

Online Harms & Digital Safety Position Paper

UNICEF Canada
February 2026

Background – Children’s Digital Lives

The current generation of children in Canada has grown up in an era of digital immersion, characterized by unprecedented access to smartphones, the internet, and social media from early childhood. With children representing approximately one-third of all internet users globally, being online has become a lifeline for many, enabling learning, play, self-expression, and connection to friends and family ([UNICEF, 2025](#); [United Nations Human Rights Office of the High Commissioner, 2025](#)). As a result, digital environments play a central role in children’s daily lives and development.

At the same time, this extensive digital engagement has shaped children’s online behaviors in ways that require greater attention to both digital risks and protective measures. Social media platforms and other forms of online services can expose children to increased risks of online harms, including bullying, sexual and commercial exploitation, self-harm, cyber-related hate speech, misinformation and disinformation, and privacy violations. These harms can have serious and lasting impacts on children’s mental health, safety and wellbeing. Children who experience online sexual abuse or bullying have significantly higher levels of anxiety, more suicidal thoughts and behaviors, and are more likely to self-harm ([UNICEF Innocenti, 2025](#)). As a signatory to the [United Nations Convention on the Rights of the Child](#), Canada has an obligation to protect children from harm and defend their best interests, including in the digital world.

Many jurisdictions around the world are exploring social media bans for young people in response to these risks, but age-based restrictions alone are not sufficient to address the challenges posed by rapidly evolving digital technologies. Duty holders, including platforms, governments and parents/caregivers, share responsibility for creating safe online environments and protecting children from harm. Effective policy must be evidence-based and grounded in a child rights framework, and a comprehensive, multi-layered approach is essential to recognize the complexity of children’s online experiences. To support safe digital engagement for children, the following actions are recommended:

- 1) Parents, caregivers, governments and private actors must center children’s rights in digital governance decisions to ensure their safe, meaningful and equitable participation;
 - 2) Governments should invest into the development of age-appropriate digital literacy programs for children, parents, and educators, ensuring all users understand online risks, data practices, and algorithmic influences;
-

- 3) Duty holders, including governments and private companies, should mandate the use of Child Rights Impact Assessments (CRIA) across the design, development, deployment and regulation of digital products and services that impact children; and
- 4) Governments should develop comprehensive, proactive and future-proof legislation, standards and regulatory frameworks that uphold and advance children’s rights and hold digital platforms accountable for online safety. Frameworks must address emerging risks from Artificial Intelligence (AI) and include review mechanisms to adapt to future technological developments.

The Best Interests of the Child in Digital Spaces

Importance of Child Participation

Children today spend more time in digital spaces than ever before ([UNICEF Innocenti, 2024](#)). Nearly half of UNICEF Canada U-Reporters (46%) report spending four to six hours per day online or on their phones outside of school hours, while 22% spend seven to nine hours online daily ([U Report, 2025](#)). This growing digital presence presents significant opportunities to empower children in ways not previously possible. Digital environments can advance the realization of children’s rights by enabling participation across civil, political, cultural, economic, and social domains. However, without appropriate safeguards, they may exacerbate harms and inequities, or create new ones. In [General Comment No. 25](#) on children’s rights in relation to digital environments, children themselves emphasized that digital spaces should support, promote and protect their safe and equitable participation. Doing so requires that children are afforded agency and opportunity to shape digital space systems, consistent with their evolving capacities, and are supported to make informed decisions about their online presence and its impacts. Promoting meaningful and safe participation is a shared responsibility among parents, caregivers, governments, and private actors. Policies and regulations on digital safety should be informed by meaningful consultation with children and youth, and any approach that involves age-based restrictions must also consider how to fill the gap that may be left by fostering safe and healthy in-person spaces for connection and belonging.

Responsibility of Duty Holders

A) Parents and Caregivers

As in the physical world, caregivers have a duty to protect children and keep them safe in online spaces. Yet many parents and caregivers did not grow up as digital natives, making it essential that they receive support to understand online risks, recognize warning signs, and engage in informed conversations with their children about digital safety. Meaningful investment in digital literacy education for both children and adults is critical to

ensure that young people are equipped with the knowledge and skills to navigate digital environments safely and can rely on trusted adults when they encounter harmful content.

Digital literacy extends beyond technical know-how; it encompasses the knowledge, skills and attitudes that enable children to be both safe and empowered in an increasingly digital world ([UNICEF Innocenti, 2019](#)). Effective digital literacy education helps children identify credible information, protect their personal data, understand how algorithms shape what they see, and respond safely when confronted with inappropriate or distressing content. Parents, caregivers, and educators need accessible, up-to-date resources that demystify digital platforms and provide practical guidance for supporting children online.

Nonetheless, even with strong digital literacy and engaged caregivers, the ubiquity of social media platforms, chatbots and algorithms-driven content means that families and educators cannot reasonably be expected to shoulder full responsibility for mitigating children's exposure to harmful content. Placing the burden entirely on households ignores the structural nature of these risks and the profound imbalance between children and the systems that shape their online experiences. All actors have a role to play in promoting children's digital safety, and that responsibility must be upheld across the digital ecosystem.

