# Building a digital environment designed with children in mind

An international best practices blueprint

5RIGHTS FOUNDATION

# About 5Rights Foundation

5Rights develops new policy, creates innovative frameworks, develops technical standards, publishes research, challenges received narratives, and ensures that children's rights and needs are recognized and prioritized in the digital world.

While 5Rights works exclusively on behalf of and with children and young people under 18, our solutions and strategies are relevant to many other communities. Our focus is on implementable change, and our work is cited and used widely around the world. We work with governments, intergovernmental institutions, professional associations, academics, businesses, and children so that digital products and services can impact positively on the lived experiences of children and young people.

MARCH 2026

# Foreword

The Convention on the Rights of the Child was adopted in 1989. The same year, the World Wide Web was invented and envisioned as a space where all users could engage as equals, free from traditional hierarchies and national control. This radical vision shaped the ethos of the emerging digital world, with early pioneers treating it as fact. By 2013 Google Executive Chair Eric Schmidt could confidently state that the online world 'is not truly bound by terrestrial laws'.[1] Yet by then, most children around the world were online, with commercial digital products and services increasingly mediating every aspect of their lives. Childhood, ignored by the libertarians of cyberspace, had been rapidly disrupted and fundamentally reshaped.

Today, the harms of an unregulated internet economy to children have crystallized, and AI has set the dial to supercharge them. Young people and their communities are clamoring for a reset. But reining in global companies requires a global approach, just as geopolitical competition for tech dominance reaches fever pitch. Under pressure, leaders are torn between letting go entirely and cracking down reactively, for example with blanket social media bans.

Thankfully, an alternative approach exists – one grounded in well-established international law and shared regulatory practice that eschews zero-sum games, is evidence-based, and has already been proven to deliver..

Five years on since the UN Committee on the Rights of the Child set out the framework for a child-rights respecting digital world, this report distills what pioneering policymakers, legislators, and regulators from all around the world have tried, tested, and refined to translate its guidance into sensible, enforceable law. Together it forms a comprehensive blueprint for coherent, tech-neutral, outcomes-based regulation that sets a floor for innovation building trust and catering to children by design and default.

It is possible to both protect and prepare children for a rapidly digitalizing world. It is possible to regulate tech so that both innovation and children can thrive. It is possible to work together towards global standards that ensure benefits accrue to all.

The era of free-for-all tech experimentation, with children as guinea pigs, must end. It is high time for governments to reassert themselves and do their duty – by children today and generations to come.

LEANDA BARRINGTON-LEACH
*5Rights Executive Director*

# Contents

# Executive Summary

In 2021, the world made children a promise with the adoption of General comment No. 25 to the UN Convention on the Rights of the Child, affirming that the rights enshrined in the most widely ratified human rights treaty in history apply fully in the digital environment.

Today, fulfilling that promise is more critical than ever. One in three internet users is a child,[2] and digital technologies increasingly mediate all aspects of their lives – from the classroom to the playground, from first friendships to how they see themselves. Given this reality, tech companies must meet the same baseline: to design all digital products and services likely to be accessed by or to impact children with their distinct rights, needs, and vulnerabilities in mind.

While legislation often tends to focus on the most egregious and visible harms, the underlying causes often remain unaddressed. From predatory business models commodifying children's attention[3] and social media platforms promoting harmful experiences[4] to educational technologies discriminatorily predicting children's outcomes[5] and AI-driven systems encouraging children to harm themselves,[6] children's experiences in the digital environment cannot be treated in isolation.

These harms stem from deliberate design, deployment, and governance choices driven by a persistent failure to prioritize children's rights and wellbeing over companies' profits.[7] Voluntary and self-regulatory approaches have enabled this pattern of exploitation to persist, failing to protect children when it matters the most.

To effectively protect children in the digital world, regulatory frameworks must therefore shift towards systemic risk management that addresses these underlying technological and commercial conditions. This approach requires tech companies to assess how their products may impact children and mitigate risks upstream, allowing children to safely enjoy the full benefits of the digital world.

Such due diligence is already standard across industries – from food safety to aviation and medicine – where products cannot reach the market without demonstrating safety.[8] When the law requires this same rigor from tech companies, evidence

shows that they increase privacy protections in children's default settings, redesign recommender systems, and restrict targeted advertising to children.[9]

So far, this rigorous approach remains fragmented across jurisdictions. Digital products and services children use, however, transcend geographic borders,[10] creating stark inequalities: children end up enjoying strong protections in some jurisdictions while their peers face exploitation and harm elsewhere when using the same products and services.

There is growing international consensus on how to address this fragmentation. Building on established best practices while raising the bar not only protects children but also benefits businesses.[11] Clear and consistent rules create a level playing field that reduces companies' regulatory burden and enables responsible innovation to thrive.[12]

**Part 1** of this report discusses common responses that fall short of implementing children's rights in the digital world as set out in UNCRC General comment No. 25.

**Part 2** expands on each of the 10 Regulatory Principles, providing clear justifications and practical examples for legislators to implement international best practices in their jurisdictions. The Annex provides an overview of existing frameworks that inform this blueprint.

## Fundamental Principles for the systemic protection of children

This blueprint reviews and builds on best practices that have emerged at the global, regional, and national levels to provide governments, policymakers, and regulators with a comprehensive framework for implementing children's rights in the digital world. By identifying common elements of best practice, it sets out 10 mutually reinforcing regulatory principles:

1. Explicitly protect children, as every individual below the age of 18.
2. Protect children across all digital spaces they are likely to access or be impacted by.
3. Make children's best interests a primary consideration.
4. Requiring age assurance to provide children with age-appropriate experiences.
5. Mandate Child Rights Impact Assessments (CRIAs).
6. Embed privacy and safety by design and default.
7. Prohibit practices likely to contribute to known harms.
8. Ensure published terms are available, age-appropriate, and upheld.
9. Mandate responsible business conduct.
10. Establish effective enforcement mechanisms.

# Introduction

The digital world has transformed childhood, bringing with it incredible new opportunities but also new risks. As one-third of all internet users globally[13] and a significantly greater proportion in Global Majority countries,[14] children, defined as all individuals under the age of 18,[15] are often among the earliest adopters of new and emerging digital technologies.[16]

The *United Nations Convention on the Rights of the Child* (UNCRC) – the most widely ratified human rights treaty in history – has long established obligations to protect children's rights. In 2021, the UN Committee on the Rights of the Child's *General comment No. 25* clarified how children's rights apply in relation to the digital environment. Building on developments in data protection, online safety, and most recently artificial intelligence (AI), there has been growing global momentum to address the impact of digital technologies on children and ensure their safe and meaningful participation.[17]

Yet, despite this progress, children continue to be exposed to preventable and foreseeable risks as technology advances at speed, largely without due regard for children, and their rights, safety, or best interests.

Responses that treat online risk solely as a matter of content removal overlook the root causes of these risks. They ignore how companies' systemic design choices – such as algorithmic amplification, engagement-driven business models, and opaque recommendation systems – prioritize commercial profit, while magnifying harm at scale.[18]

Technology is evolving quickly, often outpacing the ability of regulators to respond. Fortunately, legislators can leverage well-established principles in product safety and recent progress in privacy, data protection, online safety, and AI governance to establish foundational safeguards.

To build a digital environment designed with children in mind, this blueprint draws on international, regional, and national legislation, regulation, and policy across these areas to provide policymakers with actionable recommendations and practical examples to fulfil the duties set out in the UNCRC and its accompanying *General comment No. 25*. It establishes baseline safeguards to mitigate risks before harm occurs, recognizing that a minimum bar of safety, privacy, and protection from commercial exploitation

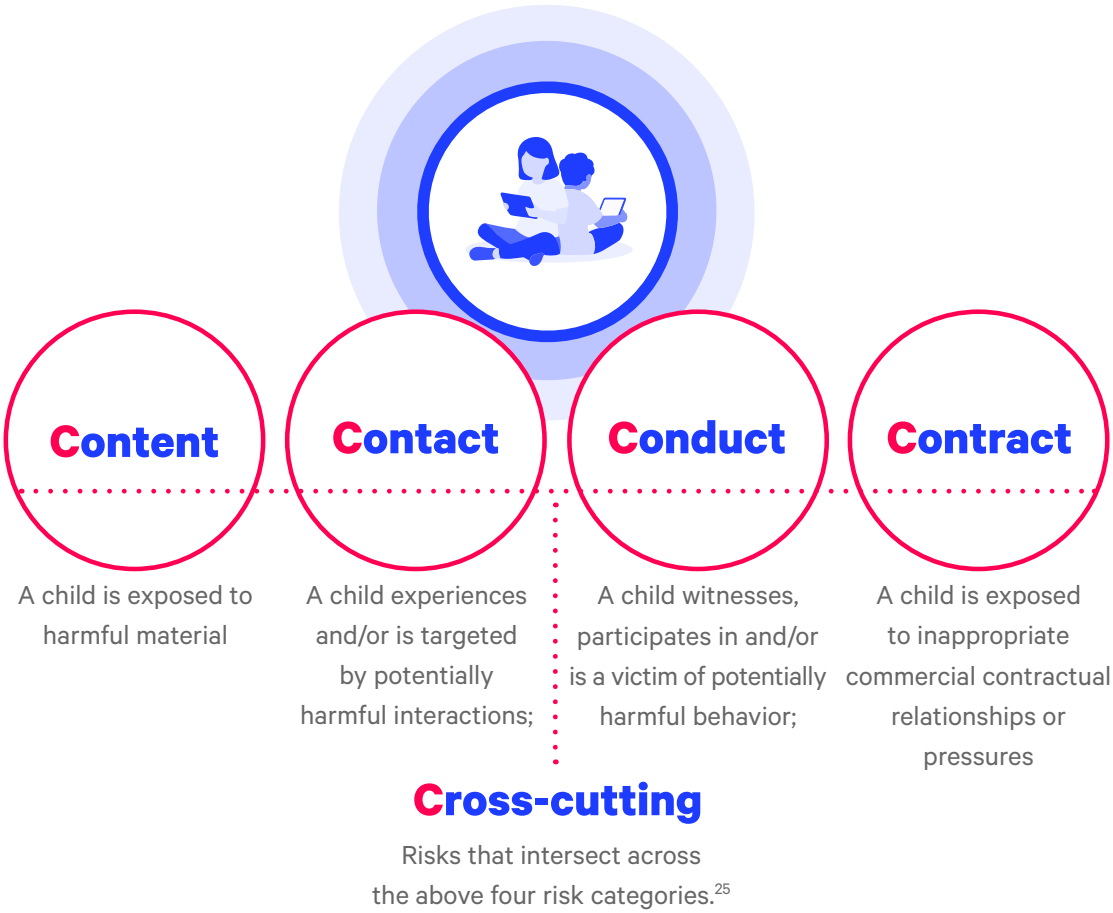
is foundational for the realization of children's rights online. The blueprint offers a comprehensive and replicable approach to build coherent regulatory frameworks that are systemic, technology-neutral, and future-proof in protecting children by design and default.[19]

**In 2024, all UN Member States unanimously recommitted in the Global Digital Compact to '[s]trengthen legal and policy frameworks to protect the rights of the child in the digital space'.[20] This blueprint is the roadmap to deliver on that commitment.**

## How does the digital world expose children to risks and harms ?

The digital world exposes children across the world to risks and harms at increasing pace and scale,[21] disproportionately affecting children in countries with limited safeguards and those from marginalized and minoritized communities.[22]

These risks are well documented and internationally recognized. The 5Cs typology of risks has become a cornerstone in global policy discussions,[23] being formally referenced across key international frameworks.[24]




Technology is not neutral – it reflects the values, biases, and priorities of those who design and deploy it. Therefore, these risks are not simply the result of individual behavior or the actions of bad actors. 5Rights' research demonstrates how deliberate design choices that prioritize commercial interest drive children towards risks on the digital products they rely on for their education, healthcare, entertainment, civic engagement, and relationships with friends and family.[26]

Common design strategies – including infinite scroll, autoplay, oversized opt-in buttons, ephemeral content, and constant notifications – encourage users to give up more of their time and attention to maximize engagement, often at the expense of their wellbeing.[27] This manipulation is pervasive, with 99% of websites and apps using deceptive design to manipulate users for commercial gain.[28]

These design strategies also contribute to impulsive use and decision-making, creating tensions between social pressures and concerns for children's safety and privacy.[29] They notably do so 'by removing all intuitive moments to end or finish a task, also known as "stopping cues" (endless scrolling, flashes of high-relevance content that are immediately hidden as the newsfeed reloads), autoplay by setting goals for users, like "streaks", and playing into loss of self-control'.[30]

The digital world does not merely fail to cater to children's needs – it intentionally predates on their vulnerabilities. While children have the right to not be commercially exploited,[31] tech companies continue to aggressively target them as a lucrative user group.[32] For example, Meta reportedly considers 8 to 12-year-olds a 'valuable but untapped audience',[33] while Google is expanding its presence in schools to create a 'pipeline of future users'.[34] Additional research reveals that 90% of websites directed to children embed one or more trackers,[35] and deceptive design patterns are significantly more prevalent on digital products and services aimed at children than on those intended for the general population.[36]

Whistleblower testimony confirms the deliberate nature of tech companies' prioritization of their own interests. Frances Haugen revealed that Meta systemically ignored its own internal data demonstrating Instagram exacerbates body image problems for 1 in 3 teen girls.[37] Similarly, internal documents reveal that TikTok intentionally targets users under 13 as a 'critical demographic', despite its own research showing users only need 35 minutes on the app to form a habit that 'correlates with a slew of negative mental health effects'.[38]

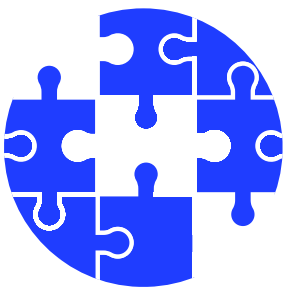
These examples demonstrate that many online harms are preventable, not inevitable. A product safety approach – long established in other industries – requires anticipating harm rather than reacting to it and building in baseline safeguards. This makes safety and privacy the default and holds those who design, develop, and deploy technology accountable for anticipating, identifying, and mitigating risks before products reach children. This blueprint equips policymakers and regulators with the tools to implement this approach.

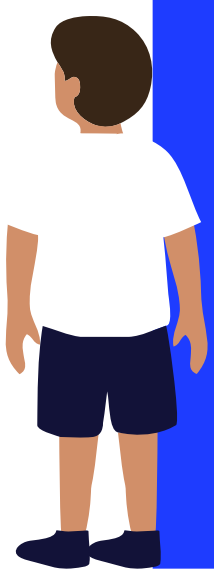
# Methodology

This blueprint is based on a mapping and legal analysis of over 50 global, regional, and national legislation, regulation, and policy documents across all continents. These frameworks were analyzed against the principles set out in UNCRC *General comment No. 25* and other established benchmarks to identify replicable best practices to implementing children's rights in the digital world.[39] The policy recommendations detailed in Part II were anchored in the latest thinking from international organizations, civil society organizations, and academia through a review of the relevant literature.

The Annex to this report provides an overview of leading frameworks from around the world reviewed for this report. Spanning continents and covering tech policy from child online safety and data protection to AI governance, these frameworks reflect how leaders worldwide are rising to the challenge of embedding children's rights and safety in the digital age.

PART 1





PART 1

# Incomplete approaches

Despite the increasing attention reflected in the analyzed documents, our review shows that international efforts have often been fragmented. Interventions have focused on the most salient harms or adopted reactive content-based approaches: relying on notice-and-takedown, proactive detection, and mandatory reporting of harmful and illegal content. While such measures remain necessary and can contribute to a safe and rights-respecting digital world for children when applied within a comprehensive and upstream approach, they are insufficient to create a digital world designed with children's rights, needs, and safety at its core.

This section highlights the shortcomings of responses that push superficial technological fixes or focus on symptoms rather than root causes. Often promoted by technology companies to shift responsibility away from themselves, these ultimately fail to ensure accountability for how digital products and services are designed, developed, and deployed.[40]

Instead, this section emphasizes the urgent need for comprehensive and systemic solutions to address the multifaceted risks the digital world poses to children, as outlined in Part II. A proactive and upstream approach holds tech companies accountable for embedding children's rights, safety, and privacy in the design of digital products and services.

