Enforcing Child-Centred Digital Safety:

Charting Canada's Legislative Path with International Best Practices

APRIL 2026

Canadian Paediatric Society

SickKids®

Child Health Policy Accelerator

Acknowledgments

Prepared by:

Reshma Patel, MPH
Clinical Research Project Coordinator,
SickKids Child Health Policy Accelerator

Teerka Baskaran
Policy and Research Intern,
SickKids Child Health Policy Accelerator

Gwendolyn Moncrieff-Gould
Policy Lead, Child Health Policy Accelerator

Charlotte Moore Hepburn, MD, FRCPC, FAAP
Medical Director, SickKids Child Health Policy Accelerator
Associate Professor, Department of Paediatrics, University of Toronto
Faculty Paediatrician,
The Hospital for Sick Children

Reviewed by

(in alphabetical order):

Samantha Grills, M.A.
Manager, Government Relations,
Canadian Paediatric Society

Jamie McCourt, MPPA
Policy Coordinator, Canadian Paediatric Society

Rachel Mitchell, MD, M.Sc., FRCPC
Assistant Professor, Department of Psychiatry, University of Toronto
Associate Scientist, Hurvitz Brain Sciences Research Program, Sunnybrook Research Institute
Staff Psychiatrist, Mood and Anxiety Disorders Program, Sunnybrook Health Sciences Centre

Alene Toulany, MD, M.Sc., FRCPC
Associate Professor, Department of Paediatrics, University of Toronto
Associate Scientist, Child Health Evaluative Sciences Program
Staff Physician, Division of Adolescent Medicine, The Hospital for Sick Children

Ashley Vandermorris, MD
Assistant Professor, Department of Pediatrics, University of Toronto
Staff Pediatrician, Adolescent Medicine, The Hospital for Sick Children
Co-Lead, Fraser Mustard Institute for Human Development Policy Bench

Acknowledgements

This white paper was prepared with the generous support of the **Waltons Trust** and **One Child Every Child**. We are grateful for their ongoing partnership.

Executive Summary

Children's and youth's lives have been profoundly reshaped by digital platforms and services, transforming how young people learn, play, socialize, and perceive the world. The rapid integration of social media accounts, anthropomorphic technologies[1] (e.g., artificial intelligence [AI] chatbots), and data extracting software (e.g., location tracking) into everyday life has outpaced legislative safeguards, leaving children and youth exposed to greater levels of manipulation and risk than ever before.[2] While digital technologies can facilitate some opportunities for education and positive social interaction, an unregulated digital environment has led to significant harm to the mental and physical health and safety of children and youth.[3]

In 2020, Canadian children and youth ranked 31st out of 38 high-income countries in overall mental well-being, underscoring the need to strengthen supports for young people in Canada.[4] Enacting online safety legislation is a necessary step, given consistent evidence linking exposure to digital harms, including excessive use and harmful content,[5–7] to increased risks of depression, anxiety, and other adverse health outcomes in children and youth.[8,9] Global leaders, including Australia, the European Union, and the United Kingdom, have taken significant steps to protect children and youth online by enacting comprehensive online safety legislation with paediatric-specific protections. Canada's continued failure to pass comparable legislation and to align with international best practices and policies highlights an urgent need for coordinated policy and legislative action.

With an aim to protect children and youth from the harms associated with illegal or harmful online content, to safeguard young people from deceptively designed digital products and services that monetize their personal data and fuel addictive use,[10] and to ensure technology companies are accountable for the online environments they create and—as of now—control, the federal government should:

1. Establish an independent online safety regulator with the authority, expertise, and resources to administer, monitor, and enforce compliance with online safety regulations. The mandate of the regulator should apply to all digital platforms, including social media, online gaming, online gambling, and generative AI, and should remain flexible enough to include emerging technologies.

2. Introduce a statutory duty of care on online platforms and services to act responsibly and safely in their operation and design, and to take reasonable measures to protect children and youth from harm.

