity and safety of Ghana’s children.



Ghana

Age-Based Definitions Across National Laws



Law / Regulation	Article	Definition of Child	Age Limit	Notes
Constitution of the Republic of Ghana, 1992	Art. 28(5)	A person below the age of eighteen years	18	Foundational definition within the supreme law of Ghana, establishing the basic age of childhood.
Children's Act, 1998 (Act 560)	Sec. 1	A person below the age of eighteen years	18	This Act consolidates laws on children's rights, welfare, maintenance, adoption, and protection.
Juvenile Justice Act, 2003 (Act 653)	Sec. 1	A person below the age of eighteen years	18	Defines "child" generally. Also defines "juvenile" (person under 18 in conflict with the law) for justice system purposes.
UN Convention on the Rights of the Child (ratified by Ghana)	Article 1	Every human being below the age of 18 years unless under applicable law, majority is attained earlier	18	International standard ratified by Ghana; forms the basis for much of Ghana's child rights legislation.
National Child Online Protection (COP) Framework (2021)	Sec. 2.2	Adopts the definition from the Children's Act, 1998 (Act 560): a person below the age of eighteen (18) years.	18	Guides the implementation of child online protection and safety measures in Ghana, using the established national legal definition.

Ghana

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses

Ghana stands among the leading African nations that have proactively established a legal and institutional framework to combat online sexual crimes against children. With growing internet penetration and digital engagement among the youth, the Ghanaian government, with the support of UNICEF, enacted the **Cybersecurity Act, 2020 (Act 1038)**, which offers targeted provisions to address digital threats to child safety.



A cornerstone of the law, Section 62(1), criminalizes the unauthorized creation and dissemination of images of children with exploitative intent. Specifically, it prohibits any person from taking or requesting photographs or recordings of a child—or from producing, obtaining, publishing, broadcasting, live-streaming, or sharing such content—when done with the purpose of exploitation.

Section 63 expands the scope of the law by criminalizing online grooming and enticement. It prohibits individuals from using internet services, bulletin boards, or any electronic communication tools to lure, solicit, groom, or prepare a child—or a person believed to be a child—for sexual activity or the production of sexually explicit content. This section reflects international legal trends by acknowledging that many online child abuse cases begin with psychological manipulation or digital contact.

A particularly significant innovation in Ghana's legal framework is its explicit criminalization of sextortion, codified under Section 66. This provision prohibits individuals from threatening to distribute intimate images of a child—whether through email, text, or social media—when the purpose is to harass, coerce, extort money, or force the victim into unwanted sexual activity.



Collectively, these provisions position Ghana as a country that takes a comprehensive and forward-looking approach to online child protection. **The Cybersecurity Act 2020 aligns national legislation with international child rights instruments, including the UN Convention on the Rights of the Child and the WeProtect Global Alliance Model National Response Framework.** By criminalizing a wide spectrum of online sexual offenses—ranging from grooming and sextortion to unauthorized image sharing—Ghana not only safeguards its children but also sets a benchmark for legislative models in sub-Saharan Africa.

Nonetheless, effective implementation remains critical. The legal infrastructure must be supported by digital literacy campaigns, accessible child reporting mechanisms, and continuous capacity building for law enforcement and judiciary actors. Only through this holistic approach can Ghana ensure that its strong legal provisions translate into real-world protection for its children in the digital age.

"The Cybersecurity Act 2020 is a crucial advancement towards creating a safer digital environment for children in Ghana."

Honourable Ursula Owusu-Ekufu, Minister for Communications and Digitalisation of Ghana



Ghana

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses



Child Sexual Abuse (CSA) and Child Sexual Exploitation (CSE)

Child Sexual Abuse (CSA) and Exploitation (CSE), including their online dimensions, are addressed through a combination of Ghana's core criminal law, child protection legislation, and specific cybersecurity laws. The primary definition of a child is established in the Children's Act.



Children's Act, 1998 (Act 560):

- Section 13 (Protection from torture and degrading treatment): Enshrines the right of a child to be protected from torture and other cruel, inhuman, or degrading treatment or punishment.



Criminal Offences Act, 1960 (Act 29):

- Section 101 (Defilement of female under 16): Criminalizes sexual intercourse with a female under the age of sixteen years.



Cybersecurity Act, 2020 (Act 1038):

Section 63 (Dealing with child for purposes of sexual abuse):

- A person shall not deal with a child for the purposes of sexual abuse.
- A person deals with a child for the purpose of sexual abuse where that person uses an electronic medium to:
 - (a) persuade, coerce or solicit a child to engage in sexual abuse; or
 - (b) facilitate the meeting of the child whether in person or through an electronic medium for the purposes of sexual abuse.

National Child Online Protection (COP) Framework: Aims to tackle Online Child Sexual Exploitation and Abuse (OCSEA) and references the relevant sections of the Cybersecurity Act. The glossary defines "Online Sexual Abuse" as "any form of sexual abuse of children which has a link to the online environment".

Sexually Explicit Conduct (involving children)

Ghanaian law does not define a single broad category of "Sexually Explicit Conduct" involving children. Instead, specific acts constituting such conduct are criminalized under:



Cybersecurity Act, 2020 (Act 1038):

- Section 62: Prohibits producing, distributing, possessing, etc., an "indecent image and photograph of a child".
- Section 63: Prohibits using electronic means to persuade, solicit, or facilitate meetings with a child for "sexual abuse".

Ghana

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses

Child Sexual Abuse Material (CSAM) / Child Pornography

In Ghana, the legal jurisdiction concerning Child Sexual Abuse Material (CSAM), also referred to as child pornography, is governed by several laws and international conventions aimed at addressing the production, possession, distribution, and facilitation of such material.



National Legal Framework

Cybersecurity Act, 2020 (Act 1038): This Act criminalizes offenses related to CSAM, including the production, possession, and distribution of child pornography through computer systems.

Children's Act, 1998 (Act 560): Section 17 of the Children's Act highlights the protection of children from abuse, neglect, and exploitation. While it does not specifically address online sexual exploitation, it provides a general framework for safeguarding children's welfare

Electronic Transactions Act, 2008 (Act 772): Section 136 prohibits the use of computer systems for producing or distributing child pornography. It also criminalizes the possession of such material.

Criminal Code: The Criminal Code addresses broader sexual exploitation of children under provisions related to indecent assault and abuse. However, it does not specifically define CSAM in digital contexts.



International Conventions

African Union Convention on Cyber Security and Personal Data Protection:

Ghana signed this convention in 2017 (though not yet ratified),⁶⁹ which defines child pornography as any visual depiction involving a minor engaging in sexually explicit conduct, including digitally generated images.⁷⁰

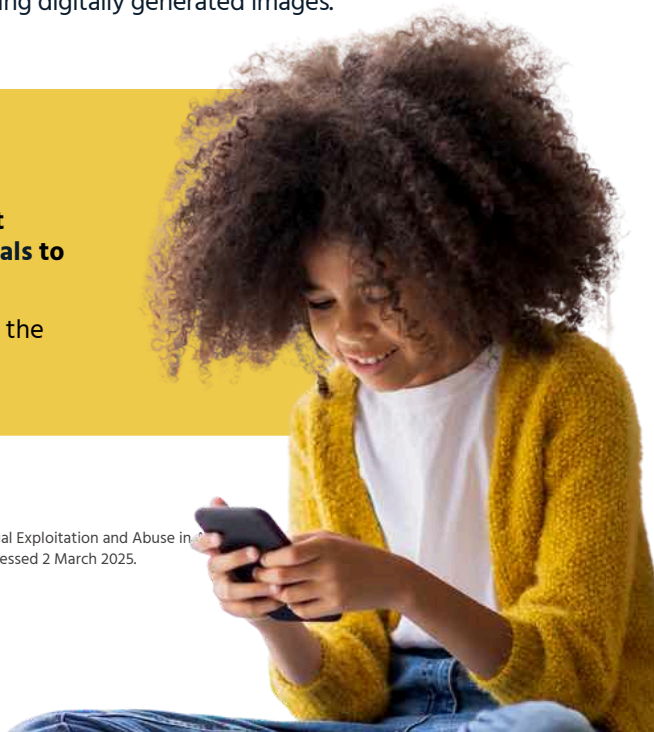
In order to combat online child sexual exploitation and abuse, including grooming,

Ghana has formulated comprehensive legislation, to mandates Internet Service Providers (ISPs) to report suspected cases of child abuse materials to a designated agency,

whereas other stakeholders are required to report if they identified gaps in the current regulatory framework.

69. UNICEF, Children's online safety concerns in Ghana 2018, <<https://www.unicef.org/ghana/media/1806/file/Child%20Online%20Safety%20%20Legislation%20and%20Policy%20Gaps.pdf>>, accessed 2 March 2025.

70. AFRICA UNION INITIATIVE ON: Strengthening Regional and National Capacity and Action against Online Child Sexual Exploitation and Abuse in Africa, files/newsevents/workingdocuments/41106-wd-Continental_Strategy_POA_Draft_16_Oct_2020_-_English.pdf, accessed 2 March 2025.



Ghana

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses



Computer-Generated CSAM / AI-Based Abuse

In Ghana, the legal framework addressing computer-generated child sexual abuse material (CSAM) and AI-based abuse is primarily governed by existing laws on cybercrime and child protection. **The current legal framework does not explicitly address AI-generated CSAM.** While existing laws criminalize child pornography broadly, they do not specifically define or regulate synthetic media created by AI technologies.



Cybersecurity Act, 2020 (Act 1038): This Act criminalizes the production, possession, and distribution of child pornography, including digital formats, through computer systems. Offenders can face fines or imprisonment of up to ten years or both.



Electronic Transactions Act (ETA), 2008 (Act 772): Section 136 of this Act also prohibits the publication, production, procurement, or possession of child pornography using computer systems.



ECOWAS Directive on Cybercrime: Ghana is bound by the ECOWAS Directive C/DIR. 1/08/11 on Fighting Cybercrime, which criminalizes the production and distribution of child pornography using ICTs. This includes computer-generated imagery depicting minors in sexually explicit conduct.



African Union Convention on Cyber Security and Personal Data Protection: Ghana signed this convention in 2017 but has yet to ratify it. The convention defines child pornography to include computer-generated imagery where minors appear to engage in sexually explicit conduct.

Grooming and Enticement

The context of online sexual exploitation of children, is primarily governed by provisions within the Cybersecurity Act, 2020 (Act 1038). This Act criminalizes grooming and enticement, whether successful or attempted, using cyberspace or electronic systems.



Cybersecurity Act, 2020 (Act 1038): The Act makes it an offense to use cyberspace (including computer systems, internet services, or other electronic devices) to seduce, solicit, lure, groom, entice, or attempt to entice a child for unlawful sexual conduct. The law applies even if the attempt is unsuccessful.



National Child Online Protection (COP) Framework:⁷¹ The glossary defines Cyber Grooming as a series of acts that facilitate cyber-enticement such as actions deliberately undertaken to befriend and establish an emotional connection with a child, to lower the child's inhibitions in preparation for sexual activity with the child.

71. NATIONAL CHILD ONLINE PROTECTION FRAMEWORK, Ghana, <<https://www.csa.gov.gh/resources/National%20COP%20Framework.pdf>>, accessed 2 March 2025.

Ghana

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses

Sextortion

In Ghana, the legal jurisdiction for sextortion is primarily governed by the Cybersecurity Act, 2020 (Act 1038). This legislation explicitly criminalizes sextortion as a form of cybercrime, addressing threats to distribute private or intimate images or videos to extort victims.



Cybersecurity Act, 2020 (Act 1038):

Section 66(1): It is illegal for any person to **threaten the distribution of private images or videos** of another individual engaged in sexually explicit conduct via electronic means (e.g., email, text, social media). This includes threats made with the intent to:

- Harass, coerce, or intimidate.
- Extort money or other benefits.
- Compel the victim to engage in unwanted sexual activity.

The Act also criminalizes threats **involving intimate images of minors and defines “intimate images”** broadly to include depictions of uncovered genital regions or breasts visible through clothing. The Cybersecurity Act criminalizes not only sextortion but also the intentional distribution of intimate images without consent if it causes emotional distress.

“Online safety for children in Ghana is not just a matter of technology — it’s about power, justice, and accountability. Despite the Cybersecurity Act 2020, children, especially girls, continue to face digital abuse without adequate protection.

Without survivor-centered systems and political will, the internet will remain a place where Ghanaian girls learn early that silence is safety, and visibility is danger.”

Hiqmat Sungdeme Saani, Founder of Paahibu Space



Rwanda

Legal Definitions of 'Child' in Rwanda

In Rwanda, the legal definition of a “child” is firmly established in its legislative framework as any person under the age of 18 years. This definition is consistent across various laws and aligns with international standards, such as the United Nations Convention on the Rights of the Child (CRC) and the African Charter on the Rights and Welfare of the Child (ACRWC), both of which Rwanda has ratified. These international instruments emphasize that every person below 18 years is entitled to special care, protection, and rights due to their vulnerability.