# 1. Limited scope

'Many [safety] changes are inconsistent across platforms, and some can be easily bypassed. True digital safety should not rely on individual settings but be embedded as a core principle in every platform.'

GUSTAVO, 17, NICARAGUA[41]

Legislative frameworks that are narrow in scope offer a limited and fragile response to the risks children face online. By applying only to certain categories of services - often social media – or targeting only the largest platforms, such approaches create significant regulatory gaps.

This fragmented scope creates a false impression of safety. Harmful practices persist or migrate to less regulated spaces, while companies structure or rebrand services to avoid obligations altogether. Focusing solely on scale or category fails to reflect the interconnected nature of the digital environment and undermines the principle that children's rights should be respected consistently, regardless of the size, function, or business model of the service they use.

Indeed, risks to children are not exclusive to social media: they are present across all digital products and services, including those claiming to support children's education.[42] Research shows that EdTech systematically harvests children's data to feed commercially exploitative business models[43] and create a 'pipeline of future users'.[44] Similar dynamics are present in AI systems, video games (often excluded from enforceable regulatory frameworks),[45] Internet of Things devices, and other new and emerging technologies.

Crucially, whether children should be safe and have their rights respected does not depend on a company's size, market share, or user base. Due diligence and risk mitigation requirements should therefore apply to all digital products and services likely to be accessed by or impact children – not only those with a significant number of child users.[46]

## Content-focused responses

'I think one thing that can feel unsafe online is when platforms recommend extreme or harmful content just because of what you clicked before. It can easily lead young people into stuff they didn't want to see'

PARMENAS, 23, KENYA

Children have the right to be safe online. Yet tech companies systematically violate their rights by designing products and services that expose them to vast amounts of harmful and illegal content, from extreme violence and self-harm to eating disorders and substance abuse. Depending on where they live, up to 3 in 4 children have encountered harmful content online,[47] and such occurrences are increasingly frequent.[48] This exposure is not accidental. It is the direct result of deliberate and systemic design choices embedded within platform architecture.[49]

Tech companies intentionally design digital products and services to optimize engagement metrics, including time spent, reach, and activity at the expense of children's rights and wellbeing.[50] Recommender systems and ranking algorithms are structurally calibrated to prioritize content that provokes strong emotional responses, routinely amplifying negative, sensational, or extreme material by design.[51] As a result, children are recommended harmful content within hours.[52] Notably, 5Rights research demonstrates that children can go from a simple search for 'slime' to porn in a single click, or from trampolining to pro-anorexia in just 3 clicks.[53]

Beyond algorithmic amplification, tech companies optimize recommender systems to promote emotionally provocative content and exploit social pressures to encourage message sharing,[54] further accelerating the spread of harmful or illegal content, misinformation, and disinformation. Tech companies have knowingly suppressed efforts to address polarization,[55] as they are commercially incentivized to promote false information – which spreads faster and further and generates more profit than accurate content.[56]

In response, legislative efforts frequently concentrate on the identification and removal of illegal or harmful content[57] – an approach that is currently more globally coordinated than system-level interventions.[58] While necessary, content removal approaches are inherently narrow in scope. They manage visible symptoms rather than the underlying

design choices,[59] failing to address the cumulative harm of such content, the broader range of online risks and the flawed architecture and design of digital services.[60] [61]

The rapid deployment of artificial intelligence systems further exacerbates this dynamic at scale. AI significantly increase the ease of generating large volumes of content, often through systems without built-in mitigation mechanisms. As a result, the detection and removal of illegal and harmful content becomes increasingly complex and resource-intensive.[62] At the same time, these design gaps enable the large-scale creation of persuasive disinformation and illegal or harmful content that can be indistinguishable from human-generated content[63]at unprecedented scale, speed, and minimal cost.[64]

Under international law, businesses have a clear responsibility to prevent their digital products and services from causing or contributing to children's rights violations.[65] Content-focused policies and regulations should therefore be strengthened to require companies to assess and address risks arising from the design, functionalities, and business model of their services to be age-appropriate and rights-respecting by design and default.[66] In so doing, tech companies must be required to address the full range of online risks, as per the 5Cs classification[67] rather than relying on reactive content moderation alone.

# 2. Consent

'I think that many times the companies make those consents very confusing. That's why many people just accept them, because they don't want to read a 7 pages long document.'

SARA, 15, SLOVENIA

Tech companies have transformed children's privacy into a tick-box exercise. Despite deliberately embedding risky features in the design of digital products and services, producing terms and conditions that would take around 17 hours to read,[68] and designing deliberately complex settings tech companies routinely shift the burden onto children and their families, expecting them to 'consent' to the collection, processing, profiling, and monetization of their personal data. These practices are inherently unfair, exploit power imbalances, and obscure the real consequences of data use.[69]

Genuine consent must be informed – with information presented in an age-appropriate manner according to children's evolving capacities – freely given, and obtained up-stream, not assumed or buried in dense legal text.[70] Yet, consent in its current form is not fit for purpose in the digital age. The assumption that children can meaningfully consent does not reflect the scale, opacity, or complexity of today's digital environment.[71] It places an unrealistic burden on children to navigate deliberately opaque technical information,[72] despite often lacking the developmental capacity to assess risks or understand long-term consequences,[73] and does not incentivize tech companies to improve their data practices.

Consent is particularly rarely informed or freely given when access to education, social life, or entertainment is conditional on agreeing to invasive and manipulative practices. This particularly impacts children from less privileged socio-economic backgrounds who often rely on free versions of digital products and services, which are generally more data invasive.[74]

Tech companies also exploit the social pressures children feel to fit in with their peers, making refusal feel impossible.[75] Research with children confirms that they cannot meaningfully engage with their privacy rights in a digital environment optimized for opacity and commercial exploitation. Rather than being informed by an understanding

of consequence, their choices are shaped by social pressures, platform incentives,[76] and the feeling that they must consent to participate.[77]

Finally, relying on parents to consent on behalf of their children is similarly inadequate, as demonstrated by the failure to meaningfully implement the *Children's Online Privacy Protection Act* (COPPA) in the United States. Published terms frequently exceed the average adult's capacity[78] and do not provide certain key information up-front,[79] precluding them from providing informed and meaningful consent. Shifting this responsibility onto parents also undermines children's agency,[80] and creates a tension between parents' desire to protect their children and allowing them to participate.[81]

# 3. Digital literacy

'We can't expect a seven-year-old to outwit a system designed by a thousand PhDs to be addictive.'

NOEL ARMANDO, 19, PANAMA

Tech companies frequently promote education and digital literacy programs as an attempt to shift responsibility for children's online safety onto children, their families, and education systems.[82]

While States should support children's understanding of the digital world, including awareness of the commercial exploitation inherent to most digital products and services,[83] education alone fails to address systemic risks. It places an unfair burden on parents and educators and diverts attention from the core responsibility of tech companies to design products and services that respect children's rights, safety, and privacy by design and default.[84]

In addition, relying on digital literacy programs places the financial burden on States – and thereby taxpayers – to develop and deliver these initiatives, while tech companies continue profiting from products and services they deliberately design to be risky.[85]

It is entirely unrealistic to expect children to safely navigate an environment built to prey on their vulnerabilities. Digital literacy, while needed, does not and cannot replace product safety.

# 4. Safety tools

'Platforms carry the heavier responsibility. They're engineered to hijack attention; blaming individuals alone is unfair.'

MUEEZ, 16, PAKISTAN

Another way tech companies frequently seek to outsource their responsibilities is by expecting parents and children to navigate and mitigate the very risks intentionally designed into digital products and services.[86] Instead of mitigating these risks, companies offer so-called safety tools, frequently marketed as empowerment features that give users control over their digital experiences. However, the promise of agency – including opting-out of risky features[87] – remains illusory as long as tech companies deliberately design and deploy risky digital products and services that expose children to harm.

Tools such as blocking, muting, disabling comments, and screen time prompts can support children's safety as part of a wider set of mitigation measures. However, these alone do not reflect a comprehensive and holistic by-design approach, and policymakers increasingly recognize that these tools, while useful, are insufficient.[88] Instead, they respond to harm after it has occurred and place the burden solely on children and their parents.

Additionally, research shows that these tools typically restrict the ability to make meaningful changes beyond binary access decisions[89] and are rarely efficient.[90] For example, a systematic review of Instagram's teen safety features found that two-thirds are either substantially ineffective or nonexistent.[91]

## Parental controls

Academic research shows that parental controls have low adoption and efficacy rates because tech companies fail to account for parents' and children's expectations.[92] Yet companies continue to overpromote parental controls as a solution, despite evidence they can pose risks to children's rights, safety, privacy, and autonomy when relied upon as a primary safeguard.[93]

Research directly supported by tech companies concludes that 'the low adoption rate [of parental controls] could indicate that parents are overwhelmed and struggle to adopt such a wide array of tools, let alone use them effectively'.[94] Parents themselves report not using parental controls because they 'don't always work as promised, offer little context about how settings affect gameplay and force binary choices that don't align with household rules or with children's maturity levels'.[95]

When in use, parental controls rarely improve children's digital experiences and can even cause harm. Parents of children who died by suicide as a result of social media were monitoring their children's activities and setting time limits but reported that these measures were often detrimental.[96] Parental controls can also provide a false sense of security, undermine children's autonomy, and prevent children from accessing age-appropriate experiences – particularly in relation to identity formation.[97]

Finally, parental controls are particularly ineffective on devices and accounts shared between adults and children. Because this practice is particularly prevalent in less privileged and marginalized groups, relying on parental controls to protect children in the digital world disproportionately affects already vulnerable children.

If used, parental controls should be age-appropriate, support children's agency,[98] and respect children's rights, evolving capacities, and best interests.[99] Whenever parental controls are in use, children should receive warnings in language they can understand, without manipulative nudges that encourage them to weaken the settings.

# 5. Access Restrictions

'Talking to a lot of my peers, many of them dislike the idea [of access restrictions] because they feel restricted. They'd rather prefer those social media platforms to be changed and regulated in a way that keeps them safe instead of them being blocked out.'

NIDHI, 16, INDIA

To address tech companies' failure to design with children in mind, legislators across the world are increasingly considering measures to prevent children under a certain age from accessing certain categories of digital products and services – often focusing on social media.[100]

Besides the significant challenges in implementing and enforcing such measures, general access restrictions fail to address tech companies' harmful business models and practices, nor do they create better or safer spaces for children. Instead, these approaches may disincentivize tech companies – both those within and beyond the restriction's scope – from providing age-appropriate and rights-respecting digital experiences for children.[101]

Importantly, restricting children's access to certain services on the basis of age is distinct from ensuring that age-dependent protections or obligations embedded in existing laws, regulations, and companies' terms of service are effectively implemented and enforced. As highlighted by the OECD, such measures are often unclear or inconsistent in their application and are frequently poorly implemented and enforced in practice, undermining effective protection for children in the digital world.[102]

As further emphasized in Principle 2 in this blueprint, it is entirely insufficient for tech companies to claim in app stores or published terms that users must be above a given age without meaningfully implementing this restriction. The United States' COPPA illustrates this problem. It sets the age of 13 as the threshold for requiring parental consent for children's data collection – a cutoff based on political negotiation rather than psychological evidence[103] that fails to recognize the rights, developmental needs, and vulnerabilities of older children.

Poor implementation and enforcement of COPPA and similar laws have allowed tech companies to evade their responsibilities through ineffective disclaimers in the product or terms of use stating the product or service is not intended for users below a certain age.[104] No matter their stated intentions, companies must be held accountable for the privacy and safety of the children using or impacted by their digital products and services.

Beyond implementation and enforcement challenges, blocking children's access to certain digital products and services without ensuring rights-respecting alternatives risks limiting the fulfillment of their rights to information and participation.[105] As the digital environment takes an increasingly central position in children's lives, accessing safe and age-appropriate digital technologies is crucial to realizing the full breadth of children's rights.[106]

States must ensure children have safe and meaningful access to the digital world.[107] However, tech companies have made the fulfilment of this right dependent on the commercial surveillance and exploitation of children, eroding their privacy, safety, critical thinking, and agency.[108] In implementing the regulatory Principles outlined in this blueprint, legislators should ensure their efforts promote the full range of children's rights, including to participation and non-discrimination.[109]

Targeted access restrictions can be a crucial component of age-appropriate design. Tech companies are responsible for ensuring all digital products, services, and features accessible to under 18s respect children's rights and are safe by design and default. Therefore, age-appropriate access restrictions can be implemented through evolving default settings, with features and functionalities only becoming available to children once they reach a given age.

To this end, digital products and services within a restriction's scope are typically expected to deploy age assurance measures to prevent underage users from gaining access. Principle 4 outlines the role of age assurance in providing children with age-appropriate experiences.

# 6. Transparency

'Nowadays, it is hard to protect ourselves in the digital world, and even harder to navigate it for children. In such times, those responsible for creating safe digital spaces must understand that these spaces should be created by respecting children.'

MARIAM, 15, ARMENIA

As highlighted in Principle 8, transparency is a foundational element for holding tech companies accountable and scrutinizing their practices and compliance. Yet in practice, companies limit or manipulate transparency by presenting information in an opaque manner, including through underreporting or overreporting.[110]

Furthermore, transparency can be weaponized to shift responsibility onto children and their caregivers.

Transparency can support children's protection by informing decisions about engagement with the digital world. For example, product placements and influencer marketing should be clearly identifiable.[111] Similarly, the use, purpose, and potential impact of AI systems should be understandable by children.[112] However, tech companies should not be allowed to continue embedding risky and manipulative practices into the design of their products and services simply because they are being transparent about it.

Transparency alone is insufficient. To meaningfully hold tech companies accountable for respecting children's rights, transparency must be accompanied by enforceable obligations, independent oversight, and effective enforcement mechanisms.

PART

PART 2

# Fundamental Principles for the systemic protection of children in the digital world

This blueprint is grounded in *General comment No. 25* to the UNCRC and builds on global, regional, and national developments – including those outlined in the Annex.

Taken together, these best practices suggest a set of interdependent Principles for establishing a baseline of protection for children in the digital world. These foundational measures should be reflected in all legislative and regulatory efforts, creating a framework for responsible innovation that builds the digital environment children deserve.

These tech-neutral and end-to-end Principles provide policymakers, regulators, and civil society with the tools to comprehensively protect children and their best interests in the digital world, from setting policy frameworks to strengthening enforcement.

REGULATORY PRINCIPLE 1

# Explicitly protect children, as every individual below the age of 18.

'I believe the most important thing that policymakers can do is remember that we are children. We're not adults yet.'

SKYE, NIGERIA & USA, 14

The digital world was built on the assumption that all its users would be treated as equals.[113] However, this one-size-fits-all approach systematically fails to account for children's distinct needs, vulnerabilities, and rights.

The UNCRC enshrines distinct rights for every individual below the age of 18.[114] It is essential to reflect this definition of children in all digital and tech legislation as it guarantees recognition of children's long-established rights.

Practical Examples

**United Nations**, *Convention on the Rights of the Child*, (1989): 'a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier' (art. 1).

**Organisation for Economic Co-operation and Development (OECD)**, *Recommendation of the Council on Children in the Digital Environment*, (2021): 'Children' refers to every individual below the age of eighteen years' (I(ii)).

**African Union**, *Child Online Safety and Empowerment Policy*, (2024), 'Child: Any person under the age of 18, as per the United Nations Convention on the Rights of the Child' (p. 2).

**Rwanda**, *Child Online Protection Policy*, (2019): 'Under Article 1 of the UN Convention on the Rights of the Child, children are generally recognized as persons under the age of 18; in Rwandan law (N°54/2011 OF 14/12/2011), a child is any person under the age of eighteen (18) years old' (p. 3).

## Recognizing children's diversity and evolving capacities

While the definition of children as all individuals under the age of 18 is a cornerstone of children's rights, it is important to recognize that children are not a homogenous group. Significant disparities exist both between and within different jurisdictions.

Children in developing countries run considerably higher risks of harms and lower levels of participation in the digital world than their peers living in developed countries.[115] Within jurisdictions, certain children experience a higher level of risk due to intersecting vulnerabilities, including a child's or their parents' race, gender, religion, political opinion, national, ethnic or social origin, or disability status.[116]

Significant differences also exist between children at various stages of development.[117] *General comment No. 20* to the UNCRC clarifies that 'the implementation of rights should take account of children's development and their evolving capacities'[118] without compromising their status as rightsholders under the UNCRC. The principle of children's evolving capacities can be summarized as the duty to empower children's agency as soon as possible, while protecting them as long as possible.[119]

Recognizing these evolving capacities,[120] certain jurisdictions distinguish between children and adolescents in their domestic legislation, ensuring both groups are considered as rightsholders under the UNCRC.