3. Adopt a design-based approach that moves beyond content moderation and age-gating by requiring platforms to implement safety-by-design measures including, but not limited to, risk assessments, privacy by default, and user empowerment for children and youth. Platforms must be required to assess and mitigate systemic risks, with meaningful penalties for non-compliance.

4. Develop and enforce a children's code to guide the enforcement of the independent regulator's child safety duties. The code must outline age- and stage-specific regulator duties and enforceable standards for services accessible to minors. It should be developed through broad consultation with civil society, including paediatricians, other child and youth care providers, caregivers, and children and youth themselves.

By acting on these recommendations, Canada can promote the health, educational, and developmental well-being of its youngest citizens, and increase alignment across international jurisdictions in this rapidly evolving digital regulatory environment.

Introduction

Today, more than 99 per cent of Canadian youth aged 15 to 24 are online and over 91 per cent use social networking sites.[11] Over 70 per cent of Canadian children aged 12 to 17 exceed a recommended two-hour daily limit of recreational screen time on school days, rising to 87 per cent on non-school days.[12] One Canadian study found that 57 per cent of children aged as young as 6 to 10 report frequent exposure to social media through platforms such as YouTube, Snapchat, and Facebook.[13] One in five young people also report negative mental and physical health effects linked with their online experiences,[9] effects that paediatricians see every day in outpatient clinics, emergency rooms, and inpatient wards across the country. These harms are driven, in part, by digital platforms that expose children to harmful,[5–7] violent,[14–16] and sexually exploitative content,[17] which has been linked to anxiety, depression,[9,18] disordered eating,[19] self-harm,[6,20] and the normalization of hatred and violence.[16]

During the critical stages of social and emotional development in childhood and adolescence, children and youth are uniquely vulnerable in the online environment and especially sensitive to social feedback, peer approval, and reward-based behavioural incentivization. We should not leave children and youth to navigate this unregulated digital world on their own.

The architecture of digital platforms is designed to monetize[21,22] and cultivate addictive use.[23] Features such as infinite scroll, autoplay, personalized content recommendation algorithms, popularity metrics, frictionless sharing, anonymity, in-app purchases, and "friend" suggestions are engineered to keep users—especially children and youth—engaged for extended periods. These engagement-driven design choices align directly with the underlying business model of several digital platforms and services, which is dependent on sustained engagement to maximize profit through continuous collection, analysis, and sale of personal data.[24]

Within this "attention economy," human attention has been transformed into a commodity, with addictive design features serving as the tools to harvest profit: the longer a child stays online, the more data are captured and monetized, providing greater incentive to incorporate addictive design features that drive prolonged and frequent engagement.[25–27] On average, technology companies collect 72 million data points on a child before they turn 13, and over 70 per cent of the most popular platforms use children's information to generate revenue.[28]

Internationally, many of Canada's closest allies have already enacted online safety laws that foster safer digital environments for children and impose meaningful accountability on technology companies.[29–33] Canada must learn from existing international models, adopt emerging best practices, and align with peer nations to prioritize the safety, privacy, and well-being of children and youth.

Canadian Context

Federal

There is overwhelming public support for federal online safety regulations in Canada.[34–36] In parallel, the Canadian government has acknowledged the urgency of regulating digital platforms, particularly to address specific public safety, national security,[37] and media-related concerns.[38] However, recent multi-partisan efforts have yielded limited success, and multiple bills have failed to receive royal assent.

In the 44th Parliament, three key pieces of legislation were introduced, yet none passed before Parliament prorogued in early 2025.

- **Bill C-63**,[39] also known as the *Online Harms* Act, was introduced by the Liberal government, and proposed a duty of care, an independent online safety regulator, and amendments to the *Canadian Human Rights Act* and *Criminal Code* to strengthen protections against hate-motivated offences. It faced criticism over its broad scope, the risk of over-censorship, and potential threats to freedom of expression.[40]

- **Bill C-412**,[41] a Conservative private member's bill entitled *The Protection of Minors in the Digital Age Act and to amend the Criminal Code*, proposed a requirement for social media platforms to remove harmful content under threat of significant fines, but it lacked appropriate enforcement strategies and did not establish an independent online regulator to oversee new accountabilities for online platforms.