The primary legislation defining a child in Rwanda is the Law No. 27/2001 Relating to the Rights and Protection of the Child, which explicitly states that a child is “anybody aged below eighteen (18) years.”

This definition is reinforced by subsequent laws, including the Law Relating to the Protection of the Child (2018), which reiterates this age threshold. The uniformity in defining a child ensures consistency in applying child protection laws across various domains such as family law, criminal justice, labor regulations, and education policies.

In labor law, for example, Rwanda’s Labour Law (2009) defines a child as anyone under 18 years and prohibits their engagement in hazardous work. This provision reflects the government’s commitment to protecting children from exploitation and ensuring their right to education and development. Similarly, Rwanda’s justice system recognizes individuals under 18 years as children; however, criminal responsibility begins at age 14. This distinction means that while children aged between 14 and 18 can be held accountable for criminal acts, they are still afforded protections under juvenile justice principles. For instance, they are tried in specialized courts with procedures tailored to their age and developmental needs.

However, while this legal framework is robust, certain nuances deserve closer examination. The distinction made for criminal responsibility at age 14 raises questions about how children in this age bracket are treated under the justice system. Although they are still legally defined as children, their accountability for criminal acts introduces a level of complexity that requires careful balancing between justice and rehabilitation. It is essential that these young offenders are treated in ways that prioritize their reintegration into society rather than punitive measures.

While exceptions in specific laws may exist—for example, regarding early marriage or emancipation—these must not undermine broader protections guaranteed to children under Rwandan law. Any deviation from the universal definition of childhood risks exposing vulnerable minors to exploitation or harm. Rwanda’s legal definition of a child as any person below 18 years provides a strong foundation for protecting children’s rights across all sectors. The country’s alignment with international standards underscores its commitment to fostering an environment where children can thrive. However, continuous vigilance is necessary to ensure that exceptions or legal nuances do not erode these protections or compromise the well-being of young people.



Rwanda

Age-Based Definitions Across National Laws



Law / Regulation	Article	Definition of Child	Age Limit	Notes
Law No. 71/2018 relating to the Protection of the Child	Article 3(6)	Any person under eighteen (18) years of age	18	Current core child protection statute; replaced Law No. 54/2011
Law No. 27/2001 relating to Rights and Protection of the Child Against Violence	Article 1	Anybody aged below eighteen (18) years with the exception of what is provided for in other laws	18	Earlier child protection law; includes exceptions referring to other laws
Justice for Children Policy	Section 2.2.1	A child, in general, is a person under the age of 18; while A child for purposes of being held criminally responsible is a person aged between 14 and 18.	18 (general); 14-18 (criminal responsibility)	Children under 14 cannot be held criminally responsible
Law No. 68/2018 of 30/08/2018 determining offences and penalties in general (Penal Code)	Article 2 (8)	Any person under the age of eighteen (18) years	18	All individuals below 18 years are considered children.
Organic Law No. 29/2004 on Rwandan Nationality	Article 3	Defines majority age as "eighteen (18) complete years of age"	18	Establishes age of majority for citizenship purposes

Rwanda

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses



Child Sexual Exploitation (CSE)

Under Rwandan law, a child is defined as any person under the age of 18 years. This definition is consistent across key legal instruments, including Law No. 27/2001 Relating to the Rights and Protection of the Child, Law No. 68/2018 Determining Offenses and Penalties in General (Penal Code), and Law No. 71/2018 Relating to the Protection of the Child.⁷²



Law No. 68/2018 (Penal Code):

- Article 259 criminalizes child trafficking for prostitution or indecent practices, with penalties ranging from 3 to 10 years' imprisonment depending on the age of the child involved and the severity of the offense.
- Article 260 addresses acts such as recruiting, manipulating, or holding a child for indecent practices or prostitution. It also criminalizes opening or renting premises for such purposes.



Law No. 27/2001 Relating to Rights and Protection of the Child Against Violence:

- Article 38 criminalizes attracting, persuading, or deceiving a child into prostitution or fornication.
- Articles 39–42 define crimes of child exploitation, imposing prison sentences and fines for supporting child prostitution, benefiting from it, or using children for pornographic purposes. Additionally, severe penalties including life imprisonment apply for kidnapping, selling, or enslaving children, while giving illicit drugs or using children in drug trafficking also carries lengthy prison terms and fines.

Sexually Explicit Conduct

Sexually explicit conduct involving children is a serious offense under Rwandan law, with comprehensive legal provisions aimed at preventing, punishing, and eradicating such acts. The legal framework addresses both the production and involvement of children in sexually explicit activities.

Rwandan law **does not explicitly define “sexually explicit conduct”** as a standalone term in its statutes. However, related **offenses involving children are covered under broader legal provisions**. For instance:



- Article 33 of Law No. 27/2001 Relating to the Rights and Protection of the Child considers any sexual relations with a child as rape, regardless of the means or methods used.
- The Penal Code (Law No. 68/2018) criminalizes acts involving sexual violence, harassment, and exploitation, including those that could be classified as sexually explicit conduct when involving minors.

72. Rwanda Child Online Protection Policy, Ministry of ICT & Innovation Republic of Rwanda, <https://rura.rw/fileadmin/Documents/ICT/Laws/Rwanda_Child_Online_Protection_Policy.pdf>, accessed 2 March 2025.

Rwanda

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses



Sexually Explicit Conduct



Law No. 68/2018 Determining Offenses and Penalties in General (Penal Code):

- Article 191 criminalizes child defilement, which includes cases where children are involved in sexual activities. Perpetrators face life imprisonment if convicted.



Law No. 71/2018 Relating to the Protection of the Child:

- Article 33 criminalizes showing pornographic images or sounds to a child.
- Article 34 prohibits recording a child's pornographic image or voice.



Law on Prevention and Punishment of Gender-Based Violence (Law No. 59/2008):

- Articles 23–27 impose severe penalties for sexual slavery, harassment, torture, and other forms of violence that may involve sexually explicit conduct.



Law No. 60/2018 of 22/08/2018 on Prevention and Punishment of Cybercrimes:

- Article 34 criminalizes the publication or facilitation of pornography through computers or other information and communication technologies.
- Article 35 addresses **harassment involving sexually explicit content shared via computers or electronic systems. Offenders who distribute indecent images, sounds, or videos without consent face imprisonment.**
- Article 36 criminalizes the use of websites or electronic messages to obtain confidential information for unlawful purposes such as accessing sexually explicit content.
- Article 38 criminalizes the transmission or publication of indecent messages using computers or electronic systems.

In efforts to address child online abuse, **Government of Rwanda has established a Child Online Protection Policy (COP Policy)**

introduced in 2019 to mitigate against those risks and harms, and to deliver a framework that meets children's needs and fulfils their rights.



Rwanda

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses



Child Sexual Abuse & Child Sexual Abuse Material (CSAM)

Rwanda has established a comprehensive legal framework to address Child Sexual Abuse (CSA) and Child Sexual Abuse Material (CSAM). The laws criminalize acts of sexual violence against children, the production and distribution of CSAM, and related offenses. These provisions align with international standards, such as the United Nations Convention on the Rights of the Child (CRC) and the African Charter on the Rights and Welfare of the Child (ACRWC).



Law Relating to the Protection of the Child (Law No. 71/2018):

- Article 26 ensures privacy protections for child victims during criminal proceedings, mandating in camera trials and prohibiting public disclosure of their identity.
- Article 23 emphasizes that any criminal proceeding involving a child must prioritize their welfare.
- Article 33 prohibits exposing children to pornographic content.
- Articles 34 and 35 address CSAM specifically by targeting its production, advertising, and distribution.
- The privacy protections under Article 26 are particularly noteworthy as they aim to minimize secondary victimization during legal processes.



Law on Prevention and Punishment of Cybercrimes (Law No. 60/2018):

Article 34 outlines critical legal protections against the misuse of digital technologies for sexual exploitation. It establishes that any individual who publishes or distributes pornographic content through a computer system or any other form of information and communication technology is committing a punishable offense.

More significantly, it criminalizes the act of grooming or soliciting a child via digital platforms—such as a computer, computer system, or online network—with the intention of arranging a meeting to engage in sexual activities. This provision reflects a strong legal stance against technology-facilitated child sexual exploitation, acknowledging the unique risks posed by online grooming and digital communication tools.



Penal Code (Law No. 68/2018):

Article 133 criminalizes child defilement, with penalties based on the victim's age:

- For victims under 14 years: Life imprisonment without mitigation.
- For victims aged 14–18 years: Life imprisonment, which may be reduced to a minimum of 25 years in mitigating circumstances.

Rwanda

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses

Computer-Generated CSAM / AI-Based Abuse

Rwanda has yet to adopt specific laws addressing Computer-Generated Child Sexual Abuse Material (CSAM) or AI-Based Abuse. However, existing legal frameworks, such as the Law No. 60/2018 on Prevention and Punishment of Cybercrimes, the Child Online Protection Policy (COP Policy), and international commitments provide foundational provisions that can be applied to these emerging threats. These laws criminalize the publication, distribution, and facilitation of CSAM through digital platforms, while also addressing broader ICT-facilitated child sexual exploitation.



Law No. 60/2018 on Prevention and Punishment of Cybercrimes:

- Article 34 criminalizes publishing or facilitating access to pornography involving children through computer systems or networks. This article indirectly applies to AI-generated CSAM by penalizing any form of child pornography distributed via digital platforms.
- Article 35 criminalizes transmitting indecent information using computers or networks, which could encompass synthetic media created using AI technologies.



Child Online Protection Policy (COP Policy):

The COP Policy emphasizes internet surveillance to detect harmful content targeting children, including violent, nude, or abusive images. It mandates the creation of a database of digital images and cases for investigation purposes. The policy encourages technical controls such as filters and flagging systems for harmful content, which can be extended to AI-generated CSAM.

Rwanda has ratified the:

United Nations Convention on the Rights of the Child (CRC) and the African Charter on the Rights and Welfare of the Child (ACRWC)

both of which obligate member states to **protect children from all forms of sexual exploitation, including emerging threats like AI-generated CSAM.**



Rwanda

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses

Grooming and Enticement

Rwanda has established legal and policy frameworks to address grooming and enticement, particularly in the context of child sexual exploitation. These provisions are embedded in laws such as Law No. 71/2018 Relating to the Protection of the Child, the Penal Code (Law No. 68/2018), and the Law on Prevention and Punishment of Cybercrimes (Law No. 60/2018).

While specific definitions of grooming are not explicitly provided, related acts such as luring, enticing, or manipulating children for sexual purposes are criminalized. The legislative updates are needed to provide explicit definitions of grooming behaviors and expand protections against non-contact offenses facilitated by technology.



Grooming involves establishing a relationship of trust with a child to manipulate them into engaging in sexual activities or exploitation. In Rwanda, grooming is addressed indirectly through laws targeting preparatory acts that lead to child exploitation or abuse.

- **The Cybercrime Law (Article 34)** explicitly criminalizes grooming using ICTs, including soliciting children for sexual purposes through digital platforms.
- The absence of an explicit definition of “grooming” in Rwandan law may limit its scope in addressing non-contact offenses where the offender does not intend to meet the child offline but engages in prolonged manipulation online.



Enticement is addressed under provisions that prohibit luring children into exploitative acts:

- **Article 37 of Law No. 71/2018** criminalizes enticing children into beggary or other exploitative practices.
- The Penal Code addresses enticement leading to sexual exploitation under broader provisions on child defilement (Article 133).



Online grooming is explicitly addressed under cybercrime laws but requires clearer definitions and expanded provisions to address non-contact offenses effectively. The increasing use of ICTs for grooming behaviors is acknowledged under the Cybercrime Law and COP Policy:

- The Cybercrime Law provides penalties for offenders who use computers or networks to solicit children for sexual purposes.
- The COP Policy mandates ISPs to monitor platforms for online grooming activities and report offenders.



Rwanda

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses

Sextortion

Cyber or online sextortion is a growing concern in Rwanda as digital platforms become more integrated into daily life. Sextortion involves the coercion of individuals, often through threats to expose intimate images or videos, in exchange for money, sexual favors, or other demands.



Law N° 60/2018 (Prevention and Punishment of Cyber Crimes)

Article 35 of the Cybercrime Law addresses "**Cyber-stalking**". It penalizes any person who intentionally uses a computer or computer system to harass or threaten another person, thereby causing distress or fear. The article explicitly encompasses several actions relevant to sextortion, including:

- Displaying, distributing, or publishing indecent documents, sounds, pictures, or videos of any person.
- In bad faith, taking pictures, videos, or sounds of any person without their consent or knowledge.
- Displaying or distributing information in a manner that substantially increases the risk of harm or violence to any other person.

The core threat element inherent in sextortion – the threat to disseminate compromising images unless demands are met – aligns directly with the definition of harassment and threats causing fear or distress under this article. Furthermore, the act of distributing, or threatening to distribute, indecent material is explicitly covered.