Practical Examples

**Brazil**, *Sanctioning administrative procedure against TikTok*, (2024): 'a child [is] a person up to twelve years of age, and an adolescent [is] a person between twelve and eighteen years of age' (para. 9.5).

**Mexico**, *Code of good practices to guide the online processing of Personal Data of children and adolescents*, (2020): 'Girl or boy: Any human being under twelve years of age.' (p. 63); 'Adolescent: A person between the ages of twelve and under eighteen' (p. 62).

REGULATORY PRINCIPLE 2

# Children must be protected across all digital spaces they are likely to access or be impacted by.

'I feel like AI is like Pandora's box because it is sent out to the world. It's never going to be fully restrained and compacted.'

HAYDN, 20, UK

Children's rights are inalienable, unconditional, and apply wherever children are.[121] In the digital world, all products and services likely to be accessed by or to impact children must therefore be safe, privacy-preserving, and respect children's rights by design and default.

Tech companies should not interpret this obligation narrowly as applying only to products directed at children or products whose terms and conditions do not exclude them. Rather, they should assess whether children are likely to access their products and services by considering diverse factors.[122]

Moreover, legislation should also apply to digital products and services that are likely to affect children indirectly.[123] This is notably the case when AI systems are trained on children's data, shape children's experiences, and generate outcomes or influence decisions likely to impact children.[124] Similarly, Internet of Things devices routinely collect and process information about unsuspecting bystanders with no relationship to the provider.[125]

Children should be recognized and protected as the digital environment and technologies continue to evolve. Therefore, legislation should be technology-neutral and future-proof.

Practical Examples

**African Union**, *Child Online Safety and Empowerment Policy*, (2024): 'The Policy will provide a strong framework for the implementation of children's existing rights in the digital environment, including by the private sector and other stakeholders making products or offering services likely to be accessed by children' (p. 5).

**Philippines**, *Guidelines on Child-Oriented Transparency* (2024): 'This Advisory applies to all PICs and PIPs engaged in the processing of children's personal data, whether in a digital or physical environment. It covers products or services specifically intended for children or likely to be accessed by children' (Section 1).

**Indonesia**, *Government Regulation on the Governance of Electronic System Operations for Child Protection*, (2025): 'Products, Services, and Features... include:

**A.** Products, Services, and Features that are specifically designed for use or access by Children; or

**B.** Products, Services, and Features that are likely be used or accessed by Children' (article 4(1)).

If, however, technology companies refuse or are unable to provide a safe, privacy-preserving, and age-appropriate digital product or service to children, they must ensure that children cannot access it. As further expanded in Principle 4, such limits on children's activities should be lawful, rights-respecting, proportionate, and necessary.[126]

REGULATORY PRINCIPLE 3

# Children's best interests must be a primary consideration.

'To the tech industry, I ask: Are you building platforms for young people, or just using them?'

GINIKACHUKWU, 17, NIGERIA

Research reveals that children's rights, safety, and privacy are systematically jeopardized as technology companies prioritize profit over children's best interests, with designers pressured to create products that commodify children's attention.[127] Tech companies' own research frequently demonstrates the impact of risky design,[128] yet in the absence of legal frameworks demanding accountability, they continue to prioritize commercial interests over children's rights and wellbeing.

As set out in the UNCRC and clarified in its accompanying *General comments Nos. 14, 16, and 25*, children's best interests must be taken into account as a primary consideration in all decisions affecting them, including in the design, development, and deployment of digital products and services likely to be accessed by children.[129]

Prioritizing the best interests of the child requires comprehensive consideration grounded in children's rights. Companies cannot selectively interpret or cherry-pick rights.[130] Whenever commercial objectives conflict with children's rights, companies have a duty to respect, protect, and fulfill these rights over commercial interests.[131]

Determining children's best interests requires accounting for their evolving capacities and specific characteristics, as clarified in *General comment No. 20* to the UNCRC.[132] Academic research and regulatory guidance outline generalized age groups, recognizing that child development is neither linear nor homogenous.[133] Importantly, older children are not necessarily less vulnerable as they typically experience reduced parental supervision and increased risk-taking behaviors.[134]

Practical Examples

**United Nations**, *General comment No. 25 on children's rights in relation to the digital environment*, (2021): 'States parties should ensure that, in all actions regarding the provision, regulation, design, management and use of the digital environment, the best interests of every child is a primary consideration' (para. 12).

**Organisation for Economic Co-operation and Development (OECD)**, *Recommendation of the Council on Children in the Digital Environment* (2021): 'Actors, in all activities concerning children's participation in, or engagement with, the digital environment, should [...] Uphold the child's best interests as a primary consideration' (II(1)).

**Canada**, Resolution of the Federal, Provincial and Territorial Privacy Commissioners and Ombuds with Responsibility for Privacy Oversight - *Putting best interests of young people at the forefront of privacy and access to personal information*, (2023): '[T]he concept of the best interests of the child [...] implies that young people's well-being and rights be primary considerations in decisions or actions concerning them directly or indirectly'.

**Indonesia**, *Government Regulation on the Governance of Electronic System Operations for Child Protection*, (2025): '"Best interest of Children" means in all phases of development up to the phase of operation of Products, Services, and Features, Electronic System Operators must prioritize the fulfilment of Children's rights and Child protection as referred to in the laws and regulations'.

**Australia**, *Basic Online Safety Expectations*, (2022): 'The provider of the service will take reasonable steps to ensure that the best interests of the child are a primary consideration in the design and operation of any service that is likely to be accessed by children' (para. 6 (2a)).

## Best interests determination

Consideration of children's best interests is essential when resolving potential tensions between different rights. In such cases, a best interests determination must be conducted to determine which rights take precedence. These are the obligations of States and cannot be delegated to technology companies.[135]

While crucial to this determination, children's views do not automatically represent their best interests.[136] For example, children in Brazil report feeling resigned to privacy risks they perceive as ubiquitous,[137] which may contribute to their increasing willingness to share data for digital rewards – such as progressing to further levels in online games.[138] Children's views must be duly considered, but States may ultimately decide not to follow them if doing so would jeopardize children's best interests.[139]

Practical Examples

**Association of Southeast Asian Nations (ASEAN)**, *Guidelines for Harmonised and Comprehensive National Legislation Against All Forms of Online Child Sexual Exploitation and Abuse,* (2023): 'They will follow the principle of proportionality in resolving conflicts between conflicting children's rights or children's rights and human rights more broadly, while applying the principle of the best interests of children as a primary consideration' (p. 4).

**African Union**, *Child Online Safety and Empowerment Policy* (2024): 'Member States are encouraged to ensure that, in all actions regarding the provision, regulation, design, management and use of the digital environment, the best interests of every child is a primary consideration. In considering the best interests of the child, all children's rights must be regarded, including their rights to seek, receive and impart information, to be protected from harm and to have their views given due weight, and ensure transparency in the assessment of the best interests of the child and the criteria that have been applied' (Guiding Principle 1a).

REGULATORY PRINCIPLE 4

# Age assurance should be used to provide children with age-appropriate digital experiences.

'[A perfect digital world] would provide access to high-quality, age-appropriate content that fosters learning, creativity, and social connections while ensuring privacy and protection from harmful influences.'

ANDREI, 19, ROMANIA

Tech companies have long claimed they could not identify their users' age.[140] Yet they deploy sophisticated mechanisms to estimate users' ages for targeted advertising or personalized content,[141] while often failing to implement similar measures to provide children with age-appropriate experiences.[142]

Age assurance – an umbrella term for both age verification and age estimation solutions – allows tech companies to recognize the presence of children and to act accordingly. Far from a silver bullet, age assurance must be understood as a potential mitigation measure within a child rights approach to the digital environment.[143]

Any age assurance method must be lawful, rights-respecting, risk-based, and proportionate.[144] This entails that age assurance should only be implemented when necessary to protect children's rights, and that the selected age assurance mechanism must be appropriate to the level and the nature of the risks children may face.

When a service is appropriate for all users – including children – there should be no requirement to establish users' ages. However, when services or functionalities present risk to children, companies should implement age assurance mechanisms commensurate with those risks. In practice, this may require the implementation of

a layered approach for specific features that are likely to expose children to risk rather than across entire services.[145]

Such age assurance measures must support children's rights and preserve children's privacy by design and default,[146] minimizing data collection to what is strictly necessary to establish a user's age or age range and using it only for this purpose.[147]

### Guidance on age assurance

Age assurance and verification methods vary in their levels of effectiveness and accuracy. International best practices for rights-respecting, privacy-preserving, and proportionate age assurance are outlined in 5Rights' *But how do they know it is a child?*[148] and enshrined in the *IEEE 2089.1-2024 Standard for Online Age Verification*:[149]

- Protect the privacy of users in accordance with applicable laws, including data protection laws and obligations, in particular the principle that the minimum amount of data necessary is collected.
- Be proportionate to the risks arising from the product or service and to the purpose of the age assurance system.
- Offer functionality appropriate to the capacity and age of a child who might use the service.
- Be secure and prevent unauthorized disclosure or security breaches.
- Not use data gathered for the purposes of the age assurance system for any other purpose.
- Provide appropriate mechanisms and remedies for users to challenge or change decisions if their age is wrongly identified.
- Be accessible and inclusive to users with protected characteristics.
- Not unduly restrict access of children to services to which they should reasonably have access, for example, news, health, and education services.
- Provide sufficient and meaningful information for a user to understand its operation, in a format and language that they can be reasonably expected to understand, including if they are a child.
- Be effective in assuring the actual age or age range of a user as required.
- Not rely solely on users to provide accurate information.

Practical Examples

**International Age Assurance Working Group**, *Joint statement on a common international approach to age assurance*, (2024): 'Where it is inappropriate or unlawful for children to be accessing a website, providers should focus on deploying an effective means of age assurance to prevent children from accessing the site' (Principle 5).

**International Telecommunications Union (ITU)**, *Child Online Protection Guidelines*, (2020): 'Implement technology that can identify the age of users and present them with a version of the application that is age appropriate. … Where possible, use age verification to limit access to content or material that, either by law or policy, is intended only for persons above a certain age. Companies should also recognize the potential for misuse of such technologies to restrict children and young people's right to freedom of expression and access to information or endanger their privacy' (pp. 32-33).

**Organisation for Economic Co-operation and Development (OECD)**, *Towards digital safety by design for children*, (2024): 'Age assurance should not be used only to bar children from adult services, but as far as possible should be used to deliver age-appropriate experiences. Age assurance mechanisms should be equitable, inclusive and reflect risk. Laws and regulations that require age assurance should be tech neutral, leave room for innovation, and not be overly prescriptive. Solutions should be principles-based, for example focusing on accuracy, usability, privacy and proportionality' (p. 31).

**Brazil**, *Digital Statute of the Child and Adolescent* (ECA Digital), (2025): 'Providers of information technology products or services aimed at children and adolescents, or likely to be accessed by them, must adopt mechanisms to provide age-appropriate experiences … while respecting progressive autonomy and the diversity of Brazilian socioeconomic contexts' (art. 10).

REGULATORY PRINCIPLE 5

# Child Rights Impact Assessments (CRIAs) must be mandated.

'[In a perfect digital world], all digital services consider the presence of child users. They also have appropriate designs for them by default.'

ALIASKAR, 18, KAZAKHSTAN

Unlike in other industries – from aviation to food safety – tech companies often address risks to children reactively, rather than anticipating and preventing them through rights-respecting design. This reactive approach exposes children to preventable risks and harms, exploitative practices, and addictive design features because companies fail to demonstrate their products and services are safe, effective, and reliable before they reach the market.

This requires a systematic risk assessment: a proactive process to anticipate the potential impact of design choices, evaluate them against the rights and best interests of the child, and take necessary measures to prevent harms before they occur in the first place.

The international framework is clear. Under the UN *Guiding Principles on Business and Human Rights*[150] and the UNCRC, companies have a responsibility to conduct Child Rights Impact Assessments (CRIAs) and identify, prevent, and mitigate risks to children's rights upstream.[151] *General comment No. 16* to the UNCRC outlines fundamental principles for conducting CRIAs,[152] while UNICEF's D-CRIA toolbox provides guidance for tech companies to conduct these assessments.[153]

CRIAs enable tech companies to evaluate the entire user journey and identify how their business models, features, functionalities, and algorithms might support or harm children's rights, safety, privacy, and wellbeing.[154] Companies must conduct CRIAs before deploying products and services, whenever they design new features, and at regular intervals. These assessments must consider how children of varying ages

and vulnerabilities effectively or likely interact with the service and identify risks – whether from individual features or combinations thereof, intentional or not[155] – with mitigations integrated within the design and development process from the outset.[156]

Beyond child protection, tech companies have clear commercial incentives to undertake CRIAs. By enabling preventative action to mitigate harms, they reduce costs and reputational damage that arise when risks are addressed ex post.[157] CRIAs also help identify design and default improvements, as well as positive features or functionalities that can enhance children's rights. When released publicly, these assessments also contribute to consumer and investor trust by fostering transparency and accountability.

CRIAs can be subdivided into narrower exercises, where appropriate. For example, Data Protection Impact Assessments (DPIAs) are mandated by the Brazilian *General Data Protection Law*, the EU's *General Data Protection Regulation*, the India *Digital Personal Data Protection Act*, and the UK's *Age Appropriate Design Code*.

Finally, tech companies should conduct impact assessments when retiring digital products and services, including AI systems.[158] These evaluations should notably address how children's personal information will be destroyed, how loss of access will impact children, as well as the repercussions on other digital products and services children rely on.[159]

Practical Examples

**United Nations**, *General comment No. 25 on children's rights in relation to the digital environment*, (2021): 'States parties should require the business sector to undertake child rights due diligence, in particular to carry out child rights impact assessments and disclose them to the public, with special consideration given to the differentiated and, at times, severe impacts of the digital environment on children' (para. 38).

**UNICEF**, *Guidance on AI and children*, (2025): 'State parties should require companies to undertake child rights due diligence, particularly child rights impact assessments, which should then be disclosed to the public. … This would ensure business stakeholders carry out impact assessments and are barred from arguing a plausible assertion of ignorance of threats' (p. 15).

**Brazil**, *Digital Statute of the Child and Adolescent* (ECA Digital), (2025): 'In cases of processing data of children and adolescents, … the controller … must … prepare an impact, monitoring, and evaluation report on personal data protection' (art. 16).

**European Union**, *Guidelines on measures to ensure a high level of privacy, safety and security for minors online*, (2025): 'Where a provider of an online platform accessible to minors is deciding how to ensure a high level of safety, privacy and security to minors on its platform, and determining the appropriate and proportionate measures for that purpose, the Commission considers that that provider should, at a minimum, identify and take into account:

**A.** How likely it is that minors will access its service …

**B.** The actual or potential impact on the privacy, safety and security of minors that the online platform may pose or give rise to …

**C.** The measures that the provider is already taking to prevent and mitigate these risks.

**D.** Any additional measures that are identified in the review as appropriate and proportionate to ensure a high level of privacy, safety and security for minors on their service.

**G.** The potential positive and negative effects on children's or other users' rights of any measure that the provider currently has in place and any additional measures' (para. 18).

**European Union**, *General Data Protection Regulation* (GDPR), (2016): 'Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data' (art. 35).

REGULATORY PRINCIPLE 6

# Privacy and safety must be embedded by design and default.

'A safer, fairer digital world requires systemic change. Platforms must embed safety and privacy into their design [and] Governments must set clear standards that uphold children's rights.'