B) Governments & Companies

[Article 3.1 of the United Nations Convention on the Rights of the Child](#) (UNCRC), together with General Comment No. 16 on the best interests of the child, affirms that all decisions made by governments, private actors, and public and private welfare organizations should prioritize the best interests of the child. Accordingly, both governments and private companies are duty bearers in safeguarding children and youth online and must take proactive action to prevent and mitigate online harm.

Government

The Government of Canada has a duty to respect, protect and fulfil the rights of every child, without discrimination, through effective legislation, regulation and enforcement & accountability mechanisms. Child-centered governance should be grounded in international human rights law, explicitly recognizing internationally agreed standards and principles including the Convention on the Rights of the Child and the principle of the best interests of the child. Legislation should apply to all digital platforms and services that children use, or that are likely to impact their rights, and should be informed by evidence, research and children's own lived experiences and perspectives. In parallel, governments should invest in digital literacy initiatives that equip children, parents, and caregivers with the knowledge and skills needed to navigate digital environments safely, critically, and confidently. In the development of legislation, governments should

conduct and require the application of Child Rights Impact Assessments (CRIAs) to identify, prevent and mitigate potential adverse impacts on children's rights.

Translating these policy commitments into meaningful protection in practice requires a comprehensive and coordinated regulatory approach. Government regulation should therefore be embedded within a broader, holistic framework that protects children without displacing them into unregulated or unsafe digital spaces. This framework should ensure that all actors, including digital platforms and service providers, meet their duty of care to uphold children's rights. To assess whether regulatory approaches are achieving their intended outcomes, governments should establish robust monitoring and evaluation frameworks, including tracking behavioral changes, well-being indicators, and broader social outcomes over time.

Companies

Social media and technology companies have a duty to design products and platforms with children's safety at the core, yet many continue to build systems that overlook children's needs and vulnerabilities. Harmful and manipulative content that promotes children's harmful engagement is relentlessly served through popular influencers, algorithms, and bots. Children's data is often harvested to shape their beliefs and influence their actions through microtargeted content, enabling digital services to compile extensive profiles of children's interests, behaviors, and online activity. Together, these practices allow algorithms to predict and promote content that will keep them scrolling, clicking, watching, and sharing.

The [United Nations Guiding Principles on Business and Human Rights](#) affirm that all businesses have the responsibility to identify, prevent, mitigate and, where appropriate, remediate their potential or actual negative impacts on human rights. To this end, companies should conduct human rights due diligence (HRDD) to understand systemic risks to children arising from the company's operations through Digital Child Rights Impact Assessments (D-CRIA). Businesses should report material impacts, risks, and opportunities related to child rights in the digital environment in their most relevant mainstream public financial filings, management reports, and/or sustainability reports.

Companies must prioritize transparency as a core element of child-centered design. Children and their caregivers should be provided with clear, accessible, and age-appropriate explanations of how data are collected, used, and shared. Disclaimers and notices should be provided in child-friendly language that supports informed decision-making rather than obscuring risks. Platforms should also offer meaningful opt-in and opt-out mechanisms for data collection and personalization, ensuring that children can exercise choice over their digital experiences. Robust transparency and consent practices are essential to building trust and safeguarding children's rights in an increasingly data-driven digital ecosystem.

Emerging Risks: Artificial Intelligence

Artificial intelligence plays an increasingly central role in the digital platforms, applications and devices that children use daily, shaping what they see, learn and who they connect with online. 58% of UNICEF Canada U-Reporters report using AI either all the time (12%), once a day (15%) or a few times a week (31%) ([U Report, 2025](#)). As the largest cohort of internet users, children will be disproportionately affected by AI across their life course (UNICEF Innocenti, 2025). While AI offers important benefits, including personalized learning, creativity, and early health detection, it also exposes children to significant risks, such as misinformation, harmful or illegal content, manipulation, developmental harms, privacy violations and unsafe AI-generated responses. In light of rapid technological change, robust legislation, standards and ethical frameworks are required to ensure children's rights are respected across the design, deployment and use of AI systems. These frameworks should establish clear guidance on regulatory oversight, mandatory testing and risk assessments for AI systems, including Child Rights Impact Assessments, strong protections for children's data, and measures to prevent AI-enabled crimes such as child sexual abuse and exploitation. To remain effective in a fast-changing technological landscape, such policies should be future-proof: flexible, adaptable, and subject to regular review and updates to ensure they continue to uphold and advance children's rights over time in the face of rapid technological development.

ABOUT UNICEF CANADA

UNICEF is the world's farthest-reaching humanitarian organization for children. Across more than 190 countries and territories, and in the world's toughest places, we work day in and day out to defend children's human rights and a fair chance to fulfil their potential, guided by the 1989 Convention on the Rights of the Child.

We thank the Committee for considering our recommendations and welcome the opportunity to appear as a witness to elaborate further. **For more information, please contact: Rebecca Davidson, Chief Programs Officer:** rdavidson@unicef.ca