Law N°68/2018 (Determining Offences and Penalties in General - Penal Code)

Article 129 of the Penal Code addresses the offense of "**Blackmail**" (French: "Chantage"). This general provision criminalizes the act of extorting or attempting to extort money, property, or any other benefit from a person by means of threats, typically involving the exposure of information that could damage the victim's reputation or cause distress. This directly applies to the extortionate demand element central to sextortion, where the threat involves the dissemination of sexually explicit material. The Penal Code's broad definition of blackmail likely encompasses threats made digitally to reveal compromising images or videos for gain.

The structure of Rwanda's criminal legislation demonstrates a complementary relationship between the specific Cybercrime Law and the general Penal Code. Law N° 60/2018 primarily addresses the method of the crime – the use of ICT, unauthorized access, digital interception, and electronic distribution. Conversely, Law N°68/2018 focuses on the nature of the underlying criminal act, such as blackmail, harassment, or offenses against morals.

Since cyber sextortion involves both the use of technology and constitutes underlying criminal behavior like blackmail and harassment, these two laws function in tandem. This allows prosecutors the flexibility to formulate charges based on both the technological means employed (under the Cybercrime Law) and the fundamental criminal conduct involved (under the Penal Code), potentially enabling more comprehensive and effective prosecutions.



Dominican Republic

Legal Definitions of 'Child' in Dominican Rep.



The Dominican Republic has established a detailed and tiered legal framework to define and protect the rights of children and adolescents, principally through Law No. 136-03, officially titled the Código para el Sistema de Protección y los Derechos Fundamentales de Niños, Niñas y Adolescentes. Enacted on August 7, 2003, this comprehensive statute stands as the backbone of child protection law in the country, systematically addressing the civil, social, educational, labor, and judicial rights of all individuals under 18 years of age. It replaced the earlier Law No. 14-94, modernizing the child protection system to reflect international standards.

At the heart of this legal structure is the categorical classification of minors into two distinct age groups —“niños/as” (children) and “adolescentes” (adolescents)—each bearing unique legal characteristics and degrees of protection under Dominican law. This classification is more than semantic; it is the key to understanding how rights, responsibilities, and protections evolve with age, culminating in full legal capacity at adulthood.

Article II of Law No. 136-03 sets forth the official definitions. A “niño” or “niña” is defined as any individual from birth up to and including twelve years of age. An “adolescente,” by contrast, refers to individuals aged thirteen through seventeen, until they reach the age of majority at 18.

This two-tiered classification is not merely theoretical—it shapes how Dominican law interacts with minors in a wide variety of contexts. For instance, criminal liability begins at age 13, meaning that “niños/as” are absolutely exempt from criminal prosecution. Adolescents, while subject to legal accountability, are processed through a specialized juvenile justice system that further distinguishes between the ages of 13–15 and 16–17 when determining the nature and length of sanctions.

Adolescents are granted increased rights to participate in decisions that affect them, particularly in legal, health, and administrative proceedings. The legal weight of their opinion grows with age. While all minors have the right to express their views, adolescents’ capacity to give valid legal consent is more broadly recognized—for example, in medical decisions or judicial matters.

In synthesis, the **Dominican Republic defines “child” as any person under the age of eighteen, subdivided legally into “niños/as” (ages 0–12) and “adolescentes” (ages 13–17).** This distinction is embedded within a constitutional and civil framework that ensures consistency across civil, criminal, labor, and family law domains. The protection of children and adolescents is not only legislated but constitutionally enshrined, prioritizing the best interests of the child as the guiding principle of all related policy and legal interpretation.

Dominican Republic

Age-Based Definitions Across National Laws



Law / Regulation	Article	Definition of Child	Age Limit	Notes
Code for the Protection of the Rights of Children and Adolescents (Law No. 136/03)	Principle II (General Principles)	A child is considered every person from his birth to twelve years, inclusive; and adolescent, from thirteen years until reaching adulthood	Child: 0-12; Adolescent: 13-17	Core child protection statute; establishes foundational definitions for other laws
Code for the Protection of the Rights of Children and Adolescents (Law No. 136/03)	Article 223	Differentiates age scales for criminal justice purposes	13-15 and 16-18	Children under 13 years "under no circumstances, are criminally responsible"
Civil Code	Article 148	Not explicitly defined, but establishes consent requirements for marriage	Females: 21; Males: 25	Requires parental consent for marriage for females under 21 and males under 25
Penal Code	Article 331	Refers to definitions in Law No. 136/03	Child: 0-12; Adolescent: 13-17	Establishes heightened penalties for sexual violations committed against a child or adolescent

Dominican Republic

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses



The Dominican Republic's legal architecture for child protection is built upon strong constitutional guarantees, further elaborated by the comprehensive **Child Protection Code (Law 136-03)**. This foundational law not only defines rights but also establishes key mechanisms like the principle of the best interest, the presumption of minority, and specific prohibitions against exploitation and abuse. However, the practical application involves navigating the interplay between Law 136-03 and other critical statutes, namely the **Penal Code (as amended by Law 24-97)**, the **High Tech Crimes Law (Law 53-07)**, and the **Trafficking Law (Law 137-03)**.

This layering of legislation creates a complex landscape where offenses, particularly those facilitated by technology, might be covered by multiple laws. For instance, the production or distribution of Child Sexual Abuse Material (CSAM) falls under both Law 136-03 (Arts. 25, 408, 411) and Law 53-07 (Art. 24). Similarly, acts constituting commercial sexual exploitation under Law 136-03 (Art. 25, 410) may also meet the definition of trafficking for sexual exploitation under Law 137-03. While this provides prosecutors with multiple avenues, it also necessitates clear understanding and potentially specific guidelines to ensure consistent application of the law and appropriate charging decisions, considering the different elements and penalties associated with each statute. **The explicit inclusion of protection against abuse via "internet or any electronic means" in Law 136-03 (Art. 13) highlights its continued relevance alongside the more specific cybercrime provisions of Law 53-07.**

Furthermore, the mandatory duty to report abuse under Law 136-03 (Art. 14) stands out as a crucial legal instrument for detection and prevention. This obligation extends beyond officials to encompass any person aware of or suspecting abuse, aiming to break cycles of silence, particularly within families or institutions where professionals interact closely with minors. The effectiveness of this provision hinges critically on widespread awareness among the obligated parties, accessible and confidential reporting channels, and consistent enforcement of the stipulated penalty for non-compliance. Practical challenges, such as fear of reprisal or lack of clarity on procedures, could potentially undermine this vital mechanism, an issue reflected in broader discussions about implementation difficulties within the child protection system.

Child Sexual Exploitation (CSE)

Child Sexual Exploitation (CSE) involves the use of a child or adolescent for the sexual gratification of another person or persons, often involving elements of commercial transaction, coercion, or abuse of vulnerability. The Dominican legal framework addresses CSE through several key statutes.

Law 136-03 (Child Protection Code):

- **Article 25:** Directly prohibits the commercialization, prostitution, and use of children/adolescents in pornography.
- **Article 410:** Specifically sanctions the commercial sexual exploitation of minors, defined as the use of a minor in sexual activities in exchange for money, favors in kind, or any other remuneration. This article targets the client/exploiter as well as facilitators.

Dominican Republic

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses



Law 137-03 (Trafficking Law):

- **Article 1 (Definitions):** Defines "Trata de Personas" (Trafficking in Persons) to include the recruitment, transportation, transfer, harboring, or receipt of persons using specific means (threat, force, coercion, abduction, fraud, deception, abuse of power/vulnerability, payment/benefit exchange) for the purpose of exploitation. The definition of "Explotación" explicitly encompasses "toda forma de explotación sexual" (all forms of sexual exploitation) and "pornografía"
- **Article 3:** Criminalizes the act of trafficking in persons, explicitly including children, adolescents, and women, for the purpose of exploitation (including sexual exploitation), emphasizing that the consent of the victim is irrelevant to the offense.

Sexually Explicit Conduct Involving Minors

This category encompasses sexual acts committed against minors that may not involve commercial elements or trafficking but constitute abuse due to the age of the victim and the absence of valid consent. The Penal Code, particularly as amended by Law 24-97 on Intra-family Violence, is the primary source for these offenses.



- **Penal Code, Art. 330:** Defines "Agresión Sexual" (Sexual Aggression) broadly as any sexual act committed with violence, coercion, threat, surprise, or deception. This serves as a foundational definition.
- **Penal Code, Art. 332:** Addresses non-consensual sexual activity within a couple's relationship (marital rape) under specific circumstances like force, incapacitation, or coercion involving third parties. While primarily concerning adults, the principles of non-consent are relevant.
- **Penal Code, Art. 332-1:** Defines "Incesto" (Incest) as any sexual act by an adult against a child or adolescent with whom they share specified kinship ties (up to 4th degree consanguinity, 3rd degree affinity), committed through deception, violence, threat, surprise, or coercion.
- **Law 136-03, Art. 396(c):** Defines and sanctions sexual abuse by adults against minors, specifying it as any sexual act imposed using force, intimidation, seduction, or surprise.

Child Sexual Abuse & Child Sexual Abuse Material (CSAM)

Child Sexual Abuse (CSA) encompasses a range of abusive sexual acts against minors, while CSAM refers to visual depictions of such abuse. The CSA define through general protection principles, which define in:



- **Law 136-03, Art. 12:** Establishes the right to personal integrity, including sexual integrity, and mandates protection from all forms of abuse.
- **Law 136-03, Art. 13:** Affirms the State's duty to protect minors from abuse, explicitly including abuse facilitated via the internet or electronic means.
- **Law 136-03, Art. 396(c):** Specifically penalizes sexual abuse committed by adults against minors, defining it as any sexual act imposed on a minor using force, intimidation, seduction, or surprise.

Dominican Republic

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses



The Child Sexual Abuse Material (CSAM) is addressed specifically in both the Child Protection Code and the High Tech Crimes Law:

- **Law 53-07, Art. 4 (Definitions):** Defines "Pornografía Infantil" (Child Pornography) as "Any representation, by any means, of children, girls, and adolescents, engaged in explicit sexual activities, real or simulated, or any representation of the genitals of children, girls, and adolescents for primarily sexual purposes". It also adopts the age definitions from Law 136-03 (child up to 12, adolescent 13-17).
- **Law 53-07, Art. 24:** Criminalizes the production, diffusion, sale, and any type of commercialization of CSAM (as defined in Art. 4) via information systems. Its paragraph specifically penalizes the acquisition and intentional possession of CSAM within an information system or its components
- **Law 136-03, Art. 25:** Prohibits the use of children and adolescents in pornography, defining pornography similarly to Law 53-07.
- **Law 136-03, Art. 408:** Sanctions the use or employment of minors in theatrical, television, or cinematographic productions featuring pornographic or sexual scenes.

The existence of CSAM provisions in both the Child Protection Code (Law 136-03) and the High Tech Crimes Law (Law 53-07) creates parallel legal avenues. Law 136-03, enacted earlier, primarily addresses the use of minors in pornography within more traditional contexts like media productions. Law 53-07, specifically designed for the digital age, explicitly targets offenses committed using information systems and notably criminalizes the acquisition and possession of CSAM, covering a broader spectrum of online conduct.

This dual framework offers prosecutors flexibility but also underscores the importance of selecting the appropriate statute based on the specific criminal act and the medium used. For instance, online possession or distribution would clearly fall under Law 53-07, while using a minor in a film might primarily engage Law 136-03. Case law confirms that both laws can be applied concurrently in relevant situations.

"There is little knowledge and information provided about the risks young people may encounter online, and limited awareness of available protection or reporting options.

Parents, teachers, and caregivers often do not fully understand the digital world or believe what children are experiencing and telling them.

Plan International's community-based work integrates online safety into broader training programs on child rights, protection, and resilience.

We need more focused initiatives and wider communication strategies to address online sexual exploitation. A major challenge is that support systems, including reporting protocols and psychological care, are often unknown or inaccessible. Law enforcement also struggles due to the anonymity of the internet."

Roland Angerer, Country Director of Plan International Dominican Republic



Dominican Republic

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses



Computer-Generated / AI-Based CSAM

The proliferation of artificial intelligence (AI) presents new challenges for legal frameworks addressing CSAM, particularly concerning synthetically generated material that realistically depicts child abuse but may not involve a real child in its creation.

The key provision is the definition of "Pornografía Infantil" in **Law 53-07, Article 4**, which includes "Toda representación, por cualquier medio, de niños, niñas y adolescentes, dedicados a actividades sexuales explícitas, **reales o simuladas...**" (Any representation, by any means, of children..., engaged in explicit sexual activities, **real or simulated...**). **The critical question is whether "simuladas" (simulated) encompasses purely synthetic, AI-generated images that realistically depict minors in sexual acts, even if no actual child was photographed or filmed. The law itself does not define "simuladas" further in this context.** An interpretation could argue that a realistic AI image is a "representation" of a minor engaged in "simulated" sexual activity, thus falling under the definition. International instruments like the Council of Europe's Lanzarote Convention refer to "realistic images representing a minor", indicating a trend towards covering such material. However, without explicit clarification in Dominican law or guiding jurisprudence, the applicability remains uncertain.