GINA, 17, EGYPT

Digital products and services are frequently designed in ways that exploit children's developmental vulnerabilities, prioritizing profit and engagement over children's rights, dignity, and wellbeing. These harms are not accidental. They are the foreseeable outcome of tech companies' deliberate design choices.[160]

Tech companies' extractive business models rely on the systematic harvesting of children's data on a massive scale – collecting far more personal data from children than is necessary to provide their services or that is in children's best interests.[161] To facilitate this commercial exploitation, companies configure default setting not to provide children with a high level of privacy and safety but to collect as much of their personal data as possible. With over 95% of users keeping default settings unchanged,[162] tech companies are amassing children's personal data on a scale and level of detail that users seldom realize. Alarmingly, by the time a child is 13, over 72 million pieces of personal data will have been captured about them.[163]

This data is then systematically shared with third parties which profile children for purely commercial purposes. Personal data is 42% more likely to be shared with advertisers on apps intended for children,[164] resulting in 79% of the 1 000 most popular apps likely to be used by children collecting and sending their personal information to advertisers.[165]

Privacy- and safety-by-design approaches, widely recognized internationally since 2010,[166] hold tech companies accountable for these choices. These systemic approaches require them to address risks proactively and embed privacy in design and default settings,[167] just as other industries design with children in mind, ensure rigorous safety standards, and remove unsafe products from the market.[168]

Privacy and safety must be the default outcome of product design, with risks to children's rights identified and addressed before harm occurs.

Accordingly, States must take legislative measures to ensure tech companies set children's data protection, privacy, and safety settings to the most protective level by default. If modified, these settings should revert to the most protective level at the end of each session. Companies must assess the features and systems of all digital products and services likely to be accessed by or to impact children, with any design elements that pose risk – individually or in combination – redesigned, disabled, or rendered inaccessible to children. The burden rests with companies to demonstrate effective risk assessment and mitigation.

Embedding high privacy and safety by default realizes children's rights to protection from harm and from commercial exploitation. It provides a robust baseline of protection, alleviates the challenges of obtaining and managing informed consent, and ensures children enter the digital world through a more protective starting point, while preserving their agency.

When built with children's best interests as a primary consideration, the design of digital products and services directs children away from risks, and towards educational, empowering, and enriching experiences.

Practical Examples

> SAFETY BY DESIGN

**United Nations**, *General comment No. 25 on children's rights in relation to the digital environment*, (2021): 'Leisure time spent in the digital environment may expose children to risks of harm, for example, through opaque or misleading advertising or highly persuasive or gambling-like design features. By introducing or using data protection, privacy-by-design and safety-by-design approaches and other regulatory measures, States parties should ensure that businesses do not target children using those or other techniques designed to prioritize commercial interests over those of the child.' (para. 110).

**European Union**, *Guidelines on measures to ensure a high level of privacy, safety and security for minors online*, (2025): 'providers of online platforms accessible to minors should: a. Ensure that privacy, safety and security by design principles are consistently applied to all account settings for minors. b. Set accounts for minors to the highest level of privacy, safety and security by default. This includes designing default settings in such a way as to ensure safe and age-appropriate settings for minors, taking into account their evolving capacities' (para. 57).

**Australia**, *Basic Online Safety Expectations*, (2022): 'Providers are expected to design and implement services that are likely to be accessed by children in a manner consistent with the objectives underlying Article 3 of the Convention of the Rights of the Child (UNCRC) that "[i]n all actions concerning children... the best interests of the child shall be the primary consideration"' (p. 30).

**Brazil**, *Digital Statute of the Child and Adolescent* (ECA Digital), (2025): 'Providers are prohibited from designing, modifying, or manipulating interfaces with the aim or effect of compromising the user's autonomy, decision-making, or choice' (art. 18 §2).

Practical Examples

> PRIVACY BY DESIGN

**Association of Southeast Asian Nations (ASEAN)**, *Guidelines for Harmonised and Comprehensive National Legislation Against All Forms of Online Child Sexual Exploitation and Abuse*, (2023): 'Furthermore, data collected should be limited to those necessary for achieving such purposes in preventing excessive data collection and subsequent violations of children's right to privacy' (p. 35).

**African Union**, *Digital Compact*, (2024): 'Member States and All Stakeholders: Advocate for and implement the principles of 'privacy by design and by default' in the development and deployment of digital technologies and services, ensuring that privacy safeguards are an integral part of the technology development lifecycle' (Pillar Nine, 2).

**Canada**, *Resolution of the Federal, Provincial and Territorial Privacy Commissioners and Ombuds with Responsibility for Privacy Oversight - Putting best interests of young people at the forefront of privacy and access to personal information*, (2023): 'Organizations must not [...] incorporate into products and services manipulative or deceptive design or behavioral incentives that influence young people to make poor privacy decisions or to engage in harmful behaviours; encourage young people to provide more information than what is necessary to use the product or service or to turn off protective privacy settings'.

**Indonesia**, *Government Regulation on the Governance of Electronic System Operations for Child Protection*, (2025): 'Electronic System Operators must configure the settings for Products, Services, and Features that are specifically designed for use or access by Children or those likely to be used or accessed by Children at a high privacy level by default [...]. Electronic System Operators may provide the option to set the privacy level [...] permanently or temporarily in accordance with Personal Data Protection Impact Assessment' (art. 10).

## 5Rights Children & AI Design Code criteria for designing and deploying AI systems with children in mind

**Developmentally appropriate**
AI systems must account for children's differing needs and vulnerabilities at different ages and stages of development, by design and default.

**Lawful**
AI systems must be compatible with relevant local, regional, national, and international law, rules, and regulations.

**Safe**
AI systems must not create or amplify risks to children's physical, mental or emotional safety and their wellbeing – including privacy and security risks.

**Fair**
AI systems must treat children and their data fairly, creating equitable and just outcomes.

**Reliable**
AI systems must function as expected, with performance and outcomes remaining robust over time, even in unexpected or harsh conditions or where atypical data is introduced.

**Meaningful redress**
AI systems must provide clear reporting and complaints mechanisms to seek actionable and effective recourse and remedy, with priority given to reports that relate to children.

**Transparent**
AI systems must offer accessible information to promote understanding of what the AI system does, accounting for the capacities and needs of children.

**Accountable**
AI companies must establish a chain of human and organizational responsibility for the lifecycle of an AI product, demonstrating conformity with the Code.

**Rights-respecting**
AI systems must uphold children's rights under the UNCRC and *General comment No. 25*, prioritizing their best interests and considering children's voices and opinions.

Practical Examples

**United Nations Secretary-General's High-level Advisory Body on AI**, *Governing AI for Humanity*, (2024): 'Prevention is better than cure: industry developers should design their products without addictive personalized features' (p. 35).

**World Economic Forum (WEF)**, *Artificial Intelligence for Children Toolkit*, (2022): 'Set the default options to the most secure and least intrusive to add an additional layer of safety for every user' (p. 26).

**Australia**, *Basic Online Safety Expectations*, (2022): 'If the service uses or enables the use of generative artificial intelligence capabilities, the provider of the service will take reasonable steps to consider end-user safety and incorporate safety measures in the design, implementation and maintenance of generative artificial intelligence capabilities on the service' (p. 41).

REGULATORY PRINCIPLE 7

# Prohibit practices likely to contribute to known harms.

'Your attention is pulled in hundreds of tiny directions — homework tabs, short-form videos, group chats, notification pings — and nothing gets deep attention. That creates anxiety, sleep problems, worse academic focus, and a creeping sense that you're always "on" but not actually present anywhere. Social comparison and performance pressure amplify that.'

MUHAMMED, 16, PAKISTAN

Tech companies often deliberately design risky digital products and services or are aware that they are exposing children to harm. Therefore, they must be required to act on evidence surfaced in internal data, CRIAs, risk assessments, and academic studies to mitigate potential harms. Where there is risk of harm, tech companies and legislators must additionally apply the precautionary principle to protect children's rights, privacy, and safety.

This requires prohibiting tech companies from deploying design features or business practices likely to contribute to known or anticipated harms. This includes recommending harmful material, encouraging children to stay on services longer than intended, automatically extending use through data-steered autoplay functions, excessive notifications, incentives for children to increase their network of friends or followers and publicly visible profiles. Deceptive design strategies deliberately deployed to erode children's agency and maximize profit must also be prohibited.[169]

Financial exploitation through in-app purchases is a clear example of known harm. 43% of children regret purchases made on social media, and 41% overspend while playing games online.[170] Online gambling and gambling-like features such as

loot boxes – purchasable items containing an unknown mix of lower and higher value rewards – are examples of dark patterns designed to nudge children into spending as much money as possible and are clearly against children's best interests.[171]

Similarly, the use of children's data in ways shown to be detrimental must be prohibited. This includes profiling or targeting of children of any age for commercial purposes on the basis of their actual or inferred characteristics (including group or collective data), targeting by association or affinity profiling,[172] and sharing children's data with third parties, unless companies can demonstrate a compelling reason that accounts for the best interests of the child.

Practical Examples

**United Nations**, *General comment No. 25 on children's rights in relation to the digital environment*, (2021): 'States parties should regulate against known harms and proactively consider emerging research and evidence in the public health sector' (para. 96).

**European Union**, *Digital Services Act*, (2022): 'Providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions' (Art.21(1)).

**China**, *Regulations on the Protection of Minors in Cyberspace*, (2023): 'No organization or individual shall produce, copy, publish or disseminate information that may affect the physical and mental health of minors ...' (art. 24).

**European Union**, *AI Act*, (2024): 'The following AI practices shall be prohibited: [...] the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm' (art. 5 (1)(b)).

**Maryland**, *Age-Appropriate Design Code Act*, (2024): 'A covered entity that provides an online product that is accessed or reasonable likely to be accessed by children may not [...] use dark patterns to [...] take any action that the covered entity knows, or has reason to know, is not in the best interests of children reasonably who access or are reasonably likely to access the online service, product, or feature' (§14-4606(A)(7)(III)).

**Brazil**, *Digital Statute of the Child and Adolescent* (ECA Digital), (2025): 'Art. 6. Providers of information technology products or services aimed at children and adolescents, or likely to be accessed by them, must take reasonable measures from the design stage and throughout the operation of their applications, with the aim of preventing and mitigating risks of access, exposure, recommendation, or facilitation of contact with the following content, products, or practices:

**III.** inducing, inciting, instigating, or assisting, through instructions or guidance, practices or behaviors that may cause harm to the physical or mental health of children and adolescents, such as physical violence or psychological harassment toward other children and adolescents, use of substances causing chemical or psychological dependency, self-diagnosis and self-medication, self-harm, and suicide;

**IV.** promotion and marketing of gambling, fixed-odds betting, lotteries, tobacco products, alcoholic beverages, narcotics, or products prohibited for sale to children and adolescents;

**V.** predatory, unfair, or misleading advertising practices, or other practices known to cause financial harm to children and adolescents' (art. 6).

Geolocation services compromise children's safety in the physical world and often operate without children's awareness. They must therefore be switched off by default, and provide clear notifications when they are in use.

Practical Examples

> GEOLOCATION

**Global Privacy Assembly (GPA)**, *Resolution on children's digital rights*, (2021): 'Online service providers should [...] provide for [...] default settings that offer the highest protection of children's personal data, and in particular the deactivation by default of certain options, such as geolocation and profiling [...]' (p. 7).

**Mexico**, *Code of good practices to guide the online processing of Personal Data of children and adolescents*, (2020): 'It is important to disable geolocation options by default, unless there is a justified reason not to do so, taking into account the best interests of the child. It is considered good practice to provide a clear signal to the holders when location tracking is active. Options for their location to be visible to others can be returned to the disabled mode at the end of each session' (p. 12).

**Canada**, *Resolution of the Federal, Provincial and Territorial Privacy Commissioners and Ombuds with Responsibility for Privacy Oversight - Putting best interests of young people at the forefront of privacy and access to personal information*, (2023): 'Turn off tracking, including location tracking, of young people by default, except if it is demonstrably necessary for the product or service to function, limited to only when the product or service is actively being used, and the activity is in the best interests of young people; [...] make any monitoring or tracking obvious to the young person;'

REGULATORY PRINCIPLE 8

# Published terms must be available, age-appropriate, and upheld.

'Even when tools are meant to be safe, young users rarely have enough control or understanding of how their data is used.'

ADIL, 16, INDIA & CANADA

Published terms are agreements governing the relationship between a digital product or service and its users. These include terms of service, privacy policies, community standards, and cookie policies, among others. They establish fundamental principles, including the use of users' personal information, the conditions they agree to, and the rules they must follow.[173]

Clear and accessible published terms are essential for transparency and trust,[174] but in practice they are typically incomprehensible to the average user, let alone children. Terms of service are written at the reading comprehension level of academic articles.[175] Research shows that reviewing the published terms of 15 popular sites would require approximately nine hours.[176] Unsurprisingly, only 1% of users read these documents.[177] This lack of accessibility is not accidental. Many digital services deliberately hide their rules and data practices behind complex and opaque legal language, as tech companies' business models rely on information asymmetry with users.[178]

In this context, children's acceptance of terms of service cannot be considered meaningful or informed.[179] Rather than constituting a bilateral contract, terms of service form 'a one-way relationship allowing the monitoring of the consent-giver who has no other option but to agree or be refused the benefit'.[180] As it stands, children cannot understand how digital products and services operate or the consequences of accepting them. States must therefore mandate age-appropriate published terms.[181]

## Best practices for age-appropriate published terms

5Rights' *Tick to Agree* and the *IEEE 2089-2021 Standard for an Age Appropriate Digital Service Framework* set out international best practices for age-appropriate published terms:

### Language
Simple language that the youngest likely user can under-stand, ensuring the underlying message and terms of agreement have been understood..

### Length
Concise text, divided into clear sections, and made available in bite-sized pieces.

### Format
Multiple formats for different age ranges.

### Navigability
Prominent placement that is easy to find, easily navigable, searchable and clearly structured to provide children and young people with the information they need or want to know.

### Timing
Presentation at relevant moments in the user journey with time-limited consent to allow children to give their ongoing agreement.

### Inclusivity
Consideration of the needs of diverse groups of children without assuming adult engagement.

Practical Examples

> AGE-APPROPRIATE TERMS

**United Nations General Assembly**, *Resolution 78/187 on the Rights of the Child in the digital environment*, (2023): 'Urges States to take measures to ensure that children are informed, in a child-friendly, easily accessible and age-appropriate way, about the collection and use of their data online' (para. 47).

**Organisation for Economic Co-operation and Development (OECD)**, *Towards digital safety by design for children*, (2024): 'Children need to understand the digital spaces they inhabit. Consequently, they need clear, timely, accessible, and age-appropriate information about how digital services work, the risks involved, and how they can be protected' (p. 6).

**Philippines**, *Guidelines on Child-Oriented Transparency*, (2024): 'PICs shall ensure that the Privacy Notice, including any information and communication relating to the processing of personal data, is readily accessible.... PICs should ... ensure that the Privacy Notices are presented in a manner that is simple and easily understandable, taking into consideration the age range of the intended or likely users. PICs must ensure that any information or communication relating to the processing of children's personal data should be concrete and definitive, and understood by intended or likely users whose personal data are involved in the specific processing activity' (Section 3B).

Besides making terms available and age-appropriate, businesses have obligations to prevent their online services from being used in ways that contribute to violations of children's rights.[182] However, that is often not the case. For example, Canadian privacy regulators found that TikTok – which prohibits users under the age of 13 from using the platform – took no action to restrict access to users it knew were underage, while continuing to harvest their data and profile them for commercial purposes.[183]

Companies must proactively uphold and enforce their published terms, including rules of conduct and content policies – treating them as binding commitments rather than aspirational statements.

Practical Examples

**Global Online Safety Regulators Network (GOSRN)**, *Position Statement: Human Rights & Online Safety Regulation*, (2023): 'Implement systems and processes … to have and uphold clear terms of service and reporting pathways. These systems and processes should be transparent and user-friendly and service providers should be accountable for them' (p. 4).

**Council of Europe,** *Guidelines to respect, protect and fulfil the rights of the child in the digital environment*, (2018): 'Recognising that parents, carers and others may rely on an online service's stated terms and conditions of service as a guide to the suitability of that service for their child, … States should require business enterprises to take reasonable, proportionate and effective measures to ensure that their terms and conditions of service are enforced' (para. 97).

**Mexico**, *Code of good practices to guide the online processing of Personal Data of children and adolescents*, (2020): 'You are encouraged to comply with and be accountable for your own posted terms, policies and standards (including privacy policies, age restrictions, rules of conduct and content policies)' (p. 11).

**United Kingdom**, *Age Appropriate Design Code*, (2020): 'If you make commitments to users about the content or other aspects of your online service then you need to have systems to ensure that you meet those commitments' (standard 6).

REGULATORY PRINCIPLE 9

# Mandate responsible business conduct.

'The digital world cannot just be handled by 'going with the flow'. We must open our eyes to what the people in power prioritize: interaction or integrity?'