- Addressing a distinct but related issue, the *Artificial Intelligence and Data Act*, part of **Bill C-27**,[42] aimed to regulate commercial AI use to ensure safety, transparency, and accountability. Criticisms of the bill included unclear definitions, limited enforcement mechanisms, and concerns over stifling innovation.

Provincial/Territorial

Provinces have also pursued efforts to hold platforms financially accountable for health and education-related harms. In 2024, British Columbia (B.C.) introduced **Bill 12**,[43] the *Public Health Accountability and Cost Recovery Act*, to enable the Government of B.C. to pursue legal action to

recover health-care costs from social media companies. Following significant pushback from industry, the province paused the legislation and launched the Online Safety Action Table.[44] This voluntary forum, which included the B.C. government and several global technology giants (including Meta, TikTok, X, Google, and Snapchat), has failed to secure any meaningful commitments related to child protection,[45] underscoring the limits of voluntary measures.

In Ontario, a group of 14 school boards and schools, known as Schools for Social Media Change, launched a $4.5 billion lawsuit against Meta, Snapchat, and TikTok, alleging that negligently designed platforms are addictive and disrupt student learning and youth mental health,[46] resulting in significant harms and costs to the education system.[47] At the time of writing, the outcome of the Ontario lawsuit remains pending.

By fall 2024, all provinces[48] had introduced policies limiting student cell phone use in schools.[49] These interventions vary considerably in both scope and implementation. While principals, educators, and students generally report positive outcomes, such as increased focus and socialization, challenges remain regarding consistent enforcement and rigorous evaluation, limiting the policy's effectiveness.[50,51] Most Canadians view the bans as either not very effective or not effective at all (43%) or remain unaware of the policy (23%) .[52] Moreover, school-based regulations do not address the significant amount of time youth spend online outside of school.

Online Harms

Online safety legislation is strongest in Canada on cybercrime, including child sexual exploitation and cyberbullying. Since 2014, youth-victim cybercrime reports have more than doubled.[53] Canada's national tipline for reporting child sexual exploitation, Cybertip.ca, has received over 4.3 million reports referring cases to local law enforcement.[54] Canada's National Strategy for Protecting Children from Sexual Exploitation on the Internet was created in 2004 and, through this strategy, the Government of Canada invests over $27 million annually to "combat sexual online exploitation."[55] While the National Strategy supports essential programming, including the Canadian Centre for Child Protection (C3P), greater resources and attention must also be invested in proactive measures to reduce the number of children and youth victimized online.

Coordinating Action

In recent years, parent groups, educators, public health organizations, and professional societies have actively worked to reduce online harm through advocacy, education, and support initiatives—promoting digital literacy and safe online practices at home and in school, while developing parent, caregiver, and youth guidance on navigating social media safely. In parallel, youth-led initiatives from Young Politicians of Canada[56] and Heads Up (the Dais),[57] among others, have worked to ensure that young people's perspectives inform federal policy

and practice. Despite these wide-reaching efforts, challenges remain in scaling interventions, ensuring platform compliance, and reaching marginalized or rural communities.

While online safety is clearly a whole-of-society problem requiring collaboration across all levels of government and sectors, the federal government holds primary responsibility for regulating technology as a matter of national concern[58] and is therefore accountable for creating safer digital environments for children. A comprehensive federal legislative and regulatory framework is needed to protect the health and development of Canadian children, youth, and families, and reduce the significant burden that online harms have on a wide range of public sectors including health care, education, and law enforcement.

International Regulatory Models: Structure, Function, Scope, and Financing

With a relatively small market, and all major digital platforms headquartered abroad, Canada faces unique challenges in exerting influence in the digital space. To enable meaningful oversight and extraterritorial compliance, Canada must strategically align its regulatory framework with international best practices.