The ambiguity surrounding the term "simuladas" constitutes a significant potential legislative gap. If interpreted narrowly to require some link to a real child (e.g., digitally altered images of real children), then purely synthetic AI-generated CSAM, which convincingly depicts abuse without using an image of an actual victim, might escape prosecution under the current law. This is particularly concerning given the increasing sophistication of AI image generation. The acknowledged need to update Law 53-07 to address evolving technological threats provides an opportunity to close this gap, although specific proposals addressing AI CSAM were not detailed in the provided materials. The challenges posed by AI in the penal process have been recognized.

The rapid advancement of AI technology capable of creating hyper-realistic depictions of child sexual abuse necessitates urgent legislative clarification. Relying on the potentially ambiguous term "simuladas" creates legal uncertainty and a loophole that could be exploited by producers and distributors of synthetic CSAM.

Explicitly including realistic computer-generated or AI-generated images that depict minors engaged in sexually explicit conduct within the legal definition of CSAM is essential to ensure comprehensive child protection in the digital era. Failure to do so leaves a critical vulnerability in the legal framework against emerging forms of technologically created abusive material.

Dominican Republic

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses

Grooming and Enticement

Grooming refers to the process whereby an adult builds an emotional connection and trust with a child or adolescent, often online, with the ultimate intention of sexually abusing or exploiting them. Enticement involves luring or persuading a minor into sexual activity or a situation where abuse can occur. Based on the available legal texts and secondary sources, the Dominican Republic currently lacks a specific criminal offense explicitly defined as "grooming" or "online solicitation of a minor for sexual purposes".

Prosecution of grooming-related conduct must therefore rely on existing, often ill-fitting, legal provisions:

Law 53-07, Art. 23 (Atentado Sexual): Applicable only if the grooming process culminates in a sexual assault committed through an information system. This fails to address the preparatory grooming phase itself.

Penal Code, Arts. 354-355 (Sustracción de menores/Abduction/Enticement): Could apply if grooming leads to luring the minor away from home for an offline meeting or abduction.

Draft Legislation (Project 00736-2021-PLO-SE): A specific draft law targeting grooming (also termed "Acoso Sexual Virtual" or Virtual Sexual Harassment)⁷⁴ was introduced in 2021.

This proposal aimed to:

- Define grooming as actions by an adult to contact a minor online, build false trust through manipulation/deception (often hiding adult identity), with the purpose of inducing sexual acts.
- Distinguish between grooming with and without a prior trust-building phase.⁷⁵
- Link penalties to Law 53-07, Art. 23 (Atentado Sexual), proposing fines (5-200x min. wage) for grooming acts leading to extortion, and 3-10 years prison for grooming aimed at sexual aggression or psychological abuse.
- Emphasize prevention via digital literacy and parental controls.
- However, legislative records indicate this specific project may have lapsed ("Perimida"), although general efforts to update cybercrime laws continue.⁷⁶

74. 00736-2021 Proyecto De Ley - Memoria Histórica del Senado de la República Dominicana, <<https://memoriahistorica.senadord.gob.do/items/ac7c5de1-57fa-483b-baa9-0b2f282ccabb/full>>, accessed 9 March, 2025.

75. memoriahistorica.senadord.gob.do, <<https://memoriahistorica.senadord.gob.do/bitstreams/f55b6822-6bfc-4387-a29a-1dbf0b89542e/download>>, accessed 9 March, 2025.

76. Ibid.



Dominican Republic

Child Sexual Exploitation, Sexually Explicit Conduct, and Related Offenses

Sextortion

Sextortion involves coercing an individual, often through threats to distribute intimate images, videos, or information, into providing money, further sexual material, or engaging in unwanted sexual acts.

Similar to grooming, the Dominican Republic does not have a specific criminal offense titled "sextortion." Cases must be prosecuted by combining elements from existing laws:

- **Law 53-07, Art. 16 (Chantaje / Blackmail):** This is the most directly relevant provision for technology-facilitated extortion. It penalizes using electronic systems to blackmail someone into providing funds, valuables, signatures, documents (digital or not), or access codes.⁷⁷ The applicability to demands for sexual acts or images, rather than just monetary/documentary items, may require interpretation.⁷⁸
- **Penal Code, Arts. 305-308 (Amenazas / Threats):** These articles address general threats, with penalties varying based on whether the threat is written or verbal, conditional or unconditional. While not detailed in the provided snippets, they form part of the Penal Code's structure⁷⁹ and could apply to the threatening element of sextortion.
- **Penal Code, Arts. 400-401 (Extorsión / Extortion):** General extortion offenses, likely involving obtaining property or signatures through force, violence, or coercion.⁸⁰ May apply if the demand is monetary, but might not fit perfectly with demands for sexual acts/images.
- **Penal Code, Art. 337 (Atentado a la Intimidad / Attack on Privacy):** Penalizes capturing, recording, or transmitting a person's image while they are in a private place, without their consent. This covers the non-consensual creation or initial acquisition of intimate material sometimes involved in sextortion.
- **Penal Code, Art. 337-1:** Critically, this article penalizes the act of conserving, disseminating to the public or a third party, or otherwise using recordings or documents obtained in violation of Art. 337 (i.e., without consent). This directly addresses the threat often central to sextortion – the non-consensual distribution of intimate material.
- **Law 53-07, Art. 21 (Difamación) & Art. 22 (Injuria Pública):** Applicable if the threat involves harming the victim's reputation through the dissemination of false or insulting information via electronic means.⁸¹

77. Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología. EL CONGRESO NACIONAL, <https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf>, accessed 9 March, 2025.

78. efectividad de la ley no. 53-07 sobre crímenes y delitos de alta tecnología, ante el - UAPA <<https://rai.uapa.edu.do/bitstream/handle/123456789/2540/EFFECTIVIDAD%20DE%20LA%20LEY%20NO.%2053-07%20SOBRE%20CR%20MENES%20Y%20DELITOS%20DE%20ALTA%20TECNOLOG%20C%208DA%20C%20ANTE%20EL%20TRIBUNAL%20DE%20ATENCI%20C%2093N%20PERMANENTE%20DEL%20DISTRITO%20JUDICIAL%20DE%20SANTIAGO%20C%20EN%20PERIODO.pdf?sequence=1&isAllowed=y>>, accessed 9 March, 2025.

79. Código Penal de la Republica Dominicana, <<https://www.oas.org/dil/esp/C%20C%20B3digo%20Penal%20de%20la%20Rep%20C%20BAblica%20Dominicana.pdf>>, accessed 9 March, 2025.

80. Ibid.

81. Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología. EL CONGRESO NACIONAL, <https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf>, accessed 9 March, 2025.



Victim Support Systems & Platform Accountability



Country Focus Indonesia

Lead Agencies

The Ministry of Women's Empowerment and Child Protection (Kementerian Pemberdayaan Perempuan dan Perlindungan Anak, KemenPPPA) plays a central role in child protection policy and coordination. The Ministry of Communication and Digital (Kementerian Komunikasi dan Digital, Komdigi, formerly Kominfo) leads on regulating the digital space, including content moderation and platform accountability. The Indonesian Child Protection Commission (Komisi Perlindungan Anak Indonesia, KPAI) is an independent body involved in monitoring, advocacy, and receiving complaints. Law enforcement agencies (Police) are responsible for investigation and enforcement.

Key Victim Support Laws/Policies

Indonesia's primary child protection law is Law No. 23/2002, amended by Law No. 35/2014 and Law No. 17/2016. These laws provide general protection against exploitation and abuse, including sexual abuse and coercion. Law No. 11/2008 concerning Information and Electronic Transactions (UU ITE), recently amended by Law No. 1/2024, addresses online crimes, including the distribution of content violating decency (Article 27(1)) and online coercion/stalking (Article 27B(1)). Law No. 44/2008 on Pornography criminalizes child pornography. Law No. 12/2022 on Sexual Violence Crimes (UU TPKS) outlines victim rights, including legal assistance and protection.

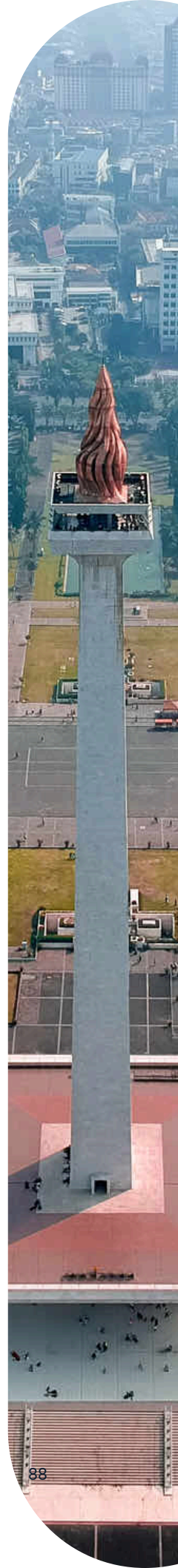
Indonesia ratified the Optional Protocol to the CRC on the Sale of Children, Child Prostitution and Child Pornography (OPSC) via Law No. 10/2012. The government is developing specific implementing regulations (RPP) under UU ITE, including the Draft Government Regulation on Child Protection in Electronic Systems (RPAPSE), focusing on age verification and parental consent.

Platform Takedown Mandates

UU ITE (Article 40) requires Electronic System Providers (PSEs) to prevent dissemination of prohibited content. The new Content Moderation Compliance System (SAMAN), operational from February 2025, mandates PSEs (including social media) to take down illegal content (pornography, terrorism, gambling etc.) upon receiving a Takedown Order Letter from Komdigi. Specific deadlines are imposed (24 hours for non-urgent, 4 hours for urgent content), with non-compliance resulting in fines administered through SAMAN.⁸² The RPAPSE aims to enforce age verification (e.g., under 18 requiring parental consent, potentially setting a minimum age like 13 or 17 based on platform risk assessments). UU ITE and the Pornography Law provide basis for prosecuting distribution of CSAM.⁸³

82. Terapkan SAMAN pada Februari 2025, Menkomdigi Perkuat Perlindungan Masyarakat di Ruang Digital, <<https://www.komdigi.go.id/berita/siaran-pers/detail/terapkan-saman-pada-februari-2025-menkomdigi-perkuat-perlindungan-masyarakat-di-ruang-digital>>, accessed 12 March 2025.

83. Building a Safer Digital World for Kids, <<https://ps-engage.com/building-a-safer-digital-world-for-kids-lessons-indonesia-can-learn-from-global-best-practices/>>, accessed 12 March 2025.



Victim Support

The legal framework, particularly following the passage of the Sexual Violence Bill (Law No. 12 of 2022), emphasizes the victim's right to treatment and recovery.

Available services, provided by both government (A key operational arm at the local level is the Unit Pelaksana Teknis Daerah Perlindungan Perempuan dan Anak (UPTD PPA)) and NGOs, aim to include:

Psychological/Counseling

Psychosocial support and mental health services are recognized needs. KemenPPPA budgets include funds for survivor rehabilitation.

Legal Assistance

Victims have the right to legal aid. Children are typically accompanied by service providers (NGOs or government agencies like UPTD PPA) throughout the legal process. The Witness and Victim Protection Agency (LPSK) provides support in cases involving threats.

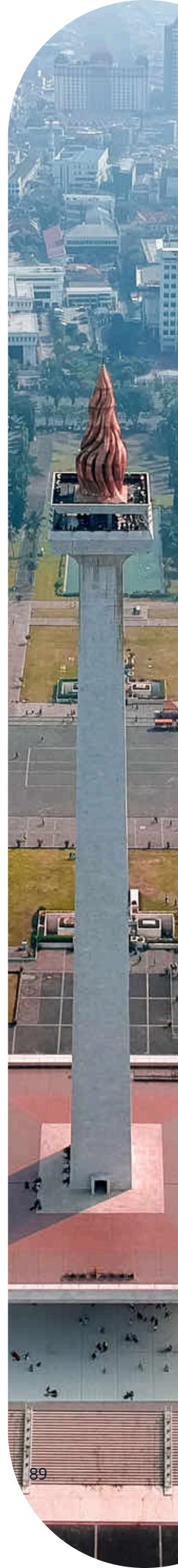
Rehabilitation/Reintegration

Services aim to cover rehabilitation and reintegration, especially crucial for survivors. This includes efforts to improve physical and mental health.

Restitution/Compensation

The right to restitution is acknowledged, particularly under laws related to trafficking (Law No. 21/2007) and further detailed in Supreme Court Regulation (Perma) No. 1 of 2022 regarding trafficking victims. This includes compensation for lost income, suffering, and treatment costs.

The LPSK plays a role in assessing and facilitating restitution requests. However, practical implementation faces significant hurdles. Challenges include the perpetrator's ability to pay, difficulties in assessing psychological harm, limited understanding of restitution rights among law enforcement, problems seizing assets, and suboptimal cross-agency coordination. Many victims are unaware of their right to claim restitution.