SHER, 16, INDONESIA

Beyond implementing safety- and privacy-by-design standards, tech companies must adopt responsible business conducts that respect children's rights across their operations, governance, and supply chains.[184] Similarly, lawmakers must require ongoing child rights due diligence (as outlined in Principle 5), transparent reporting, enforceable standards, regular independent third-party audits, and effective remedies for breaches of children's rights.[185]

A high level of transparency is crucial for accountability.[186] Regulators cannot effectively oversee companies' practices without access to relevant information. Companies must proactively publish CRIAs, risk assessments, and internal documents[187] as well as grant vetted researchers access to data for independent audits of systemic risks, including algorithms and mitigation measures.[188] Beyond enabling oversight, transparency also mitigates business risk by driving innovation across the industry and building trust with investors and advertisers.[189]

In addition, tech companies should continuously monitor their digital products and services to detect unanticipated or evolving risks. In doing so, businesses should provide records of changes implemented,[190] proactively report incidents,[191] ensure relevant staff are adequately trained, and appropriately resource Trust & Safety teams.[192]

However, transparency and ongoing monitoring alone are insufficient. Independent oversight and effective enforcement are necessary to meaningfully hold tech companies accountable for children's rights. As further expanded in Principle 10, independent regulators should have the authority and capacity to oversee tech

companies and investigate potential breaches, specific incidences of harm as well as the longer-term structural impacts of business conduct.

Companies must also cultivate internal accountability and demonstrate compliance, by keeping appropriate records, providing relevant staff training, and supporting whistleblowers.[193] Importantly, this extends to the entire supply chain and therefore requires tech companies to map upstream and downstream risks and uses.[194]

States must promote and ensure compliance with industry codes and technical standards that reflect the highest levels of safety, privacy, and ethics for children,[195] such as the *IEEE 2089 Standard for an Age Appropriate Digital Services Framework*[196] or the Conscious Advertising Network's *Guiding Principles on Children's Rights and Wellbeing*.[197] Conformity to these standards must be verified by independent third parties through audits that can also be conducted in the context of certification schemes whereby compliance results in accreditation,[198] such as the *IEEE Age Verification Certification Program*.[199] Voluntary codes fail to hold companies accountable to their principles and allow businesses to continue their risky practices while broadcasting their membership.[200]

Governments can promote responsible business conduct by setting standards for public procurement[201] and public-private partnerships[202] grounded in children's rights, safety, and privacy and based on independent certification.

Practical Examples

**Global Online Safety Regulators Network (GOSRN)**, *Position Statement: Human Rights & Online Safety Regulation*, (2023): 'Promote governance structures that prioritise the safety of users and encourage shared responsibility and accountability to minimise, detect and eliminate online harms, with the goal of embedding safety into the culture and leadership of an organisation' (p. 4).

**World Economic Forum (WEF)**, *Global Principles on Digital Safety: Translating International Human Rights for the Digital Context*, (2023): 'Providing clarity and transparency about a service's approach to digital safety, including by making public, and providing transparency on … the processes and systems in place to mitigate against abuse and data on the outcomes' (p. 6).

**United Nations Educational, Scientific and Cultural Organization (UNESCO)**, *Recommendation on the Ethics of AI*, (2021): 'Appropriate oversight, impact assessment, audit and due diligence mechanisms, including whistle-blowers' protection, should be developed to ensure accountability for AI systems and their impact throughout their life cycle. Both technical and institutional designs should ensure auditability and traceability of (the working of) AI systems in particular to address any conflicts with human rights norms and standards and threats to environmental and ecosystem well-being' (para. 43).

**Australia**, *Online Safety Act*, (2021): 'The Commissioner may … require the provider to … prepare periodic reports about the extent to which the provider complied with the applicable basic online safety expectations …' (Section 56 (2)).

## Reporting mechanisms, complaints, and redress

Businesses also have the responsibility to provide effective remedies for violations of children's rights, privacy, and safety in the digital world.[203] While remedies address residual violations that were not prevented upstream, they are not an adequate mitigation measure[204] but rather a crucial element of a holistic response to children's safety.

This requires mandating prominent, meaningful, and age-appropriate tools for reports, complaints, and redress.[205] Children must be able to report risky features and functionalities, unfair decisions, and specific incidents. These reporting mechanisms should be free, safe, confidential, responsive, and child-friendly.[206] Importantly, tech companies must be transparent regarding their reporting processes, disclosing how and when reports are handled, as well as how children's data is treated.[207] Tech companies must also respond to user reports – prioritizing those received from children – and implement meaningful changes in response.[208]

Practical Examples

> REPORTING MECHANISMS

**International Telecommunications Union (ITU)**, *Child Online Protection Guidelines*, (2020): 'Clear and transparent reporting mechanisms should be made available to users who have concerns about content and behaviour. Furthermore, reporting needs to be followed up appropriately, with timely provision of information about the status of the report. Although companies can vary their implementation of follow-up mechanisms on a case-by-case basis, it is essential to set a clear time frame for responses, communicate the decision made regarding the report, and offer a method for following up if the user is not satisfied with the response' (p. 20).

**Council of Europe**, *Guidelines to respect, protect and fulfil the rights of the child in the digital environment*, (2018): 'Member States should ensure the effective implementation of their obligations [...] to fulfil a child's right to an effective remedy when their human rights and fundamental freedoms have been infringed in the digital environment. This entails the provision of available, known, accessible, affordable, and child-friendly avenues through which children, as well as their parents or legal representatives, may submit complaints and seek remedies' (para. 67).

**Mexico**, *Code of good practices to guide the online processing of Personal Data of children and adolescents*, (2020): 'It is recommended to provide prominent and accessible tools that help girls, boys and adolescents exercise their rights to personal data protection, and report complaints or concerns, through their legal representative' (p. 12).

REGULATORY PRINCIPLE 10

# Effective enforcement mechanisms should be in place.

'I envision a digital world that has accountability mechanisms at its core.'

KATLEHO, 17, LESOTHO

As affirmed by the UN Committee on the Rights of the Child, 'it is the lack of implementation or the poor enforcement of laws regulating business that pose the most critical problems for children'.[209]

Weak enforcement allows preventable harms to persist and undermines the realization of children's rights in practice. Similarly, voluntary and self-regulatory approaches have failed to protect children. With regards to AI,[210] a global study reveals that less than half of global respondents are willing to trust AI systems.[211] Children's rights cannot depend on corporate goodwill or discretionary compliance.

At present, noncompliance is frequently a rational and profitable business decision. Financial penalties are often absorbed as a cost of doing business, with fines amounting to only a fraction of daily or weekly revenues.[212] Effective enforcement therefore requires meaningful, dissuasive, and proportionate consequences, as evidence demonstrates that such actions drive tech companies to design more rights-respecting and age-appropriate digital products and services.[213]

To ensure businesses meet their responsibilities, States should effectively implement and enforce legislation,[214] and strengthen regulatory agencies by ensuring 'they have sufficient powers and resources to monitor and to investigate complaints and to provide and enforce remedies for abuses of children's rights'.[215] While supervisory measures such as guidance, notices, and monitoring may be effective regulatory action, independent regulators must be granted the necessary enforcement power and authority to take decisive formal action to address systemic noncompliance.[216]

This includes the ability to require changes to digital products and services, features, and business models that are likely to expose children to serious risk, as well as the power to impose fines and to temporarily or permanently suspend a company's access to the regulated market.

This authority must be supported by adequate institutional capacity and expertise, including coordination with international counterparts[217] through international forums such as the Global Privacy Assembly or the Global Online Safety Regulators Network. Domestically, regulators with overlapping or complementary mandates must coordinate closely, ensuring that complaints and findings are acted upon.

Practical Examples

**United Nations General Assembly**, *Resolution 78/187 on the Rights of the Child in the digital environment*, (2023): 'Reiterates its call upon States to ensure a clear and predictable environment, including through legal and regulatory measures, ... which strengthens regulatory agencies' responsibility for the development of standards for the protection of the rights of the child, with powers and resources to monitor data privacy practices, investigate violations and abuses and receive communications from individuals and organizations, and to provide appropriate remedies' (para. 37).

**African Union**, *Child Online Safety and Empowerment Policy*, (2024): 'Strengthen the capacity of regulators for the oversight and enforcement of child online privacy and safety legal frameworks'. (p. 14)

**Indonesia**, *Government Regulation on the Governance of Electronic System Operations for Child Protection*, (2025): 'Administrative sanctions ... may be in the forms of: a. written reprimand; b. administrative fines; c. temporary suspension; and/or d. termination of access' (art. 38(2)).

**Brazil**, *Digital Statute of the Child and Adolescent* (ECA Digital), (2025): 'In case of noncompliance with the obligations set forth in this Law, ... offenders shall be subject to the following penalties:

1. warning, with a period of up to thirty (30) days to adopt corrective measures;
2. simple fine of up to ten percent (10%) of the economic group's turnover in Brazil in its last fiscal year ;
3. temporary suspension of activities;
4. prohibition from exercising activities'. (art. 35)

# Conclusion

By embedding privacy, safety, and security standards upstream at the point of design, legislators can transform the digital environment and reduce risks posed by exploitative features, predatory contracts, and content at scale.

Research shows that when laws are enforced robustly, tech companies implement meaningful changes, including strengthening children's default settings, changing recommender systems, and restricting targeted advertising to children.[218] Far from holding innovation back, accountability raises the bar by creating a level playing field that allows responsible businesses to compete on safety and quality.

When designed and deployed with children's rights in mind, technology can fulfill its promises of democratizing access to education, encouraging children to develop fully, and improving accessibility for diverse children.

But this future requires intention, accountability, and the leadership to consistently prioritize children's safety, privacy, and best interests. The time for voluntary promises has passed. As this blueprint demonstrates, international best practices provide the basis for impactful action. Governments, policymakers, and regulators must now act to build the digital world children deserve.

My experience shows that while digital spaces create opportunities, children's rights are far from fully protected. Young users face opaque data practices, targeted content we cannot control, and safety measures that arrive only after harm has occurred. Much of the digital world was not designed with children in mind, and navigating it often feels like being forced to grow up faster than we should. Children deserve digital systems that respect our privacy, protect us from harm, and treat us as rights-holders, not as data points or third-party partners.

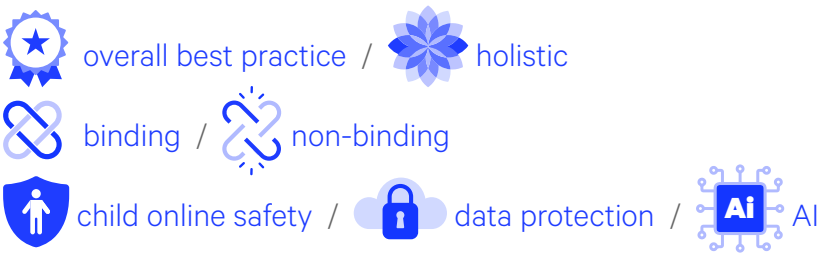
GINA, 17, EGYPT

ANNEX

# Overview of selected analyzed frameworks

The frameworks outlined in this Annex all contain elements of best practice for the realization of a digital world designed with children in mind. These emerge from various approaches – ranging from online safety and platform regulation to data protection and AI governance. While certain documents represent comprehensive best practices, others contain individual sections or clauses essential to a holistic and upstream approach to tech accountability and children's safety and rights in the digital world.

**Legend**



# Global frameworks

## UNITED NATIONS

*Convention on the Rights of the Child* (1989) and *General comment No. 25 on children's rights in relation to the digital environment* (2021)

The United Nations' *Convention on the Rights of the Child* (UNCRC) is the most widely ratified international human rights treaty in history – by every UN Member State except the US. It enshrines children's indivisible and interdependent rights, including to privacy,[219] to not be exploited,[220] to protection,[221] to freedom of expression[222] and of thought,[223] to education,[224] and to play.[225]

The UN Committee on the Rights of the Child's *General comment No. 25* clarifies how States' obligation to respect, protect,[226] and fulfil children's rights apply in the digital world.[227] Building on UNCRC *General comment No. 16* and the UN *Guiding Principles on Business and Human Rights*,[228] it also emphasizes the responsibilities of the business sector to respect children's rights, and to prevent, mitigate, and – where appropriate – provide effective remedies for violations.[229] In the 5 years since its development, UNCRC *General comment No. 25* has informed, accelerated, and directly shaped laws, regulation, and normative frameworks at the global, regional, and national levels.[230]

## INTERNATIONAL TELECOMMUNICATIONS UNION (ITU)

*Child Online Protection Guidelines* (2020)

The International Telecommunications Union developed a series of *Child Online Protection Guidelines* targeting children, parents and educators, industry, and policymakers. The guidelines for policymakers supports national legislators in developing frameworks that build upon child online protection developments, highlighting key areas[231] including the development of a regulatory policy and capacity building to protect children from all types of online harms.[232]

## ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD)

*Recommendation of the Council on Children in the Digital Environment* (2021)

The Council Recommendation lays out a set of principles to protect children from online risks and promote the opportunities and benefits that the digital world provides. These are intended to form the basis for policy frameworks, and notably recommend the 'adoption of measures that provide for age-appropriate child safety by design'[233] and the implementation of 'evidence-based policies to support children in the digital environment'.[234]

## G20

*High Level Principles for Children Protection and Empowerment in the Digital Environment* (2021)

Building on the OECD *Recommendation on Children in the Digital Environment*, G20 Digital Ministers set out principles to protect and respect children's rights in the digital environment. They suggest that '[g]overnments should promote the adoption of measures that provide for age-appropriate child safety by design'.[235]

## GLOBAL PRIVACY ASSEMBLY (GPA)

*Resolution on children's digital rights* (2021)

The Global Privacy Assembly is a forum for international collaboration between over 130 data protection and privacy authorities.[236] In 2021, Data Protection Authorities from every continent unanimously reiterated key elements of UNCRC *General comment No. 25*, including the prohibition of manipulative practices and the use or transmission of children's data to third parties for commercial or advertising purposes. The Resolution establishes that tracking must be off by default, age assurance mechanisms must be proportionate to risk and privacy-preserving, and service providers should refrain from commercially profiling children.

## WORLD ECONOMIC FORUM (WEF)

*Artificial Intelligence for Children Toolkit* (2022)

The *AI for Children Toolkit* guides technology companies in building fair, inclusive, responsible, safe, and transparent AI for children. The toolkit provides actionable guidance to different actors in the development process to balance innovation with responsibility and place children at the center of AI design.

## UNITED NATIONS GENERAL ASSEMBLY

*Resolution 78/187 on the Rights of the Child in the digital environment* (2023)

The 2023 United Nations' *General Assembly Resolution on the Rights of the Child* in the digital environment is a strong and high-level reiteration by all UN Member States of UNCRC *General comment No. 25*. It calls on States to require 'digital technology and other relevant industries to respect the rights of the child' and to 'strengthen regulatory agencies' responsibility for the development of standards for the protection of the rights of the child'.[237]

## GLOBAL ONLINE SAFETY REGULATORS NETWORK (GOSRN)

*Position Statement: Human Rights & Online Safety Regulation* (2023)

The Global Online Safety Regulators Network is a group of national regulators with mandates covering online safety. Online safety regulators from around the world reiterated their commitment to promote a rights-based approach to digital regulation centered on the best interests of the child, children's rights to privacy and protection from exploitation, as well as the interdependence and indivisibility of these rights.[238]

## WORLD ECONOMIC FORUM (WEF)

*Global Principles on Digital Safety: Translating International Human Rights for the Digital Context* (2023)

The World Economic Forum's Global Coalition for Digital Safety brings together leaders from the public and private sectors to improve global coordination on online safety. The Principles aim to operationalize human rights principles for digital safety by setting out concrete interventions for governments and online service providers.

## ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD)

*Towards digital safety by design for children* (2024)

Recognizing the risk landscape children experience online and the emergence of various digital safety laws, the report sets forth key components of safety by design to ensure a coherent international regulatory strategy. These include implementing child-centered design, protecting children's privacy, and leveraging age assurance to provide age-appropriate experiences.[239]

## UNITED NATIONS GENERAL ASSEMBLY

*Global Digital Compact* (2024)

Part of the 2024 *Pact for the Future*, the *Global Digital Compact* builds on UNCRC *General comment No. 25* and UNGA *Res. 78/187*. All UN Member States unanimously recommitted to 'strengthen legal and policy frameworks to protect the rights of the child in the digital space'[240] and to 'prioritize the development and implementation of national online child safety policies and standards' [241] by 2030.