Victim Support

Victims and those reporting abuse can utilize several channels:

Government Hotlines/Reporting Systems

KemenPPPA operates the SAPA 129 call center (accessible via phone, WhatsApp, and the SEJIWA Mental Health Service line 119) for reporting violence against women and children. Simfoni PPA is the online data system. The National Police (Bareskrim Polri) manages Patolisiber.id for reporting cybercrimes, including CSAM.

Local Service Units

UPTD PPA are intended as the primary local government service points. Community-Based Integrated Child Protection (PATBM) exists in some areas for initial assistance and referral.

NGOs

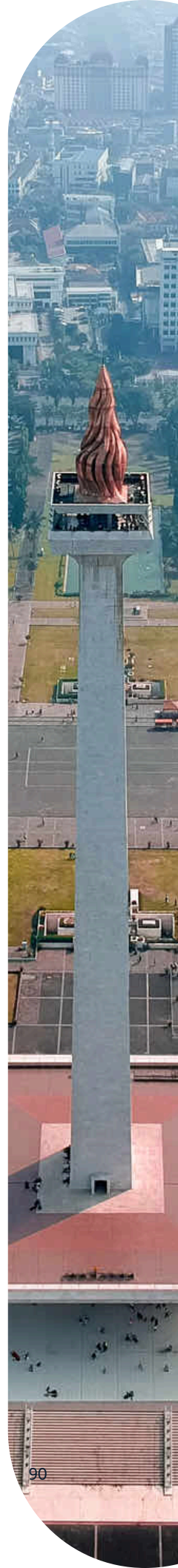
Organizations like ECPAT Indonesia and others provide direct support or facilitate access to services. The IWF/ECPAT portal allows anonymous CSAM reporting.

Law Enforcement

Direct reporting to Police PPA Units or Cyber Crime Units occurs, often followed by collaboration with service providers.

LPSK

Can be accessed via call center 1500-148 or WhatsApp for emergency hotline services and protection.





Despite those support channels, access remains a major issue. Research indicates children experiencing OCSEA rarely use formal channels like police or helplines, preferring to confide in friends or siblings. Key challenges include:

- **Limited Awareness:** Many children, especially vulnerable groups, and the general public lack knowledge of reporting mechanisms and available services. Awareness of online risks and safety measures is also low among children and caregivers.
- **Resource Constraints:** Government efforts are acknowledged but need to be more extensive. Support services, including UPTD PPA, suffer from insufficient human and budgetary resources. This limits their reach, particularly in remote areas, and the availability of trained professionals like clinical psychologists. Calls to increase prevention budgets have been made.
- **Service Quality/Accessibility Issues:** The SAPA 129 hotline has faced issues with long wait times, poor connectivity, lack of toll-free access, and confidentiality concerns. UPTD PPA are not established in every region, limiting nationwide access. Services may not cater specifically to children with disabilities or other vulnerable groups.
- **Stigma:** Stigma surrounding sexual violence discourages reporting by victims and families. A concerning belief persists among many children and caregivers that victims are at fault if their intimate images are shared.

A significant observation is the gap between Indonesia's legislative advancements and the on-the-ground reality of service delivery. While laws like the 2022 Sexual Violence Bill represent progress, the capacity of the designated service providers, particularly the UPTD PPA network, is hampered by foundational issues.

The recommendation to ensure UPTD PPA are established in every region and adequately resourced underscores that the intended primary government interface for victims is currently insufficient in its reach and capacity. This points to a system where policy intent outpaces implementation capability, leaving many victims without accessible or effective support, especially for the nuances of OCSEA which requires specialized knowledge.

Country Focus

The Philippines

Lead Agencies

The Department of Social Welfare and Development (DSWD) is a key agency, providing victim support and chairing the Inter-Agency Council on Violence Against Women and their Children (IACVAWC). The Department of Justice (DOJ) oversees prosecution, including through its Task Force on Child Protection. Law enforcement rests with the Philippine National Police (PNP) and the National Bureau of Investigation (NBI). The Department of Information and Communications Technology (DICT) is involved in policy implementation, monitoring ISPs, and online safeguarding policies. The Council for the Welfare of Children (CWC) also plays a role, including operating a helpline.⁸⁴

Key Victim Support Laws/Policies

The 1987 Constitution mandates state protection for children.³⁵ Republic Act (RA) 7610 (Special Protection Against Child Abuse, Exploitation and Discrimination Act, 1992) provides a foundational framework. RA 9775 (Anti-Child Pornography Act, 2009) specifically criminalized the creation, distribution, and possession of child pornography, including provisions on grooming and ISP liability.⁸⁵ RA 10175 (Cybercrime Prevention Act, 2012) addressed computer-related offenses, including child pornography committed through computer systems.⁸⁶ The most recent and significant law is RA 11930 (Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act, 2022), which strengthened previous laws by clarifying definitions, enhancing penalties, imposing stricter duties on electronic service providers (ESPs), internet intermediaries, and financial intermediaries (detection, reporting, preservation of evidence), and mandating multi-agency collaboration. The Implementing Rules and Regulations (IRR) for RA 11930 were signed in May 2023, crucial for its operationalization. 41 RA 9262 (Anti-Violence Against Women and Their Children Act, 2004) may also be relevant in domestic contexts.

Platform Takedown Mandates

RA 9775 mandated ISPs to install filtering software, report suspicious sites to NBI/PNP within 7 days, and block CSAM content upon notification. RA 11930 reinforces and expands these obligations for a broader range of ESPs and intermediaries, requiring proactive detection, reporting, and preservation of evidence of OSAEC/CSAEM. Specific takedown timelines (e.g., 48 hours for CSAM under RA 9775 after notification) are mandated.⁸⁷ The DICT and the National Telecommunications Commission (NTC) are tasked with monitoring compliance.⁸⁸ Private sector initiatives, like PLDT and Smart Communications blocking millions of CSAM web addresses, demonstrate industry action, potentially spurred by legal mandates.

84. DSWD calls on public to report violence vs women and kids in homes, communities as nation observes Women's Month, <<https://www.dswd.gov.ph/dswd-calls-on-public-to-report-violence-vs-women-and-kids-in-homes-communities-as-nation-observes-womens-month/>>, accessed 12 March 2025.

85. safeonline.global, <https://safeonline.global/wp-content/uploads/2023/12/DH_Philippines_advocacy_note_layout-1.pdf>, accessed 12 March 2025.

86. SC Affirms Conviction of Child Pornographer - Supreme Court of the Philippines, <<https://sc.judiciary.gov.ph/sc-affirms-conviction-of-child-pornographer/>>, accessed 12 March 2025.

87. Safe Online Global (N 85)

88. Philippine Department of Information and Communications Technology emphasises online child safety - OpenGov Asia, <<https://opengovasia.com/2021/02/20/philippine-department-of-information-and-communications-technology-emphasises-online-child-safety/>>, accessed 12 March 2025.



Victim Support

The Philippines offers a relatively broad spectrum of support services for OCSEA victims, facilitated by both government agencies and NGOs, though significant challenges in accessibility and effectiveness persist.

Psychological/Counseling

Trauma-informed care, psychosocial support, and mental health services are available through DSWD, NGOs like IJM, CPN (via WCPUs), Bantay Bata, Bahay Tuluyan, and CURE Foundation. The DOJ-DSWD partnership specifically includes psychosocial intervention.

Legal Assistance

Legal aid and support throughout the prosecution process are provided by the DOJ, Public Attorney's Office (PAO), CHR, IJM, and other NGOs. The use of recorded child victim interviews aims to reduce re-traumatization during legal proceedings.

Rehabilitation/Reintegration

This includes shelter (DSWD, NGOs like Bantay Bata, Bahay Tuluyan, CURE), medical care (often via WCPUs in hospitals supported by CPN, or NGOs like IJM, CURE), educational support (including Alternative Learning Systems - ALS), family interventions, and socio-economic services provided by various NGOs. Reintegration support is a recognized need but often deemed inadequate.

Restitution/Compensation

While the legal framework allows for restitution, ensuring victims actually receive court-ordered restitution or compensation from civil judgments is highlighted as a challenge and prioritized recommendation. A US court notably awarded restitution to two Filipino survivor victims in a specific case. The development of victim compensation guidelines was mentioned as a future plan in 2016.



Victim Support

Victims can access support through various routes:

Reporting

Reports can be made via the DSWD SMS hotline (3456) , directly to PNP (WCPC, ACG) or NBI units , through NGO hotlines like Bantay Bata 163, or via international channels like the NCMEC CyberTipline which are forwarded to Philippine authorities.

Support Provision

Services are delivered through government facilities (DSWD shelters, regional offices) , specialized police units (WCPC) , hospital-based Women and Children Protection Units (WCPUs) supported by CPN, NGO-run shelters and comprehensive programs , and specialized inter-agency task forces.

A Protocol for Case Management of Child Victims of Abuse, Neglect, and Exploitation exists to guide the process. The DOJ-DSWD referral program aims to link legal aid clients with psychosocial support.

The international prominence of the Philippines in OCSEA discussions creates a unique dynamic. This visibility attracts vital international funding, technical assistance, and partnerships (e.g., PICACC, collaborations with IJM, UNICEF, foreign law enforcement), which undoubtedly fuels the development of advanced laws and specialized units.

Yet, this same international focus results in an immense influx of reports, particularly through global channels like the NCMEC CyberTipline. The national response system, although relatively specialized, struggles under the weight of this volume due to resource constraints.

This suggests that capacity building must focus not only on enhancing sophistication but critically on expanding scale and resources to effectively process the high caseload generated by global awareness and reporting mechanisms directed towards the country.





Despite the breadth of services and pathways, significant hurdles remain:

- **Resource Constraints:** There is a persistent need for more trained anti-trafficking personnel, increased operational funding for task forces, and better digital forensic equipment to handle the high volume of cases. Funding for crucial community reintegration services is inadequate.
- **Victim Identification:** Authorities sometimes fail to consistently screen and identify trafficking victims, particularly in complex situations like online scam operations, leading to potential penalization of victims. Identifying victims of child pornography and child labor trafficking remains difficult.
- **Service Adequacy and Gaps:** Community reintegration services, including trauma-informed care and job training, are insufficient. There is a need for increased support for specialized care programs, particularly those tailored for OSEC victims.
- **Data Management:** The lack of a unified, reliable system for consolidating statistics on victim identification and assistance hinders effective monitoring and planning. A unified database for victims and perpetrators is needed.
- **Coordination:** While structures like IACAT, IACACP, and task forces exist, ensuring seamless coordination and systematic incorporation of survivor input into policy and program design requires strengthening.
- **Restitution:** Practical access to and enforcement of court-ordered restitution remains a significant challenge.⁸⁹
- **Reporting Barriers:** Broader research, including data from the Philippines, indicates that children experiencing OCSEA are unlikely to report to formal authorities like police or helplines (only around 3% in one multi-country study).⁹⁰ Disclosure is more common within informal networks like friends and family.⁹¹

89. 2024 Trafficking in Persons Report: Philippines - State Department, <<https://2021-2025.state.gov/reports/2024-trafficking-in-persons-report/philippines/>>, accessed on 13 March 2025.

90. Disrupting Harm - ECPAT, <<https://ecpat.org/disrupting-harm/>>, accessed on 13 March 2025.

91. disrupting harm - evidence-based actions to end online child sexual exploitation and abuse, <https://safeonline.global/wp-content/uploads/2024/11/Disrupting-Harm_Evidence-Based-Actions-Final.pdf?utm_campaign=Insight%20%26%20Foresight%20%7C%20December%202024&utm_medium=email&utm_source=Mailjet>, accessed on 13 March 2025.

Country Focus

Ghana

Lead Agencies

The Cyber Security Authority (CSA) is the primary agency, established by Act 1038, responsible for regulating cybersecurity activities, including child online protection. The Ministry of Gender, Children and Social Protection (MoGCSP) holds the mandate for overall child welfare, protection policy, and social protection interventions. The Ghana Police Service, particularly its Domestic Violence and Victim Support Unit (DOVVSU), handles investigation and victim support for domestic violence and abuse cases, including those involving children. The Ministry of Communications and Digitalisation oversees the broader digital sector. The Ghana Education Service (GES) is involved in school-based safety and digital literacy programs.⁹²

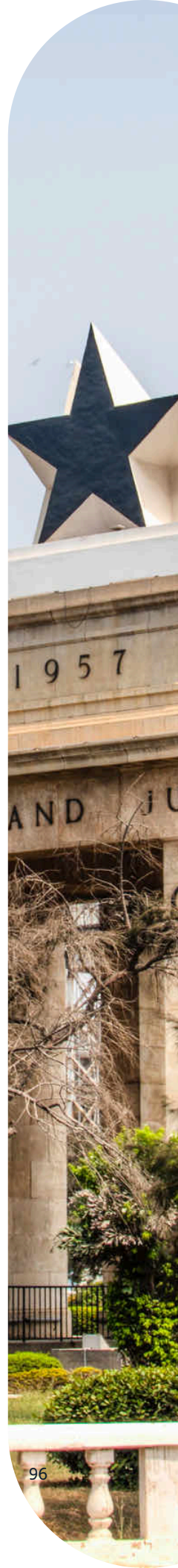
Key Victim Support Laws/Policies

The Cybersecurity Act, 2020 (Act 1038) is the cornerstone legislation for online safety. It establishes the CSA, defines and criminalizes various cybercrimes including specific child protection offenses like online grooming, enticement for sexual abuse, production, possession, publishing, sharing, and online streaming of CSAM, and non-consensual sharing of intimate images. Penalties can reach up to 25 years imprisonment. The Act also provides the basis for blocking and filtering illegal content. Supporting this is the National Child Online Protection (COP) Framework, which has been reviewed and updated in collaboration with UNICEF. Ghana also runs a National Cyber Security Awareness Programme (NCSAP) themed "A Safer Digital Ghana". Broader legal context includes the Children's Act, 1998 (Act 560), Juvenile Justice Act, 2003 (Act 653), Domestic Violence Act, 2007 (Act 732), and the Criminal Offences Act, 1960 (Act 29), although the Criminal Code may lack specific definitions for all online offenses.

Platform Takedown Mandates

Act 1038 explicitly authorizes service providers to block, filter, or take down content that undermines child protection online. The CSA is currently developing the legislative instrument (secondary regulations) for Act 1038, which will include provisions to hold non-compliant service providers accountable, specifically mentioning penalties for collecting children's data without parental consent and refusing to report harmful content against children. The CSA actively encourages the private sector and media to report harmful content. Act 1038 also mandates reporting of cybersecurity incidents to the relevant Computer Emergency Response Team (CERT) within 24 hours. Service providers are required to retain subscriber data for 6 years and traffic/content data for 12 months under certain conditions related to investigations.

92. CSA || News - Cyber Security Authority, <<https://www.csa.gov.gh/csa-children-online-engagement>>, accessed 13 April, 2025



Victim Support

Hotlines/Reporting

The CSA operates Cybersecurity/Cybercrime Incident Reporting Points of Contact (PoC), including a dedicated Child Online Protection Reporting Portal launched in October 2020 to facilitate reporting of CSAM, potentially directly to platforms like Facebook. The Ghana Police Service, particularly DOVVSU, has a helpline (055-100-0900). A general police hotline (18555) is also available. Other potential reporting points include the Orange Support Centre (GBV focus, 0800111222), the Legal Aid Commission, and NGO hotlines like Pearl Safe Haven.

Counseling/Psychological Support

DOVVSU provides referrals to clinical psychologists, social workers, and counselors attached to the unit. MoGCSP, through the Department of Social Welfare, likely offers psychosocial support as part of its mandate to protect vulnerable groups. NGOs such as Pearl Safe Haven may also provide counseling. The need for victim support services is recognized within the COP framework.

Rehabilitation/Long-term Care

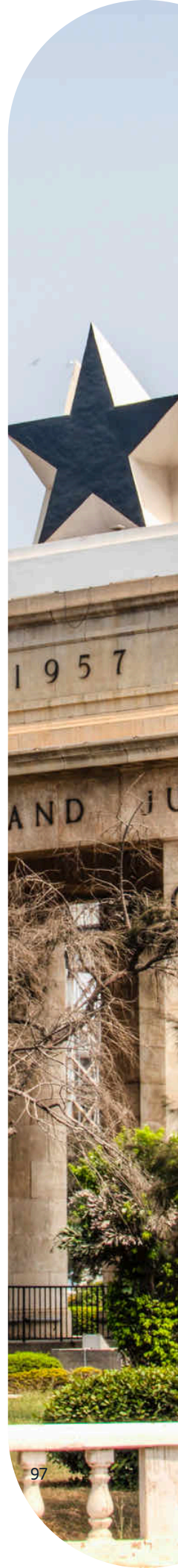
Specific programs for online harm victims are not detailed. MoGCSP oversees general social protection programs for vulnerable populations.

Legal Assistance

The Legal Aid Commission offers services to those in need. DOVVSU investigates and prosecutes relevant cases. Training for prosecutors on the COP provisions in Act 1038 is underway.

NGO Role

NGOs are integral partners. UNICEF provides significant support to the CSA, MoGCSP, and Police, including funding, technical assistance for reviewing the COP framework, establishing the first child protection digital forensics lab, capacity building for law enforcement and social workers, and awareness campaigns. The Ghana NGOs Coalition on the Rights of the Child (GNCRC), an ECPAT member, works on awareness and capacity building.





The system faces substantial challenges that significantly impede effective victim support:

- Severe Under-resourcing:** Support services specifically for CSEC survivors are described as "highly inadequate" primarily due to a lack of resources, insufficient staffing, and inadequate transportation.⁹³ The Police Cybercrime Unit's reporting point suffers from limited national visibility and under-resourcing. General resource constraints also affect broader anti-trafficking efforts, and helplines may face similar limitations.
- Low Awareness and Reporting:** Extremely low public awareness of OCSEA among the public, law enforcement, and even victims' families acts as a major barrier to identifying victims and encouraging reporting. Victim stigmatization further contributes to significant under-reporting. Children also report difficulty discussing online risks or experiences with caregivers.
- Capacity and Training Gaps:** A lack of specialized expertise, particularly in digital forensics for tracking online perpetrators, hinders investigations.⁹⁴ There is inadequate capacity among key professionals (police, prosecutors, judges, staff in CU and DOVVSU) to effectively prevent and respond to online abuse cases.⁹⁵
- Coordination:** While collaboration is recognized as essential, effective coordination between different agencies and with NGOs needs strengthening. The lack of uniform reporting standards makes assessing the effectiveness of units like DOVVSU difficult. Disruptions to informal information sharing due to COVID-19 also highlighted coordination vulnerabilities.
- Legal and Policy Gaps:** Despite the progress with Act 1038, gaps remain. The Act's definition of 'sexually explicit conduct' is unclear, and it lacks provisions for essential therapeutic support for victims. Prior to Act 1038, significant gaps in the legal framework were noted. Ghana has also not ratified the Optional Protocol to the CRC on the Sale of Children, Child Prostitution and Child Pornography (OPSC), leaving a gap in international legal commitments.
- Data Scarcity:** Historically, there has been a lack of comprehensive data on the prevalence and nature of online abuse in Ghana⁹⁶, although recent surveys by the CSA are beginning to provide some insights.⁹⁷

93. Ghana* - ECPAT, <https://ecpat.org/wp-content/uploads/2021/08/Ex_Summary_GHANA_FINAL.pdf>, accessed on 13 March 2025.

94. Ghana National Cyber Security Policy & Strategy - ITU, <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/National-Cyber-Security-Policy-Strategy-Revised_23_07_15.pdf>, accessed on 13 March 2025.

95. Child Online Protection | UNICEF Ghana, <<https://www.unicef.org/ghana/child-online-protection>>, accessed on 13 March 2025.

96. Ibid.

97. CYBERSECURITY IS A SOCIETAL PROBLEM WHEN IT COMES TO CHILD ONLINE PROTECTION – Dr. Antwi-Boasiako - CSA || News, <https://www.csa.gov.gh/csa_and_development_partners.php>, accessed on 13 March 2025.

Country Focus

Rwanda

Lead Agencies

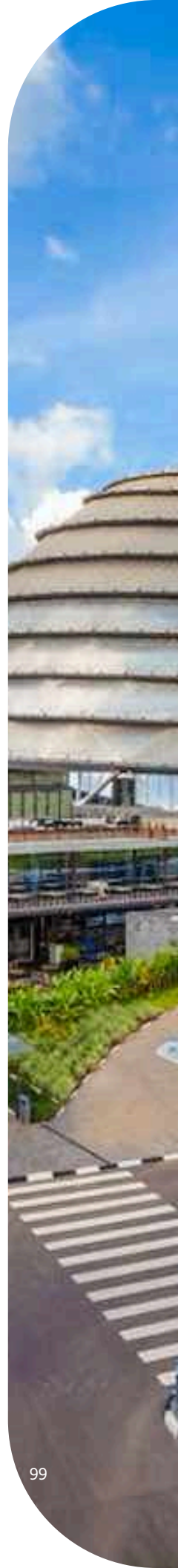
The Ministry of ICT and Innovation (MINICT) is designated as the lead coordinator for the Child Online Protection (COP) Policy and its implementation. The Rwanda Utilities Regulatory Authority (RURA) is likely involved in regulating ISPs and technical aspects. The National Cyber Security Authority (NCSA) likely contributes through the Rwanda Computer Emergency and Security Incident Response Team (Rw-CSIRT). The National Child Development Agency (NCDA), formerly the National Commission for Children (NCC), is the primary government body responsible for coordinating child protection and welfare programs. Law enforcement functions related to cybercrime and CSEA fall under the Rwanda Investigation Bureau (RIB) and the National Public Prosecution Authority (NPPA). The Ministry of Education (MINEDUC) and the Rwanda Basic Education Board (REB) are crucial for implementing school-based digital literacy and safety programs.

Key Victim Support Laws/Policies

The National Child Online Protection (COP) Policy, formally adopted in 2019, serves as the central strategic framework specifically addressing online risks for children. This policy aims to mitigate content, contact, conduct, and commercial risks through a multi-pillar approach covering institutional capacity, legal frameworks, response systems, technical controls, education, research, and international cooperation. General child protection is governed by laws such as Law N°54/2011 on the Rights and Protection of the Child. Laws addressing Gender-Based Violence (GBV) and sexual violence are also relevant, given the overlap between online and offline harm and the high prevalence of violence against children in Rwanda.

Platform Takedown Mandates

The COP Policy (Policy Area 4: Technical Controls) outlines specific mandates for platforms and ISPs. It requires establishing methods for notice and takedown of illegal Child Abuse Material (CAM) in collaboration with industry. Crucially, it includes provisions for legislation allowing local ISPs to block access to hosts that fail to remove notified illegal content. Service providers are required to implement flagging systems for users to report unsuitable content, alongside transparent and robust monitoring systems. Furthermore, the policy mandates government-led internet surveillance to detect content harmful to children, including the collection, analysis, and storage of abusive images for investigations, and the creation of a national database of digital images and cases of child abuse to monitor internet activity and link cases. This indicates a more direct government role in content monitoring and removal compared to solely relying on platform self-regulation or user reports.



Victim Support

Rwanda offers a notably integrated system for responding to child abuse and GBV, centered around the Isange One Stop Centre model, alongside community-level initiatives and a developing focus on online protection.

Comprehensive Integrated Services (via IOSC)

The Isange One Stop Centres are designed to provide a holistic range of services in a single, accessible location (usually district hospitals). These include:

- **Medical Care:** Including emergency contraception, HIV prophylaxis, STI prevention, general medical treatment, and specialized medical forensic examinations crucial for legal cases.
- **Psychosocial Support:** Counseling and psychological support provided by trained psychologists and social workers.
- **Legal Services:** Assistance with the legal process, potentially including representation.¹¹⁵ Victims of GBV are exempt from court fees.
- **Police Investigation:** Immediate involvement of Judicial Police Officers (JPOs) to start investigations.
- **Shelter & Relief:** Safe houses with basic provisions are available at IOSCs for immediate safety needs.
- **Reintegration Support:** IOSCs aim to provide follow-up and support for reintegration.¹¹⁵ These services are provided free of charge and are available 24/7.

Community-Level Support (via IZU)

The Inshuti z'Umuryango volunteers provide grassroots support, including promoting positive parenting, raising community awareness about child rights and protection issues, offering basic counseling to prevent conflict and violence, identifying and referring child protection cases (including abuse, neglect, exploitation) to appropriate services (like IOSCs or social workers), and supporting family reunification efforts.

Reporting Channels

Victims or witnesses can report through dedicated hotlines 115, directly to the police (RNP/RIB), at Isange One Stop Centres, or via community volunteers (IZU) or Child Protection Committees.

Legal Aid

Available through IOSCs and potentially through organizations like the Legal Aid Forum (LAF).





Rwanda's approach to victim support, particularly through the Isange One Stop Centre model, stands out for its integration and centralization of response services. This provides a strong mechanism for reacting to reported cases of GBV and child abuse with comprehensive, high-quality care.

The addition of the IZU network also offers a valuable layer of community-based prevention and referral.

Strengths: The IOSC model is widely recognized as a major strength, offering high-quality, integrated, multi-sectoral care that minimizes re-traumatization by bringing services to the victim. Its significant scale-up across district hospitals enhances geographical accessibility.

The strong legal and policy framework provides a solid foundation. The extensive network of trained IZU community volunteers provides a crucial link for prevention, identification, and referral at the grassroots level.

The formal adoption of the comprehensive COP Policy and Implementation Plan demonstrates proactive engagement with online risks. Collaboration between government agencies (Police, MIGEPROF, MINISANTE, MINIJUST) within the IOSC framework appears to be effective.

Challenges: Despite progress, the overall child protection system is still considered "emerging," and the number of children needing support continues to exceed the system's current capacity. Social pressures and stigma may still inhibit reporting of violence, despite available services.

While IOSCs are widespread, ensuring consistent quality and reach, particularly in remote or underserved areas, remains an ongoing challenge.⁹⁸ Assessing the real impact of initiatives like Gender Accountability Days faces difficulties.