## UNITED NATIONS SECRETARY-GENERAL'S HIGH-LEVEL ADVISORY BODY ON AI

*Governing AI for Humanity* (2024)

The final report of the *UN Secretary-General's High-level Advisory Body on AI* outlines a blueprint for addressing AI-related risks through global collaboration. The report mainstreams children's rights throughout and calls for strong protection and privacy for children, mandates child impact assessments and age-appropriate design.[242]

## UNICEF

*Taking a Child Rights-Based Approach to Implementing the UNGPs in the Digital Environment* (2024)

To support the implementation of the UN *Guiding Principles on Business and Human Rights* in the digital world, this contribution provides an overview of the key children's rights concepts in the digital environment.[243] It notably recognizes that 'Meeting the corporate responsibility to respect human rights in the digital environment requires policies and processes to identify and address child rights impacts'.[244]

# Regional frameworks

## AFRICAN UNION

*African Charter on the Rights and Welfare of the Child* (1990)

Echoing the UNCRC, the *African Charter on the Rights and Welfare of the Child* (ACRWC) enshrines children's rights to privacy,[245] to not to be exploited,[246] and to freedom of thought[247]. The African Committee of Experts on the Rights and Welfare of the Child (ACERWC) emphasizes that children have the same rights online as they do offline,[248] and that children's rights enshrined in the ACRWC therefore apply fully in the digital world.[249]

## EUROPEAN UNION

*General Data Protection Regulation* (2016)

The EU *General Data Protection Regulation* stipulates that 'children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data' (Recital 38), reflecting the vulnerabilities associated with their age and developmental capacities, as well as their established rights. The adoption of the GDPR in 2016 set a new global norm, has influenced regulatory reform and inspired new laws around the world.

## COUNCIL OF EUROPE

*Guidelines to respect, protect and fulfil the rights of the child in the digital environment* (2018)

The Council of Europe Guidelines aim to assist Member States developing domestic approaches to respect, protect, and fulfill children's rights in the digital world. The guidelines call on States to require businesses to meet their responsibility to respect children rights by taking precautionary measures and mandating safety and privacy by design and default.[250]

## ORGANIZATION OF AMERICAN STATES

*Guidelines for Empowering and Protecting Child and Adolescent Rights on the Internet in Central America and the Dominican Republic* (2018)

Recognizing the prominence of the digital divides in Central America, the Guidelines draw on regional best practices to formulate proposals for strengthening the promotion and protection of children's rights in the digital environment. The Guidelines call for capacity building of relevant authorities[251] and dialogue toward the development of a model inter-American law on digital inclusion and the protection of children in the digital world.[252]

## EUROPEAN UNION

*Digital Services Act* (2022) and *Guidelines on measures to ensure a high level of privacy, safety and security for minors online* (2025)

The European Union's *Digital Services Act* sets out obligations for online platforms to ensure a safe and rights-respecting online environment. Article 28 and its accompanying guidelines require online platforms to ensure a high level of privacy, safety, and security for children. These include requirements for recommender systems, interface design, registration processes, and age assurance.

## ASSOCIATION OF SOUTHEAST ASIAN NATIONS (ASEAN)

*Guidelines for Harmonised and Comprehensive National Legislation Against All Forms of Online Child Sexual Exploitation and Abuse* (2023)

The Guidelines provide a framework for ASEAN Member States to review their legislation on protecting children from online child sexual exploitation and abuse, with the aim to strengthen national approaches throughout the region. The guidelines aim to promote a child-rights based and harmonized approach throughout ASEAN Member States.

## AFRICAN UNION

*Child Online Safety and Empowerment Policy* (2024)

Building on UNCRC *General comment No. 25*, the African Union's *Child Online Safety and Empowerment Policy* outlines key principles, goals, and strategies for creating a safer digital environment for children in Africa. The ten policy areas identified are: institutional capacity, legal and regulatory frameworks, personal data and identity, response and support systems, business and children's rights, training, education, public awareness, research and development, and international cooperation.

## COUNCIL OF EUROPE

*Framework Convention on Artificial Intelligence* (2024)

The first international treaty on Artificial Intelligence specifically recognizes children's distinct rights under the UN *Convention on the Rights of the Child*, as elaborated in its *General comment No. 25*. Article 18 requires States to account for the specific needs and vulnerabilities of children in their implementation of the Convention.

## EUROPEAN UNION

*AI Act* (2024)

The AI Act is a comprehensive regulatory framework that categorizes AI systems based on their level of risk. This law sets a strong precedent for tech regulation, explicitly recognizing children's rights as outlined in *General comment No. 25*. A central goal of the *AI Act* is to safeguard children from the specific vulnerabilities they face in the online environment with an outright ban on AI systems exploiting the vulnerabilities of age. Additionally, it requires rigorous risk assessment for 'high-risk' AI systems, including those used in education and mandates transparency, through watermarking deepfakes and alerting users about AI interactions.

# National frameworks

## RWANDA

*Child Online Protection Policy* (2019)

Adopted in 2019, Rwanda's *Child Online Protection Policy* sets out a roadmap to implement international best practices in children's data protection in the Rwandan context. The Policy recommends introducing corporate responsibility standards[253] and data protection regulations;[254] implementing safety, rights, and ethics by design;[255] and ensuring the protection of children form commercial pressures.[256]

## UNITED KINGDOM

*Age Appropriate Design Code* (2020)

The *Age Appropriate Design Code* (AADC) is the first-ever statutory code of practice for protecting children's data in the digital world. Grounded in the *General Data Protection Regulation*, it consists of 15 enforceable and complementary standards that, when implemented together, hold tech companies accountable to deliver a high level of privacy protection by design and default. Its standards have been replicated across all continents.[257]

## MEXICO

*Code of good practices to guide the online processing of Personal Data of children and adolescents* (2020)

Mexico's now-dissolved National Institute for Transparency, Access to Information and Personal Data Protection issued non-binding guidelines for age-appropriate design, replicating broadly the UK AADC's standards.

## IRELAND

*Fundamentals for a Child-Oriented Approach to Data Processing* (2021)

Ireland's Data Protection Commission sets out standards for all organizations collecting and processing children's data. The Fundamentals recognize that children – defined as anyone under the age of 18 – use services beyond those that are directed at them, emphasizing that mixed-audience services may choose to establish a high level of data protection for all users, negating the need to distinguish between adults and children.

## AUSTRALIA

*Online Safety Act* (2021) and *Basic Online Safety Expectations* (2022)

Australia's *Online Safety Act* and its accompanying *Basic Online Safety Expectations* outline how digital products and services must take reasonable steps to keep users in Australia safe and hold tech companies accountable for user safety. Companies must notably prioritize children's best interests in the design and operation of services likely to be used by children.

## CALIFORNIA

*Age-Appropriate Design Code* (2022)

Modeled on the UK's *Age Appropriate Design Code*, the California *Age-Appropriate Design Code* similarly requires companies to design products that children use with safety and privacy in mind. Implementation includes providing high safety settings by default (such as safe search or family and friend settings), preventing unknown adults from direct messaging minors, offering tools for breaks and rest from compulsive services, and protections from third-party advertisers.

## CHINA

*Regulations on the Protection of Minors in Cyberspace* (2023)

The regulations mandate internet platforms to prioritize children's health and wellbeing, prevent harm, and conduct regular impact assessments on the protection of minors online. They notably prohibit digital products, services, and features that are addictive to children, as well as impose restrictions on how much time and money tech companies can allow children to spend on their digital products and services.

## INDONESIA

*Government Regulation on the Governance of Electronic System Operations for Child Protection* (2025)

In 2025, Indonesia became the first Global Majority country to adopt binding regulation for age-appropriate design. The law requires that digital products and services likely to be accessed by children put children's rights and best interests above commercial interests, by delivering a high level of privacy by design and default.

## BRAZIL

*Digital Statute of the Child and Adolescent* (ECA Digital) (2025)

As the first Latin American country to enshrine age-appropriate design standards into law, Brazil requires tech companies to assess and mitigate the risks faced by children on their products and services. Key measures in the *ECA Digital* include prohibitions of manipulative design and other commercially exploitative practices such as behavioral profiling and emotional analysis, as well as expert supervision over AI tools and recommender systems to ensure their safety.

# Endnotes


1 Schmidt, E. & Cohen, J. (2013). *The New Digital Age*. (p. 3).
2 Livingstone, S., Carr, J., & Byrne, J. (2015). *One in Three: Internet Governance and Children's Rights*.
3 5Rights Foundation. (2023, April 11). *Disrupted Childhood: The cost of persuasive design*.
4 5Rights Foundation. (2021, September 17). *Pathways: How digital design puts children at risk*.
5 Digital Futures for Children. (2025). *EdTech matters for children's learning, privacy and other rights*. London School of Economics and Political Science.
6 Center for Countering Digital Hate. (2025, August 6). *Fake Friend: How ChatGPT is betraying teenagers.* / Gerken, T. (2024, December 11). *Chatbot "encouraged teen to kill parents over screen time limit"*. BBC. / Smith, B. (2024, December 27). *An AI chatbot told me to murder my bullies.* The Telegraph.
7 5Rights Foundation. (2023, April 11). *Disrupted Childhood: The cost of persuasive design*.
8 Polo, N. (2025, August 29). *Will the UK AI Bill protect people and society?*. Ada Lovelace Institute.
9 Wood, S. (2024, May 20). *Impact of regulation on children's digital lives*. London School of Economics and Political Science. / John, M., & Kate, B. (2024, March). *UK Age-Appropriate Design Code: Impact Assessment*. Children and Screens.
10 UNICEF. (2025, June). *Childhood in a Digital World.*
11 OECD. (2024, June 19). *Towards digital safety by design for children*. (p. 5).
12 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para. 39).
13 Livingstone, S., Carr, J., & Byrne, J. (2015, November). *One in Three: Internet Governance and Children's Rights.*
14 Ghai, S., Magis-Weinberg, L., Stoilova, M., Livingstone, S., & Orben, A. (2022, August). *Social Media and Adolescent Well-being in the Global South*. Current Opinion in Psychology, 46(46), 101318.
15 United Nations. (1989, November 20). *Convention on the Rights of the Child*. OHCHR. (Art. 1).
16 UNICEF. (2025, June). *Childhood in a Digital World*.
17 This report has notably built on: 5Rights, *Child Online Safety Toolkit*. 5Rights, *Children & AI Design Code*. 5Rights, *Approaches to Children's Data Protection*. 5Rights, *A High Level of Privacy, Safety & Security for Minors*. Digital Futures for Children, *Child Rights by Design*. Digital Futures for Children, *Mapping the Global Impact of General comment No. 25*. UNICEF, *Taking a Child Rights-Based Approach to Implementing the UNGPs in the Digital Environment*. UNICEF, *Artificial Intelligence Governance in Motion*. UNICEF, *Policy Guidance on AI for Children*. UNICEF, *Keeping children safe online: Trends in online platform regulation and emerging lessons*. Council of Europe, *Mapping Study on Legal Frameworks relating to AI and Children's Rights*. OECD, *Towards digital safety by design for children*. Forbrukerrådet, *Commercial exploitation of children and adolescents online*. Internet Society, *The Global Online Safety Benchmark*. Chatham House, *Towards a global approach to digital platform regulation*.
18 5Rights Foundation. (2023, April 11). *Disrupted Childhood: The cost of persuasive design*.
19 Cavoukian, A. (2009, August). *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario.
20 United Nations. (2024, September 22). *Global Digital Compact*. UN Office for Digital and Emerging Technologies. (Para. 23(c)).
21 Risk is commonly defined as the probability of harm.
22 Stoilova, M., Livingstone, S., & Khazbak, R. (2021). *Investigating Risks and Opportunities for Children in a Digital World: A rapid review of the evidence on children's internet use and outcomes*. In UNICEF. (p. 7).
23 OECD. (2021, January 8). *Children in the Digital Environment: Revised typology of risks*.
24 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. / OECD. (2012, February 16). *Recommendation of the Council on Children in the Digital Environment*. / African Union. (2024, May 21). *African Union Child Online Safety and Empowerment Policy*.

25 Livingstone, S., & Stoilova, M. (2021, June 11). *The 4Cs: Classifying Online Risk to Children*. Children Online: Research and Evidence.
26 5Rights Foundation. (2021, September 17). *Pathways: How digital design puts children at risk*. / 5Rights Foundation. (2023, April 11). *Disrupted Childhood: The cost of persuasive design*.
27 5Rights Foundation. (2022, February 3). *Risky by Design*. / 5Rights Foundation. (2023, April 11). *Disrupted Childhood: The cost of persuasive design*.
28 Office of the Privacy Commissioner of Canada. (2024). *Sweep Report 2024: Deceptive Design Patterns*.
29 UN Special Rapporteur on the right to privacy. (2021, January 25). *A/HRC/46/37: Artificial intelligence and privacy, and children's privacy*. OHCHR. (Para. 91).
30 European Parliament. (2023). *Resolution on addictive design of online services and consumer protection in the EU single market*. (Para. J)
31 United Nations. (1989, November 20). *Convention on the Rights of the Child*. OHCHR. (Arts. 32 & 34). United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para. 103).
32 Raffoul, A., Ward, Z. J., Santoso, M., Kavanaugh, J. R., & Austin, S. B. (2023). *Social media platforms generate billions of dollars in revenue from U.S. youth: Findings from a simulated revenue model*. PLoS ONE, 18(12).
33 Wells, G., & Horwitz, J. (2021, September 28). *Facebook's Effort to Attract Preteens Goes Beyond Instagram Kids, Documents Show*. The Wall Street Journal.
34 Kingkade, T. (2026, January 23). *Google's work in schools aims to create a 'pipeline of future users," internal documents say*. NBC News.
35 Moti, Z., Senol, A., Bostani, H., Zuiderveen, B. F., Moonsamy, V., Mathur, A., & Acar, G. (2023, December 10). *Targeted and Troublesome: Tracking and Advertising on Children's Websites*. 45th IEEE Symposium on Security and Privacy.
36 Office of the Privacy Commissioner of Canada. (2024). *Sweep Report 2024: Deceptive Design Patterns*.
37 Milmo, D., & Skopeliti, C. (2021, September 18). *Teenage girls, body image and Instagram's "perfect storm"*. The Guardian.
38 5Rights Foundation. (2024, October 18). *TikTok knows it is harming children*. / Allyn, B., Goodman, S., & Kerr, D. (2024, October 11). *TikTok executives know about app's effect on teens, lawsuit documents allege*. NPR.
39 Other benchmarks include IEEE Standards Association. (2021, November 9). *IEEE 2089 Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children*. / 5Rights Foundation. (2022c, September 2). *Approaches to children's data protection: A comparative international mapping*.
40 Agência Pública, & Centro Latinoamericano de Investigación Periodística. (2025). *A Mão Invisível das Big Techs*. / Béjar, A., Molly Rose Foundation, Cybersecurity for Democracy, Parents for Safe Online Spaces, Fairplay, & Heat Initiative. (2025, September 26). *Teen Accounts, Broken Promises*. Fairplay.
41 Children and youth quotes used throughout this report originate from 5Rights Youth Ambassadors.
42 Digital Futures for Children. (2025). *EdTech matters for children's learning, privacy and other rights*. London School of Economics and Political Science.
43 Hooper, L., Livingstone, S., & Pothong, K. (2022). *Problems with data governance in UK schools: the cases of Google Classroom and ClassDojo*. / Human Rights Watch. (2022, May 25). *Governments Harm Children's Rights in Online Learning*.
44 Kingkade, T. (2026, January 23). *Google's work in schools aims to create a "pipeline of future users," internal documents say*. NBC News.
45 Xiao, L. Y., & Lund, M. L. (2025). *Non-compliance with and non-enforcement of UK loot box industry self-regulation on the Apple App Store: a longitudinal study on poor implementation*. Royal Society Open Science, 12(5).
46 UNICEF, & UN Human Rights. (2024, November 18). *Taking a Child Rights-Based Approach to Implementing the UNGPs in the Digital Environment*. (p. 6).
47 eSafety Commissioner. (2022). *How common is exposure to content associated with harm among children in Australia?* / Statistics Canada. (2024, February 27). *Young people and exposure to harmful online content in 2022*. / Winther, D. K., Stoilova, M., Büchi, M., Twesigye, R., Smahel, D., & Livingstone, S. (2023,

July). *Children's exposure to hate messages and violent images online*. UNICEF. / OECD. (2025, May 15). *How's Life for Children in the Digital Age?* (p.55).