Prior to the COP policy development, capability gaps related to understanding and addressing online-specific risks were identified, suggesting that building specialized knowledge for OCSEA across the system (including IOSC staff and IZUs) is crucial. Continuous awareness-raising and education about online dangers are needed for children, parents, and communities.

98. Rwanda: Trafficking | Ecolinet, <<https://www.ecolinet/en/file/local/2119887/rwandatrafficking2024final.pdf>>, accessed on 13 March 2025.

Country Focus

Dominican Republic

Lead Agencies

The National Council for Children and Adolescents (Consejo Nacional para la Niñez y la Adolescencia, CONANI) is the governing body for child protection policies. The Attorney General's Office (Procuraduría General de la República) is responsible for prosecution and provides victim assistance. The Dominican Institute of Telecommunications (Instituto Dominicano de las Telecomunicaciones, INDOTEL) regulates the telecom sector and is involved in initiatives related to internet access and safety. The Ministry of Education (Ministerio de Educación de la República Dominicana, MINERD) leads educational initiatives, including digital literacy programs. Law enforcement agencies (Police) are involved, but their specific role in online child protection is less detailed in the provided snippets compared to other countries.

Key Victim Support Laws/Policies

The primary legal framework is Law 136-03, the Code for the Protection of the Rights of Children and Adolescents. This law provides general protection but lacks specific, detailed provisions addressing the nuances of online sexual exploitation and abuse. A major identified gap is the absence of a dedicated, up-to-date National Action Plan specifically targeting the sexual exploitation of children (online or offline) since 2006. Existing national plans touching on the issue have expired. While a Policy for the Prevention and Attention of Early Unions and Adolescent Pregnancies was adopted in 2021, it reportedly lacks focus on the links between early unions and sexual exploitation.

A new Penal Code was pending approval (as of Sept 2022) which aimed to criminalize promoting the DR as a destination for child sex tourism, but it still lacked provisions for extraterritorial jurisdiction over most CSEA crimes committed by or against Dominican citizens abroad. The country has ratified the Convention on the Rights of the Child (CRC). The Committee on the Rights of the Child's 2023 observations highlighted the need for legal review, including banning corporal punishment, establishing a minimum age of sexual consent, criminalizing sexual exploitation, and applying a rights-based approach to protect girl victims of GBV.

Platform Takedown Mandates

Specific legal mandates compelling platforms or ISPs to detect, report, or remove CSEA/CSAM content within defined timeframes (similar to laws in the Philippines, Ghana, Rwanda, or Indonesia's SAMAN) are not clearly documented in the provided materials and appear to be a significant gap. Instead, the approach seems focused on collaboration. UNICEF/Plan International's project involves collaborating with Internet service providers (ISPs) to identify and remove online sexual exploitation content and raise awareness. This suggests reliance on voluntary cooperation rather than strong legal obligations with enforcement mechanisms.



Victim Support

Hotlines/Reporting

CONANI likely serves as a primary contact point for child protection issues. The Attorney General's Office handles prosecution and victim assistance. An existing helpline is being strengthened specifically for online violence cases through a UNICEF/Plan International project. The lack of a legal provision allowing anonymous complaints to initiate investigations is noted as a gap. While not confirmed for DR specifically, Child Helpline 116 is listed internationally.

Counseling/Psychological Support

CONANI coordinates psychological support for children affected by domestic violence, aiming for emotional recovery. The Attorney General's office provides victim assistance, potentially including counseling. NGO Destiny Rescue, active in the DR, provides aftercare services as part of its reintegration program, which likely includes psychosocial support.

Rehabilitation/Long-term Care

CONANI works on relocating and supporting children orphaned by violence against women within their extended families. Destiny Rescue offers reintegration programs for rescued children. Specific long-term care options focused on recovery from online harm are not detailed.

Legal Assistance

The Attorney General's Office provides victim assistance, which may encompass legal support. However, significant legal barriers exist, such as statutes of limitations for reporting sexual crimes against children 98 and insufficient access to compensation for victims through the justice system.

NGO Role

International NGOs appear to be major drivers of the response to online child safety issues. UNICEF and Plan International are jointly supporting the establishment and implementation of the national response board, building capacity of local actors, strengthening the helpline, raising awareness, and collaborating with ISPs. World Vision partners with CONANI and Indotel on promoting child rights online. Destiny Rescue is actively involved in conducting rescue operations, including for OSEC victims, and providing reintegration services. ECPAT provides critical analysis and advocacy on the legal and policy landscape.





Despite the existence of specialized units and protocols, several challenges impact the accessibility and effectiveness of services:

- **Resource Constraints:** CONANI, the lead agency, has faced historical underfunding, potentially limiting its capacity for coordination and service delivery. General resource limitations common in low- and middle-income countries likely affect the availability of trained professionals and the reach of services.
- **Coordination and Strategy:** While a protocol exists and a national response board is being formed, the lack of an updated national action plan specifically targeting CSEC (since 2006) suggests a potential lack of cohesive strategic direction.⁹⁹
- **Awareness and Reporting:** Raising public awareness about OCSEA and available services is an ongoing need. Under-reporting remains a likely issue due to stigma, fear, or lack of knowledge.
- **Legal Framework Gaps:** Significant gaps identified include the lack of extraterritorial jurisdiction for most CSEC offenses, hindering prosecution of crimes committed abroad by Dominicans or against Dominican children by foreigners. The absence of mandatory, government-regulated child protection standards for the tourism industry is also a major concern, given the country's status as a tourist destination.
- **Vulnerable Populations:** Children of Haitian descent and migrant children face heightened vulnerabilities due to potential barriers in accessing education, documentation, and protection services, increasing their risk of exploitation.

99. Dominican Republic | ECPAT, <https://ecpat.org/wp-content/uploads/2022/09/Eng-ECO_BRIEFING_Dominican-Republic_September2022_Final-1.pdf>, accessed on 13 March 2025.

Insights & Recommendations

A photograph of a diverse family of four—father, mother, and two young children—gathered around a laptop. The father, on the left, has a beard and is smiling. The mother, on the right, is also smiling and waving her hand. The two children, a boy and a girl, are both smiling and looking at the laptop screen. The girl is wearing a paper crown. The scene is warm and celebratory, with a wooden table and a glass of water visible in the foreground.

Insights & Considerations for Online Platforms

The digital environment, shaped by platforms like YouTube, TikTok, Instagram, and Snapchat, is a defining reality for children and adolescents globally. While these platforms offer rich opportunities for connection and creativity, they also expose young users to serious risks such as cyberbullying, grooming, child sexual exploitation and abuse (CSEA/CSAM), harmful content, and privacy violations. Despite policy commitments and safety tools, a significant gap remains between platform intentions and their practical enforcement.

A key concern is the inadequacy of current age verification practices, which often allow underage users unsupervised access to online spaces ill-suited for their developmental stage. Content moderation struggles with scale, nuance, and the limitations of artificial intelligence (AI), especially in managing emerging threats such as AI-generated abuse material. While proactive detection using AI/ML is promising, it often focuses on known CSAM and may overlook new materials or hidden abuse patterns amplified by algorithmic content delivery systems.

Importantly, in discussing advanced technologies, it is essential to distinguish between risks and safeguards. While generative AI poses novel harms, strong encryption plays a critical role in protecting children's safety online. Encryption helps secure personal communications, prevents unauthorized data access, and supports safer digital environments, particularly for marginalized or vulnerable children.

User reporting tools and parental controls remain limited in their uptake and effectiveness, often hampered by stigma, fear, or lack of digital literacy among children and caregivers. These challenges are echoed in diverse national contexts—such as Indonesia, the Philippines, Ghana, Rwanda, and the Dominican Republic—where mobile-first internet use, inconsistent legal frameworks, and under-resourced institutions further exacerbate risks.

Addressing these complex challenges requires a multi-pronged and collaborative response from platforms, policymakers, educators, parents—and critically, from children themselves.

"Parents and families have a big role to play in protecting children from online abuse because it is within the family that we nurture and educate them (children) values, help them to develop both physically and emotionally morality, psychology, and character of our children."

Prof. Jeannette Bayisenge, Minister of Gender and Family Promotion of Rwanda

14th Children's Summit and the World Children's Day in Rwanda, 2020.



Recommendations for Online Platforms

Prioritize Safety by Design

Embed child safety considerations into the core design and functionality of platforms, particularly algorithmic recommendation systems, rather than treating safety solely as a reactive moderation task. Conduct rigorous impact assessments of features on child well-being.

Strengthen Age Assurance

Invest in and implement more reliable, privacy-preserving age verification methods beyond self-attestation, potentially exploring tiered access or functionalities based on verified age bands.

Enhance Proactive Detection

Continue investing in sophisticated AI/ML capabilities to detect new and emerging threats, including novel CSAM, grooming behaviors, harmful challenges, and cyberbullying patterns. Address biases in training data and develop strategies for AI-generated content and E2EE environments.

Improve Moderation Processes

Increase resources for well-trained, culturally competent human moderators globally, providing robust mental health support.

Enhance training and quality assurance to improve the consistency and accuracy of moderation decisions.

Enhance Proactive Detection

Platforms should meaningfully involve children in the development and evaluation of safety features, such as through youth advisory panels that offer ongoing insights into digital trends and risks.

As digital natives, children often encounter emerging threats first.

Listening to their voices ensures platform responses remain relevant, effective, and aligned with global child rights standards, including Article 12 of the UNCRC and General Comment No. 25.



Recommendations for Online Platforms

Increase Meaningful Transparency

Commit to publishing regular, standardized, and independently verifiable transparency reports detailing child safety efforts.

Reports should include granular data on CSEA detection (proactive vs. reactive, known vs. new), grooming interventions, age verification enforcement, algorithm audits, and the effectiveness of reporting mechanisms, following established frameworks.

Simplify and Promote Reporting

Design reporting tools that are more intuitive and accessible, especially for children. Provide users with clear, timely feedback on the status and outcome of their reports.

Empower Users and Parents

Improve the usability and visibility of parental controls and safety settings. Develop and promote accessible educational resources for both children and parents on navigating platforms safely.



Recommendations for Policymakers/Governments

Modernize Legal Frameworks

Review and update national laws to explicitly address the full range of online risks (grooming, cyberbullying, sextortion, AI CSAM, livestreaming abuse), ensuring alignment with international human rights standards and imposing clear obligations on platforms. Consider legislation mandating Safety by Design principles.

Strengthen Enforcement & Oversight

Establish clear regulatory authority and provide adequate resources for monitoring platform compliance with child safety laws and policies. Enforce existing mandates (e.g., ISP/ESP reporting) and impose meaningful penalties for non-compliance.

Enhance Support Service

Increase funding, training, and capacity for national child helplines, specialized victim support services (including mental health), and law enforcement units dedicated to investigating online crimes against children.

Mandate Algorithmic & Data Transparency

Require platforms to conduct and publish regular, independent audits of their algorithms' impact on child safety and well-being.

Mandate transparency regarding data collection and use practices involving minors.

Invest in Nationwide Digital Literacy

Allocate substantial public funding for comprehensive digital literacy and online safety education, integrated into school curricula from an early age and delivered through community programs targeting children, parents, and educators. Ensure programs are inclusive and address the needs of vulnerable groups, including children with disabilities.

Support Research & Data Collection

Fund independent academic research to better understand children's online experiences, evaluate the effectiveness of platform safety measures and interventions, and monitor emerging risks. Improve national systems for collecting data on online harms affecting children.

Recommendations for Educators/Parents

Educate Proactively

Teach children age-appropriately about online risks, including recognizing grooming tactics, understanding privacy settings, dealing with cyberbullying, identifying misinformation, and knowing how and when to report concerns.

Foster Open Communication

Cultivate an environment where children feel safe and comfortable discussing their online lives—both positive and negative experiences—without fear of judgment or immediate punitive action. Listen actively and respond supportively.

Utilize Available Tools

Familiarize yourselves with platform safety settings and parental controls, implement them where appropriate, but understand their limitations and do not rely on them solely for protection.



Family Digital Plan



Model Responsible Digital Citizenship

Be mindful of personal online behavior, screen time, and sharing practices (including "sharenting"—sharing information about children online).

Stay Informed and Engaged

Keep abreast of the platforms children use, emerging online trends, and potential risks. Engage in ongoing learning about online safety.