48 Robinson, A. (2025, May 29). *Reports of Harmful Content Rise by 20% in 2024*. SWGfL.

49 Nash, V., & Felton, L. (2024). *Treating the Symptoms or the disease? Analysing the UK Online Safety Act's Approach to Digital Regulation*. Policy & Internet, 16(4).

50 5Rights Foundation. (2023, April 11). *Disrupted Childhood: The cost of persuasive design*. / 5Rights Foundation. (2021, September 17). *Pathways: How digital design puts children at risk*.

51 Metzler, H., & Garcia, D. (2023). *Social Drivers and Algorithmic Mechanisms on Digital Media*. Perspectives on Psychological Science, 19(5), 735–748. / Barrett, N. (2024, October 13). *Facebook, X and TikTok: How social media algorithms shape speech*. BBC. / Regehr, K., Shaughnessy, C., Zhao, M., & Shaughnessy, N. (2024). *Safer Scrolling: How Algorithms Popularise and Gamify Online Hate and Misogyny for Young People*. University College London & University of Kent.

52 5Rights Foundation. (2021, September 17). *Pathways: How digital design puts children at risk*.

53 5Rights Foundation. (2022, September 17). *Just One Click - How digital design puts children at risk and how we can fix it*.

54 Howard, P., Neudert, L.-M., Prakash, N., & Vosloo, S. (2021). *Digital misinformation / disinformation and children*. In UNICEF. (p. 12). / Merrill, J., & Oremus, W. (2021, October 26). *Five points for anger, one for a "like": How Facebook's formula fostered rage and misinformation*. Washington Post.

55 Horwitz, J., & Seetharaman, D. (2020, May 26). *Facebook Executives Shut Down Efforts to Make the Site Less Divisive*. Wall Street Journal.

56 Vosoughi, S., Roy, D., & Aral, S. (2018). *The Spread of True and False News Online*. Science, 359(6380), 1146–1151.

57 King & Spalding. (2025, July 10). *The Global Content Regulation Landscape – Developments in the EU, UK, U.S., and Beyond*.

58 Afina, Y., Buchser, M., Krasodomski, A., Rowe, J., Sun, N., & Wilkinson, R. (2024, January 8). *Towards a global approach to digital platform regulation*. Chatham House. (p. 9).

59 Nash, V., & Felton, L. (2024). *Treating the Symptoms or the disease? Analysing the UK Online Safety Act's Approach to Digital Regulation*. Policy & Internet, 16(4).

60 Forbrukerrådet. (2024, November 14). *Commercial exploitation of children and adolescents online: How to ensure a rights-respecting digital childhood*. (p. 17).

61 Howard, P., Neudert, L.-M., Prakash, N., & Vosloo, S. (2021). *Digital misinformation / disinformation and children*. In UNICEF. (p. 11).

62 Dhamani, N., & Engler, M. (n.d.). *How Generative AI Makes Content Moderation Both Harder and Easier*. Integrity Institute. / Internet Society. (2025). *Global Online Safety Benchmark*. (p. 106).

63 Myers, A. (2023, February 27). *AI's Powers of Political Persuasion*. Stanford University. / Nightingale, S. J., & Farid, H. (2022). *AI-synthesized faces are indistinguishable from real faces and more trustworthy*. Proceedings of the National Academy of Sciences, 119(8).

64 UNICEF. (n.d.-a). *Generative AI: Risks and Opportunities for Children*.

65 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para. 36).

66 UNICEF, & UN Human Rights. (2024, November 18). *Taking a Child Rights-Based Approach to Implementing the UNGPs in the Digital Environment*. (p. 6).

67 OECD. (2021, January 8). *Children in the Digital Environment: Revised typology of risks*.

68 Kleinman, Z. (2020, November 6). *Popular app T&Cs "longer than Harry Potter"*. BBC.

69 Amnesty International. (2019, November 21). *Surveillance giants: How the business model of Google and Facebook threatens human rights*.

70 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para. 71).

71 Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). *Children's Data and Privacy Online: Growing up in a Digital Age - An Evidence Review*. In London School of Economics and Political Science. (p. 11). / 5Rights Foundation. (2024, June 22). *Twisted Toys: Toying With Children's Lives*.

72 Nemmaoui, S., Baslam, M., & Bouikhalene, B. (2023). *Privacy conditions changes' effects on users' choices and service providers' incomes*. International Journal of Information Management Data Insights, 3(1).

73 5Rights Foundation. (2023, October 3). *Digital Childhood*. / 5Rights Foundation. (2025, March 18). *Children & AI Design Code*.

74 Stoilova, M., Livingstone, S., & Atabey, A. (2025, September). *Children's rights in the age of generative AI: Perspectives from the global South*. London School of Economics and Political Science. (p. 10).
75 5Rights Foundation. (2023, October 3). *Digital Childhood*.
76 evealing Reality. (2025). *Children's Data Lives 2025*. Information Commissioner's Office
77 Revealing Reality. (2025). *Children's Data Lives 2025*. Information Commissioner's Office. (Chapter 2).
78 Benoliel, U., & Becher, S. (2019). *The Duty to Read the Unreadable*. Boston College Law Review. / Calver, T. (2018, July 6). *Social site terms tougher than Dickens*. BBC.
79 Office of the Privacy Commissioner of Canada, Commission d'accès à l'information du Québec, Office of the Information and Privacy Commissioner for British Columbia, & Office of the Information and Privacy Commissioner of Alberta. (2025, September 23). *Joint investigation of TikTok Pte. Ltd*. (Para. 95).
80 Stoilova, M., Bulger, M., & Livingstone, S. (2023). *Do parental control tools fulfil family expectations for child protection? A rapid evidence review of the contexts and outcomes of use*. Journal of Children and Media, 18(1), 29–49.
81 Revealing Reality. (2025). *Children's Data Lives 2025*. Information Commissioner's Office.
82 OECD. (2025, May 15). *How's Life for Children in the Digital Age?* (p. 22).
83 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Paras. 21 & 105).
84 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Paras. 39 & 70).
85 CIO Africa. (2019, May 15). *Government spends Sh27billion in Digital Literacy Programme*.
86 OECD. (2025, May 15). *How's Life for Children in the Digital Age?* (p. 22). See, for example, Meta. (2025, April 8). *We're Introducing New Built-In Restrictions for Instagram Teen Accounts, and Expanding to Facebook and Messenger*. / Presser, A. (2025, March 11). *New ways we're supporting parents and helping teens build balanced digital habits*. TikTok.
87 Pothong, K. (2019). *Youth Jury Policy Deliberation: Towards a Fair and Responsible Internet*. Children & Society, 34(1), 93–108. / Coleman, S., Pothong, K., Perez Vallejos, E., & Koene, A. (2017). *The Internet On Our Own Terms: How Children and Young People Deliberated About Their Digital Rights*. 5Rights Foundation.
88 Afina, Y., Buchser, M., Krasodomski, A., Rowe, J., Sun, N., & Wilkinson, R. (2024, January 8). *Towards a global approach to digital platform regulation*. Chatham House. (p. 19).
89 OECD. (2025, May 15). *How's Life for Children in the Digital Age?* (p. 22).
90 Internet Society. (2025). *Global Online Safety Benchmark*. (p. 106).
91 Béjar, A., Molly Rose Foundation, Cybersecurity for Democracy, Parents for Safe Online Spaces, Fairplay, & Heat Initiative. (2025, September 26). *Teen Accounts, Broken Promises*. Fairplay. (p. 9).
92 Stoilova, M., Bulger, M., & Livingstone, S. (2023). *Do parental control tools fulfil family expectations for child protection? A rapid evidence review of the contexts and outcomes of use*. Journal of Children and Media, 18(1), 29–49. / Internet Society. (2025). *Global Online Safety Benchmark*. (p. 106).
93 Wood, S. (2024, May 20). *Impact of regulation on children's digital lives*. London School of Economics and Political Science. / Stoilova, M., Bulger, M., & Livingstone, S. (2023). *Do parental control tools fulfil family expectations for child protection? A rapid evidence review of the contexts and outcomes of use*. Journal of Children and Media, 18(1), 29–49.
94 Family Online Safety Institute. (2025). *Connected and Protected: Insights from FOSI's 2025 Online Safety Survey*.
95 McNair, R., & Grimes, S. M. (2025, July 6). *Parental controls on children's tech devices are out of touch with child's play*. The Conversation.
96 Balt, E., Mérelle, S., Robinson, J., Popma, A., Creemers, D., van den Brand, I., van Bergen, D., Rasing, S., Mulder, W., & Gilissen, R. (2023). *Social media use of adolescents who died by suicide: lessons from a psychological autopsy study*. Child and Adolescent Psychiatry and Mental Health, 17.
97 Wood, S. (2024, May 20). *Impact of regulation on children's digital lives*. London School of Economics and Political Science. / Smirnova, S., Livingstone, S., & Stoilova, M. (2021, September). *Understanding of user needs and problems: a rapid evidence review of age assurance and parental controls*. EuConsent.
98 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para. 11).
99 Livingstone, S., & Sylwander, K. R. (2025). *There is no right age! The search for age-appropriate ways to support children's digital lives and rights*. Journal of Children and Media, 19, 6–12.

100 Dimou, I. (2025, October 8). *The global struggle to regulate children's social media use*. Digital Watch Observatory.
101 Livingstone, S., & Sylwander, K. R. (2025). *There is no right age! The search for age-appropriate ways to support children's digital lives and rights*. Journal of Children and Media, 19, 6–12.
102 OECD. (2025). *Age assurance practices of 50 online services used by children*.
103 Jargon, J. (2019, June 18). *How 13 Became the Internet's Age of Adulthood*. Wall Street Journal.
104 5Rights Foundation. (2021, October 21). *But how do they know it's a child? Age Assurance in the Digital World*. (p. 9-10). / Grimes, Grimes, S. M. (2021, July). *Digital Playgrounds: The Hidden Politics of Children's Online Play Spaces, Virtual Worlds, and Connected Games*. University of Toronto Press. (Chapter 6).
105 London School of Economics and Political Science. (n.d.). *Protecting, not excluding: why banning children from social media undermines their rights*.
106 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para. 4) / International Telecommunication Union. (2020). *Guidelines for policy-makers on Child Online Protection*. (p.3) / United Nations. (2024, September 22). *Global Digital Compact*. UN Office for Digital and Emerging Technologies. / United Nations. (2023, December 19). *UNGA Resolution 78/187 on the Rights of the Child in the digital environment*.
107 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para. 9).
108 Forbrukerrådet. (2024, November 14). *Commercial exploitation of children and adolescents online: How to ensure a rights-respecting digital childhood*. / Hempel, J. (2018, May 17). *What Happened to Facebook's Grand Plan to Wire the World?*. WIRED. / Tidy, J. (2024, February 4). *Facebook at 20: Four ways the app changed the world*. BBC.
109 5Rights Foundation. (2022, May 13). *Child Online Safety Toolkit*. (p. 27).
110 5Rights Foundation. (2025, March 17). *Analysis on the first round of Risk Assessment Reports under DSA*
111 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para 41). / Rahali, M., & Livingstone, S. (2022). *#SponsoredAds: Monitoring influencer marketing to young audiences*. London School of Economics and Political Science.
112 5Rights Foundation. (2025, March 18). *Children & AI Design Code*. (pp. 41-44).
113 Short, J., Schiller, R., Silbey, S., Jones, N., Hemmatian, B., & Bowman-Carpio, L. (2022). *The Dog That Didn't Bark: Looking for techno-libertarian ideology in a decade of public discourse about big tech regulation*. The Ohio State Technology Law Journal.
114 United Nations. (1989, November 20). *Convention on the Rights of the Child*. OHCHR. (Art. 1).
115 Livingstone, S., Carr, J., & Byrne, J. (2015). *One in Three: Internet Governance and Children's Rights*. (p. 8)..
116 United Nations. (1989, November 20). *Convention on the Rights of the Child*. OHCHR. (Art. 2(1)).
117 5Rights Foundation. (2023, October 3). *Digital Childhood*.
118 United Nations Committee on the Rights of the Child. (2016, December 6). *General comment No. 20 (2016) on the implementation of the rights of the child during adolescence*. OHCHR. (Para. 1).
119 Lansdown, G. (2005). *The evolving capacities of the child*. In digitallibrary.un.org. UNICEF Innocenti.
120 United Nations Committee on the Rights of the Child. (2016, December 6). *General comment No. 20 (2016) on the implementation of the rights of the child during adolescence*. OHCHR. (Para. 39)
121 UNICEF. (n.d.). *The ABCDE of Rights*.
122 Information Commissioner's Office. (n.d.). *Services covered by this code*. / Federal Trade Commission. (2020, July). *Complying with COPPA: Frequently Asked Questions.* / CEN/CENELEC, & IEEE. (2023). *Age appropriate digital services framework*. (Section 5 & 8). / Information Commissioner's Office. (n.d.-a). *"Likely to be accessed" by children – FAQs, list of factors and case studies*.
123 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para 4).
124 5Rights Foundation. (2025, March 18). *Children & AI Design Code*. (p. 14).
125 Business at OECD, & United States Council for International Business Foundation. (n.d.). *Privacy, Immersive Technologies and the Metaverse*.
126 Livingstone, S., & Sylwander, K. R. (2025). *There is no right age! The search for age-appropriate ways to support children's digital lives and rights*. Journal of Children and Media, 19, 6–12. (p. 9).

127 5Rights Foundation. (2021, September 17). *Pathways: How digital design puts children at risk*.
128 See for example: Robins-Early, N. (2025, October 27). *More than a million people every week show suicidal intent when chatting with ChatGPT, OpenAI estimates*. The Guardian. / Milmo, D., & Skopeliti, C. (2021, September 18). *Teenage girls, body image and Instagram's "perfect storm"*. The Guardian.
129 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Paras. 12, 13, & 110).
130 Livingstone, S., Cantwell, N., Özkul, D., Shekhawat, G., & Kidron, B. (2024, March). *The best interests of the child in the digital environment*. London School of Economics and Political Science.
131 United Nations Committee on the Rights of the Child. (2013, May 29). *General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1)*. (Para 39). / Livingstone, S., Cantwell, N., Özkul, D., Shekhawat, G., & Kidron, B. (2024, March). *The best interests of the child in the digital environment*. London School of Economics and Political Science.
132 United Nations Committee on the Rights of the Child. (2016, December 6). *General comment No. 20 (2016) on the implementation of the rights of the child during adolescence*. OHCHR. (Para. 22).
133 5Rights Foundation. (2025, March 18). *Children & AI Design Code*. (pp. 51-54). / 5Rights Foundation. (2023, October 3). *Digital Childhood*. (pp. 15-23).
134 5Rights Foundation. (2025, March 18). *Children & AI Design Code*. (p. 19 ). / 5Rights Foundation. (2023, October 3). *Digital Childhood*. (pp. 21-23).
135 Livingstone, S., Cantwell, N., Özkul, D., Shekhawat, G., & Kidron, B. (2024, March). *The best interests of the child in the digital environment*. London School of Economics and Political Science.
136 United Nations Committee on the Rights of the Child. (2013, May 29). *General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1)*. (Para. 97).
137 Fortim, I., & Zandavalli, S. D. (2025). *RIGHTS.AI: Children's Experiences of Generative Artificial Intelligence in Brazil*. London School of Economics and Political Science.
138 Baghdasaryan, B., Sivaneson, K., & Vosloo, S. (2025, September 26). *What's in a child's best interests online?* UNICEF.
139 United Nations Committee on the Rights of the Child. (2013, May 29). *General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1)*. (Para. 97).
140 Lenhart, A., & Owens, K. (2021). *The Unseen Teen: The Challenges of Building Healthy Tech for Young People*. Data & Society. / Livingstone, S., Carr, J., & Byrne, J. (2015). *One in Three: Internet Governance and Children's Rights*.
141 Office of the Privacy Commissioner of Canada, Commission d'accès à l'information du Québec, Office of the Information and Privacy Commissioner for British Columbia, & Office of the Information and Privacy Commissioner of Alberta. (2025, September 23). *Joint investigation of TikTok Pte. Ltd*.
142 5Rights Foundation. (2021, September 17). *Pathways: How digital design puts children at risk*. (p. 84). / Office of the Privacy Commissioner of Canada, Commission d'accès à l'information du Québec, Office of the Information and Privacy Commissioner for British Columbia, & Office of the Information and Privacy Commissioner of Alberta. (2025, September 23). *Joint investigation of TikTok Pte. Ltd*.
143 5Rights Foundation. (2021, October 21). *But how do they know it's a child? Age Assurance in the Digital World*.
144 5Rights Foundation. (2021, October 21). *But how do they know it's a child? Age Assurance in the Digital World*. (p.48). CEN/CENELEC, & IEEE. (2023). *Age appropriate digital services framework*. (Section 8.3). / OECD. (2024, June 19). *Towards digital safety by design for children*. (p.31).
145 5Rights Foundation. (2021, October 21). *But how do they know it's a child? Age Assurance in the Digital World*. (p.49). European Commission. (2025). *Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065*. (§36).
146 5Rights Foundation. (2021, October 21). *But how do they know it's a child? Age Assurance in the Digital World*. (p.48-50).
147 5Rights Foundation. (2021, October 21). *But how do they know it's a child? Age Assurance in the Digital World*. (p.48).
148 5Rights Foundation. (2021, October 21). *But how do they know it's a child? Age Assurance in the Digital World*. (pp.48-53).
149 IEEE Standards Association. (2024, March 21). *IEEE 2089.1 Standard for Online Age Verification*. (Art. X(b)).