References

- 2020 Trafficking in Persons Report: Philippines - State Department, https://www.state.gov/reports/2020-trafficking-in-persons-report/philippines__trashed/
- 2023 Key Threats to Digital Trade - CCIA, https://ccianet.org/wp-content/uploads/2024/10/CCIA_2024-NTE-Digital-Trade-Barriers-Asia-Pacific.pdf
- 2024 Trafficking in Persons Report: Philippines - State Department, <https://2021-2025.state.gov/reports/2024-trafficking-in-persons-report/philippines/>
- ACTION TO END CHILD SEXUAL ABUSE AND EXPLOITATION: - Unicef, <https://www.unicef.org/media/89096/file/CSAE-Report-v2.pdf>
- Access to Justice Interviews with Justice Professionals - Disrupting Harm, <https://ecpat.org/wp-content/uploads/2022/03/Indonesia-RA4-J.pdf>
- Achieving holistic services for victims of GBV and child abuse | HeForShe, <https://www.heforshe.org/en/solutions/achieving-holistic-services-victims-gbv-and-child-abuse>
- Afrouz, R. (2021). The nature, patterns, and consequences of technology-facilitated domestic abuse: A scoping review. *Trauma, Violence, & Abuse*, 24(2), 1-15. doi.org/10.1177/15248380211046752
- An act defining the crime of child pornography, prescribing penalties therefor and for other purposes - LawPhil, https://lawphil.net/statutes/repacts/ra2009/ra_9775_2009.html
- Asset Publisher - Octopus Cybercrime Community - The Council of Europe, https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/ghana/pop_up
- Backe, E., Lilleston, P., & McCleary Sills, J. (2018). Networked individuals, gendered violence: A literature review of cyberviolence. *Violence and Gender*, 5(3), 135-146. doi.org/10.1089/vio.2017.0056
- Bailey, J., & Burkell, J. (2021). Tech-facilitated violence: Thinking structurally and intersectionally. *Journal of Gender-Based Violence*, 5(3), 531-542. doi.org/10.1332/239868021X16286662118554
- Child Development, Protection and Promotion, <https://www.ncda.gov.rw/1/child-development-protection-and-promotion>
- Child Online Africa, <https://childonlineafrica.org/>
- Child online protection | UNICEF Dominican Republic, <https://www.unicef.org/dominicanrepublic/en/topics/child-online-protection>
- Child online protection | UNICEF Ghana, <https://www.unicef.org/ghana/child-online-protection>
- Child online protection | UNICEF Philippines, <https://www.unicef.org/philippines/topics/child-online-protection>
- Child Online Protection in Rwanda - 5Rights Foundation, <https://5rightsfoundation.com/wp-content/uploads/2024/10/cop-in-rwanda-report.pdf>
- Child Online Protection in Rwanda - Ohccu, <https://www.ohccu.co.uk/ohccu-projects-1/child-online-protection-in-rwanda>
- Child Online Protection in Rwanda - UEL Research Repository - University of East London, <https://repository.uel.ac.uk/download/1c4e37fa14d6b9f9e2ade14712746478eef40fe8b4f49f8380c47a12b3633daa/1351605/cop-in-rwanda-report.pdf>
- Child Sexual Abuse And Exploitation Prevention Interventions By Law Enforcement - ECPAT, <https://ecpat.org/wp-content/uploads/2024/11/Role-of-Law-Enforcement-in-Prevention-Case-Study-Indonesia.pdf>
- ChildFund Philippines ChildFund Philippines forges partnerships for safer internet, <https://childfund.org.ph/childfund-philippines-forges-partnerships-for-safer-internet/>
- COMPENDIUM OF GOOD PRACTICES IN ADJUDICATING TRAFFICKING IN PERSONS CASES IN ASEAN MEMBER STATES - Supreme Court, <https://sc.judiciary.gov.ph/wp-content/uploads/2024/12/Book-1-CACJ-WG-Trafficking-v1.8.pdf>
- CONANI: Consejo Nacional para la Niñez y la Adolescencia, <https://conani.gob.do/>
- Cyber Crime - Accra - Ghana Police Service, 2025, <https://police.gov.gh/en/index.php/cyber-crime/>
- Cybercrime Prevention Act of 2012 RA No 10175 — Bar - Respicio & Co. Law Firm, <https://www.respicio.ph/bar/2025/tag/Cybercrime+Prevention+A+ct+of+2012+RA+No+10175>
- CYBERSECURITY IS A SOCIETAL PROBLEM WHEN IT COMES TO CHILD ONLINE PROTECTION – Dr. Antwi-Boasiako - CSA || News, https://www.csa.gov.gh/csa_and_development_partners.php
- DATA INSIGHT 5 PROMISING GOVERNMENT INTERVENTIONS ADDRESSING ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE, <https://safeonline.global/wp-content/uploads/2023/12/Disrupting-Harm-Data-Insight-5-Promising-Government-Interventions-addressing-OCSEA.pdf>
- Disrupting harm - evidence-based actions to end online child sexual exploitation and abuse, https://safeonline.global/wp-content/uploads/2024/11/Disrupting-Harm_Evidence-Based-Actions-Final.pdf
- Disrupting Harm in Indonesia – Evidence on online child sexual exploitation and abuse - ECPAT, https://ecpat.org/wp-content/uploads/2022/09/DH_Indonesia_ONLINE_final.pdf
- Disrupting Harm in Indonesia – Evidence on online child sexual exploitation and abuse - Unicef, <https://www.unicef.org/innocenti/media/4141/file/DH-Indonesia-Report-2022.pdf>
- DISRUPTING HARM IN THE PHILIPPINES - ECPAT, https://ecpat.org/wp-content/uploads/2022/04/DH_Philippines_ONLINE_FINAL.pdf

References

- Dominican Republic - ECPAT, <https://ecpat.org/country/dominican-republic/>
- Dominican Republic - U.S. Department of Labor, https://www.dol.gov/sites/dolgov/files/ILAB/child_labor_reports/tda2006/dominicanrepublic.pdf
- Domestic Violence & Victim Support Unit – DOVVSU - Ghana Police Service, <https://police.gov.gh/en/index.php/domestic-violence-victims-support-unit-dovvsu/>
- ECPAT Summary Paper on Online Child Sexual Exploitation, <https://ecpat.org/wp-content/uploads/2021/05/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf>
- ECPAT Summary Paper on Sexual Exploitation of Children in Travel and Tourism, accessed on April 13, 2025, <https://ecpat.org/wp-content/uploads/2021/05/ECPAT-Summary-paper-on-Sexual-Exploitation-of-Children-in-Travel-and-Tourism-2020.pdf>
- Efforts to Prevent Online Sexual Abuse and Exploitation of Children (OSAEC) in the Philippines - ASEAN, https://asean.org/wp-content/uploads/2024/11/Evidence-of-CoP-in-Action-Report_2023.pdf
- Electronic Information and Transactions Law (Act No. 11/2008) [Undang-Undang Informasi Dan Transaksi Elektronik (UU No. 11/2008)] - CYRILLA <https://cyrilla.org/en/entity/d535u3b8bqb?page=2>
- Ending Online Child Sexual Exploitation and Abuse | UNICEF, <https://www.unicef.org/media/113731/file/Ending-Online-Sexual-Exploitation-and-Abuse.pdf>
- Encourage the Implementation of Victim Assistance Funds and Services for Victims of Sexual Violence - INFID, <https://infid.org/en/dorongan-implementasi-dana-bantuan-korban-dan-pelayanan-korban-kekerasan-seksual/>
- Face Your Peers: - Plan International, https://plan-international.org/uploads/sites/25/2022/03/youth_peer_educators_module_v3_pages.pdf
- Failing Women? Structural Violence's Relevance in Responses to Sexual Violence: A Case Study of Rwanda, <https://digitalcommons.fairfield.edu/cgi/viewcontent.cgi?article=1102&context=jogc>
- Final IOSC Evaluation Report_2013.docx - UN Women GATE, <https://gate.unwomen.org/EvaluationDocument/Download?evaluationDocumentID=3609>
- Formal support services and (dis)empowerment of domestic violence victims: perspectives from women survivors in Ghana - PubMed Central, <https://pmc.ncbi.nlm.nih.gov/articles/PMC10583341/>
- Ghana - ECPAT, <https://ecpat.org/country/ghana/>
- Ghana - Octopus Cybercrime Community - The Council of Europe, <https://www.coe.int/en/web/octopus/-/ghana>
- Ghana National Cyber Security Policy & Strategy - ITU, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/National-Cyber-Security-Policy-Strategy-Revised_23_07_15.pdf
- HANDBOOK ON SERVICE MECHANISMS FOR WITNESSES AND/OR VICTIMS OF TRAFFICKING IN PERSONS IN INDONESIA, https://indonesia.iom.int/sites/g/files/tmzbd1491/files/documents/01%20Handbook%20on%20Service%20Mechanisms%20for%20Witnesses%20and_or%20Victims%20of%20Trafficking%20in%20Persons%20in%20Indonesia%20%281%29.pdf
- ICE works with Philippine law enforcement to capture cybersex operators and rescue child victims, <https://www.ice.gov/news/releases/ice-works-philippine-law-enforcement-capture-cybersex-operators-and-rescue-child>
- IMPLEMENTATION OF LEGAL PROTECTION AGAINST CHILD RAPE VICTIMS IN THE FAMILY ENVIRONMENT (STUDY AT UPTD PPA SIDOARJO DISTRICT) - E-Journal Fakultas Hukum Universitas Bhayangkara Surabaya, <https://ejournal.fh.ubhara.ac.id/index.php/derecht/article/download/213/205/844>
- Improving Shelters for Child Victims of Trafficking in the Dominican Republic, <https://www.iom.int/news/improving-shelters-child-victims-trafficking-dominican-republic>
- Indonesia - Safeguarding Childhood, <https://safeguardingchildhood.com/safe-guarding-childhood/indonesia/>
- Indonesia: Law No. 12 of 2022 on Sexual Violence Crimes and Online Gender-Based Violence Against Women Legal Briefing September, https://www.icj.org/wp-content/uploads/2023/09/Briefing-Paper-on-OGBV_ENG.pdf
- Indonesians urged to report online child sexual abuse, <https://www.iwf.org.uk/news-media/news/indonesians-urged-to-report-online-child-sexual-abuse/>
- Information and electronic transaction law effectiveness (UU-ITE) in Indonesia, https://www.researchgate.net/publication/224251183_Information_and_electronic_transaction_law_effectiveness_UU-ITE_in_Indonesia
- Integration of Child Protection and Social Protection for Child Victims of Violence in Indonesia - Asean Social Work Journal, <https://www.aseansocialwork.com/index.php/asw/article/download/103/52>
- Inter-Agency Council Against Child Pornography (IACACP), https://www.childprotectionnetwork.org/wp-content/uploads/2019/09/PSB_2016-Support_against_Online_Child_Abuse_compiled.pdf
- LEAP-Report.pdf - Unicef, <https://www.unicef.org/sites/default/files/2020-04/LEAP-Report.pdf>
- LEGAL PROTECTION FOR VICTIMS OF HUMAN TRAFFICKING CRIMES - Journal of Law and Sustainable Development, <https://ojs.journalsdg.org/jlss/article/download/1513/1120/9757>
- Legal Protection for Children in Cases of Online Sexual Abuse: A Comparative Study - Jambe Law Journal, <https://mail.jlj.unja.ac.id/index.php/home/article/download/167/51>
- Ministry of Gender, Children and Social Protection, <https://www.mogcsp.gov.gh/>

References

- Montesanti, S. R., & Thurston, W. E. (2015). Mapping the role of structural and interpersonal violence in the lives of women: implications for public health interventions and policy. *BMC Women's Health*, 15, 100. doi.org/10.1186/s12905-015-0256-4
- NORC at the University of Chicago and the International Center for Research on Women (ICRW). (2022). Landscape analysis of technology-facilitated gender-based violence: Findings from Asia. USAID. pdf.usaid.gov/pdf_docs/PA00Z7GS.pdf
- Plan International. (2020). Free to be online? Girls' and young women's experiences of online harassment. Plan International. planinternational.org/uploads/2022/02/sotwgr2020-commsreport-en-2.pdf.
- Posetti, J., Shabbir, N., Maynard, D., Bontcheva K, and Aboulez, N. (2021). The Chilling: Global trends in online violence against women journalists. UNESCO. en.unesco.org/publications/thechilling
- Robinson, L., I, S. R., Ono, H., Quan-Haase, A., Mesch, G., Chen, W., Schulz, J., Hale, T. M., & Stern, M. J. (2015). Digital inequalities and why they matter. *Information, Communication & Society*, 18(5), 569– 582. doi.org/10.1080/1369118X.2015.1012532
- Shanahan, M. (2022). The mobile gender gap report 2022. GSM Association. gsma.com/r/wp-content/uploads/2022/06/The-Mobile-Gender-GapReport-2022.pdf.
- UNFPA Technical Division. (2021). Technology facilitated gender-based violence: Making all spaces safe. United Nations Population Fund. unfpa.org/sites/default/files/pub-pdf/UNFPATFGBV-Making%20All%20Spaces%20Safe.pdf.
- UNFPA (2022). The Virtual is Real. unfpa.org/events/the-virtual-is-real
- United Nations Children's Fund (UNICEF). (2023). Bridging the gender digital divide: Challenges and an urgent call for action for equitable digital skills development.
- UNICEF. data.unicef.org/resources/ictgenderdivide/.
- Vaughan C., Bergman S., Robinson A., Mikkelsen S. (2023). Measuring technology-facilitated genderbased violence: A discussion paper. UN Population Fund, New York. unfpa.org/publications/measuring-technology-facilitated-gender-basedviolence-discussion-paper