150 United Nations Working Group on Business and Human Rights. (2025). *Artificial intelligence procurement and deployment: ensuring alignment with the Guiding Principles on Business and Human Rights*.
151 UNICEF. (2025, July). *Assessing child rights impacts in relation to the digital environment*.
152 United Nations Committee on the Rights of the Child. (2013, April 17). *General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights*. (Paras. 78-81).
153 UNICEF. (2025, July). *Assessing child rights impacts in relation to the digital environment*.
154 International Telecommunication Union. (2020). *Guidelines for industry on Child Online Protection*. (p. 28).
155 Mukherjee, S., Pothong, K., & Livingstone, S. (2021). *Child Rights Impact Assessment: A tool to realise child rights in the digital environment*. 5Rights Foundation. (p.10). / United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para. 38). / United Nations Committee on the Rights of the Child. (2013a, April 17). *General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights*. (Para. 78). / Livingstone, S., Lievens, E., & Carr, J. (2020). *Handbook for policy makers on the rights of the child in the digital environment*. Council of Europe. (p.19).
156 United Nations Committee on the Rights of the Child. (2003, November 27). *General comment No. 5 (2003): General measures of implementation of the Convention on the Rights of the Child*. (Para. 45).
157 Mukherjee, S., Pothong, K., & Livingstone, S. (2021). *Child Rights Impact Assessment: A tool to realise child rights in the digital environment*. 5Rights Foundation. (p. 3).
158 IEEE Standards Association. (2021, November 9). IEEE 2089 Standard for an *Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children*. (pp. 43-44).
159 Rights Foundation. (2025, March 18). *Children & AI Design Code*. (p. 49).
160 5Rights Foundation. (2023, April 11). *Disrupted Childhood: The cost of persuasive design*. / 5Rights Foundation. (2021, September 17). *Pathways: How digital design puts children at risk*.
161 Amnesty International. (2023, November 7). *"I Feel Exposed": Caught in TikTok's Surveillance Web*. / Information Commissioner's Office. (2025, March 3). *Investigations announced into how social media and video sharing platforms use UK children's personal information*.
162 Spool, J. (2011, September 14). *Do users change their settings?* UIE. / Ng, A. (2019, December 21). *Default settings for privacy -- we need to talk*. CNET.
163 SuperAwesome. (2018, June 12). *SuperAwesome launches Kid-Safe Filter to prevent online ads from stealing children's personal data*.
164 Pixalate. (2022). *Mobile Apps: Google vs. Apple COPPA Scorecard*.
165 Pixalate. (2022). *Mobile Apps: Google vs. Apple COPPA Scorecard*.
166 International Conference of Data Protection and Privacy Commissioners. (2010). *Resolution on Privacy by Design*.
167 Cavoukian, A. (2009, August). *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario. / European Union. (2016, April 27). *General Data Protection Regulation*.
168 OECD. (2024, June 19). *Towards digital safety by design for children*. (p. 7). / Polo, N. (2025, August 29). *Will the UK AI Bill protect people and society?* Ada Lovelace Institute.
169 Tech Oversight Project. (2026, January 25). *Unsealed Court Documents Show Teen Addiction was Big Tech's "Top Priority"*.
170 Ofcom. (2025, June 26). *Research into persuasive design features and potential child financial harms*.
171 5Rights Foundation. (2022, February 3). *Risky by Design – In-game purchases*.
172 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para. 42).
173 5Rights Foundation. (2021, October 4). *Tick to Agree: Age appropriate presentation of published terms*. (pp. 8-9).
174 Hsieh, M. H. (2009). *A case of managing customer relationship management systems: Empirical insights and lessons learned*. International Journal of Information Management, 29(5), 416–419. / Jadil, Y., Rana, N. P., & Dwivedi, Y. K. (2022). *Understanding the drivers of online trust and intention to buy on a website: An emerging market perspective*. International Journal of Information Management Data Insights, 2(1).
175 Benoliel, U., & Becher, S. (2019). *The Duty to Read the Unreadable*. Boston College Law Review.
176 Calver, T. (2018, July 6). *Social site terms tougher than Dickens*. BBC.
177 Sandle, T. (2020, January 29). *Report finds only 1 percent reads "Terms & Conditions"*. Digital Journal.
178 Nemmaoui, S., Baslam, M., & Bouikhalene, B. (2023). *Privacy conditions changes' effects on users' choices and service providers' incomes*. International Journal of Information Management Data Insights, 3(1).

179 UC Berkeley School of Information. (2021, July 9). *Do we actually agree to these terms and conditions?*
180 Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). *Children's Data and Privacy Online: Growing up in a Digital Age - An Evidence Review*. In London School of Economics and Political Science. (p. 11).
181 nited Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para. 39).
182 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para. 36).
183 Office of the Privacy Commissioner of Canada, Commission d'accès à l'information du Québec, Office of the Information and Privacy Commissioner for British Columbia, & Office of the Information and Privacy Commissioner of Alberta. (2025, September 23). *Joint investigation of TikTok Pte. Ltd*.
184 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Paras. 35-39).
185 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para. 70).
186 Conscious Advertising Network. (2025, April 17). *Children's Rights and Wellbeing Guide*.
187 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para. 38).
188 5Rights Foundation. (2025, March 18). *Children & AI Design Code*. (p. 42).
189 UNICEF. (2025, June). *Guidance for business*.
190 Wood, S. (2024, May 20). *Impact of regulation on children's digital lives*. London School of Economics and Political Science. (p. 74). / UNICEF, & UN Human Rights. (2024, November 18). *Taking a Child Rights-Based Approach to Implementing the UNGPs in the Digital Environment*. (pp. 17-18).
191 5Rights Foundation. (2025, March 18). *Children & AI Design Code*. (pp. 40-41).
192 5Rights Foundation. (2025, March 10). *Advancing Trust & Safety: systems and standards for online safety professionals*. / eSafety Commissioner. (2024, July). *Basic Online Safety Expectations: Regulatory Guidance*.
193 Information Commissioner's Office. (n.d.-b). *Governance and accountability*.
194 5Rights Foundation. (2025, March 18). *Children & AI Design Code*. (pp. 15-16).
195 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Paras. 24, 39, & 56).
196 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Paras. 25, 39, 56, 62, 74, 103, & 124).
197 Conscious Advertising Network. (2025, April 17). *Children's Rights and Wellbeing Guide*.
198 5Rights Foundation. (2025, March 18). *Children & AI Design Code*. (pp. 43-44).
199 EEE Standards Association. (2025, July 25). *IEEE Online Age Verification Certification Program*.
200 da Mota, M. (2024, February 12). *Voluntary Codes of Practice for AI Lack Accountability*. Centre for International Governance Innovation.
201 Digital Futures Commission. (2023). *A Blueprint for Education Data: Realising children's best interests in digitised education*. / United Nations Working Group on Business and Human Rights. (2025). *Artificial intelligence procurement and deployment: ensuring alignment with the Guiding Principles on Business and Human Rights*.
202 UNICEF, & UN Human Rights. (2024, November 18). *Taking a Child Rights-Based Approach to Implementing the UNGPs in the Digital Environment*. (p. 7).
203 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para. 35). /United Nations Committee on the Rights of the Child. (2013, April 17). *General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights*. (Paras. 28, 42 and 82) / United Nations. (2012, January 1). *Guiding Principles on Business and Human Rights*. OHCHR.
204 Research shows that while *3-in-4 children* are aware of these tools, they often question whether they should take the steps to report as they *feel it rarely leads to take-downs*.
205 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Paras. 36 & 55).
206 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para. 44).
207 Baghdasaryan, B., Sivaneson, K., & Vosloo, S. (2025, September 26). *What's in a child's best interests online?* UNICEF.

208 5Rights Foundation. (2025, March 18). *Children & AI Design Code*. (pp. 44-47).
209 United Nations Committee on the Rights of the Child. (2013, April 17). *General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights*. (Para. 61).
210 Dubiniecki, A. (2024, January 25). *Trustworthy AI: String Of AI Fails Show Self-Regulation Doesn't Work*. Forbes.
211 Gillespie, N., & Lockey, S. (2025, April 29). *Global study reveals trust of AI remains a critical challenge*. Melbourne Business School.
212 Koch, R. (2025, January 17). *Big Tech earns enough in less than 3 weeks to pay all 2024 fines*. Proton.
213 Atabey, A., & Hooper, L. (2024). *International regulatory decisions concerning EdTech companies' data practices*. London School of Economic and Political Science. (pp. 4-5).
214 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Paras. 37, 82, and 114).
215 United Nations Committee on the Rights of the Child. (2013, April 17). *General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights*. Refworld. (Para. 61(a)).
216 Wood, S. (2024, May 20). *Impact of regulation on children's digital lives*. London School of Economics and Political Science. (p. 75).
217 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para. 124). Wood, S. (2024, May 20). *Impact of regulation on children's digital lives*. London School of Economics and Political Science. (p. 75) / International Telecommunication Union. (2020). *Guidelines for policy-makers on Child Online Protection*. (pp. 30-31). / Afina, Y., Buchser, M., Krasodomski, A., Rowe, J., Sun, N., & Wilkinson, R. (2024, January 8). *Towards a global approach to digital platform regulation*. Chatham House. (p. 45).
218 Wood, S. (2024, May 20). *Impact of regulation on children's digital lives*. London School of Economics and Political Science. / John, M., & Kate, B. (2024, March). *UK Age-Appropriate Design Code: Impact Assessment*. Children and Screens.
219 United Nations. (1989, November 20). *Convention on the Rights of the Child*. OHCHR. (Art. 16).
220 United Nations. (1989, November 20). *Convention on the Rights of the Child*. OHCHR. (Art. 36).
221 United Nations. (1989, November 20). *Convention on the Rights of the Child*. OHCHR. (Art. 19).
222 United Nations. (1989, November 20). *Convention on the Rights of the Child*. OHCHR. (Art. 13).
223 United Nations. (1989, November 20). *Convention on the Rights of the Child*. OHCHR. (Art. 14)
224 United Nations. (1989, November 20). *Convention on the Rights of the Child*. OHCHR. (Art. 28).
225 United Nations. (1989, November 20). *Convention on the Rights of the Child*. OHCHR. (Art. 31).
226 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para. 37).
227 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para. 4).
228 UNICEF, & UN Human Rights. (2024, November 18). *Taking a Child Rights-Based Approach to Implementing the UNGPs in the Digital Environment*.
229 United Nations Committee on the Rights of the Child. (2021, March 21). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. OHCHR. (Para. 35). / United Nations Committee on the Rights of the Child. (2013, April 17). *General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights*. (Paras. 28, 42 and 82). / UNICEF, & UN Human Rights. (2024, November 18). *Taking a Child Rights-Based Approach to Implementing the UNGPs in the Digital Environment*.
230 Sylwander , K. R., & Livingstone, S. (2026, March 2). *Mapping the global impact of UNCRC General comment No. 25 on children's rights in the digital environment*. London School of Economics and Political Science.
231 International Telecommunication Union. (2020). *Guidelines for policy-makers on Child Online Protection*. (pp. 2-3).
232 International Telecommunication Union. (2021). *Keeping children safe in the digital environment: The importance of protection and empowerment*. (pp. 5-6).
233 OECD. (2012, February 16). *Recommendation of the Council on Children in the Digital Environment*. (III(5)).
234 OECD. (2012, February 16). *Recommendation of the Council on Children in the Digital Environment*. (III(4)).
235 G20. (2021, August 5). *High Level Principles for Children Protection and Empowerment in the Digital Environment*. (Section 2, 2.5).

236 Global Privacy Assembly. (2025). *Global Privacy Assembly*.
237 United Nations. (2023, December 19). *UNGA Resolution 78/187 on the Rights of the Child in the digital environment*. (OC 37).
238 Global Online Safety Regulators Network. (2023, September). *Position Statement: Human Rights & Online Safety Regulation*. (pp. 2-3).
239 OECD. (2024, June 19). *Towards digital safety by design for children*. (p. 6).
240 United Nations. (2024, September 22). *Global Digital Compact*. UN Office for Digital and Emerging Technologies. (Para. 23(c)).
241 United Nations. (2024, September 22). *Global Digital Compact*. UN Office for Digital and Emerging Technologies. (Para. 31(b)).
242 United Nations Secretary-General's High-level Advisory Body on AI. (2024, September). *Governing AI for Humanity*. (p. 32).
243 Office of the United Nations High Commissioner for Human Rights. (n.d.). *Business and Human Rights in Technology Project*.
244 UNICEF, & UN Human Rights. (2024, November 18). *Taking a Child Rights-Based Approach to Implementing the UNGPs in the Digital Environment*.
245 African Union. (1999, November 29). *African Charter On The Rights And Welfare Of The Child*. (Art. 10). / United Nations. (1989, November 20). *Convention on the Rights of the Child*. OHCHR. (Art. 16).
246 African Union. (1999, November 29). *African Charter On The Rights And Welfare Of The Child*. (Art. 15). / United Nations. (1989, November 20). *Convention on the Rights of the Child*. OHCHR. (Art. 36).
247 African Union. (1999, November 29). *African Charter On The Rights And Welfare Of The Child*. (Art. 9) / and United Nations. (1989, November 20). *Convention on the Rights of the Child*. OHCHR. (Art. 14).
248 African Committee of Experts on the rights and Welfare of the Child. (2021). *General Comment No. 7 on article 27 on Sexual Exploitation of the African Charter on the Rights and Welfare of the Child*. (Para. 55).
249 African Committee of Experts on the Rights and Welfare of the Child. (2023). *Day of the African Child 2023 Concept Note*. (Para. 5).
250 Council of Europe. (2018, September). *Guidelines to respect, protect and fulfil the rights of the child in the digital environment*. (Paras. 52-53).
251 Organization of American States. (2018, January). *Guidelines for Empowering and Protecting Child and Adolescent Rights on the Internet in Central America and the Dominican Republic*. (p. 4).
252 Organization of American States. (2018, January). *Guidelines for Empowering and Protecting Child and Adolescent Rights on the Internet in Central America and the Dominican Republic*. (p. 19).
253 Davidson, J., Kidron, B., & Phillips, K. (2019, September 22). *Rwanda Child Online Protection Policy*. 5Rights Foundation. 5.4.4(A).
254 Davidson, J., Kidron, B., & Phillips, K. (2019, September 22). *Rwanda Child Online Protection Policy*. 5Rights Foundation. 5.4.2(C).
255 Davidson, J., Kidron, B., & Phillips, K. (2019, September 22). *Rwanda Child Online Protection Policy*. 5Rights Foundation. 5.4.4(B).
256 Davidson, J., Kidron, B., & Phillips, K. (2019, September 22). *Rwanda Child Online Protection Policy*. 5Rights Foundation. 5.4.4(E).
257 5Rights Foundation. (2022c, September 2). *Approaches to children's data protection: A comparative international mapping*. / UNICEF. (2025a, May). *Innovations in Data Governance for Children - Children's Codes*.