To support this alignment, a scan of global digital safety regulations was undertaken, identifying 11 jurisdictions, many of which are members of the Global Online Safety Regulators Network (GOSRN).[59] Jurisdictions reviewed in detail include Australia, the European Union (EU), Fiji, France, Germany, Ireland, New Zealand, the Republic of Korea, Slovakia, South Africa, and the United Kingdom (UK).[1]

Table 1 outlines the type of regulator, their core regulatory functions, and presence of a child-specific mandate for each peer jurisdiction. The regulatory functions are grouped based on four functions, as identified and defined by GOSRN[60]:

- **Ex ante regulation** – Responsible for the development and enforcement of preventive and proactive codes, standards, and guidance
- **User complaints and investigations** – Duties include content scanning, receiving and investigating individual user complaints, issuing content removal and blocking notices, partnering with law enforcement and hotline networks, and service blocking or restriction orders
- **Information gathering and enforcement** – Equipped to support systemic oversight and transparency, non-compliance notices and financial penalties, court orders, and injunctions
- **Prevention research and engagement** – Designed to enable public education and awareness, research and grants, horizon scanning, and industry engagement

Table 1. Regulatory authorities of peer jurisdictions

Jurisdiction	Independent Regulator	Regulatory Functions				Regulatory Area	
	Independent Regulator	Ex ante regulation	User complaints & investigations	Information gathering & enforcement	Prevention research & engagement	Child -specific protections	Scope limited to online safety
Australia	Yes	Yes	Yes	Yes	Yes	Yes	Yes
EU	Yes*	Yes	Yes; no user complaints	Yes	Yes	Yes	No
Fiji	Yes	No	Yes; no service blocking or restriction orders	Yes; no oversight or transparency	Yes; no research and horizon scanning	Yes	Yes
France	Yes	Yes	Yes	Yes	Yes	Yes	No
Germany	No	Yes	Yes	Yes	Yes	Yes	No
Ireland	Yes	Yes	Yes	Yes	Yes	Yes	No
New Zealand	No; voluntary enforcement only	Yes; voluntary	Yes; no enforcement powers	No	Yes	Yes	Yes
Republic of Korea	Yes	Yes	Yes	Yes; no oversight and transparency	Yes	Yes	No
Slovakia	Yes	Yes	Yes	Yes; no court orders and injunctions	Yes	Yes	No
South Africa	Yes	Yes	Yes; no service blocking or restriction orders	Yes	Yes	Yes	No
UK	Yes	Yes	Yes; no user complaints	Yes	Yes	Yes	No

* As noted below, the EU requires that each member state appoint an independent regulator.

[1] The research draws on published legislation, publicly available information from government and regulator websites, and international regulatory indexes. All sources are listed in the Appendix.

Independent Regulators

While organizational models differ internationally, a clear global pattern emerges: most peer jurisdictions have established independent statutory regulators, including the EU, Australia, and the UK.

- The **EU**'s *Digital Services Act* (DSA) came into force in November 2022, requiring each member state to designate an independent national regulator, known as a digital services coordinator (DSC), to supervise and enforce the DSA in their respective countries. Examples of DSCs include Arcom in **France** and Coimisiún na Meán in **Ireland**.

- **Australia** first established an eSafety Commissioner in 2015, with a mandate centred on protecting children and youth from online harms. However, the eSafety Commissioner's regulatory and enforcement powers were expanded significantly in 2021 under the *Online Safety Act* to include a mandate to protect all Australians from serious online abuse.

- The **UK** adopted an alternate approach, electing to expand the mandate of its existing communications regulator, Ofcom, under the *Online Safety Act (2023)*.

Within the EU, the European Commission and Germany are unique cases. As a supranational body, the EU Commission is not an independent regulator in the traditional sense. However, it exercises independence, enforcement powers, and expertise, while coordinating with independently established DSCs in each member state. **Germany** has a designated DSC, but responsibilities are also shared with pre-existing specialized agencies, including the Federal Agency for the Protection of Children and Young People in Media, established under earlier online safety laws.

By contrast, **New Zealand** has not established an independent regulator. Instead, NetSafe, a charitable organization, is the sole agency appointed under the *Harmful Digital Communications Act* to handle user complaints. Without enforcement powers, it relies on voluntary cooperation from digital platforms. Following a two-year review of the effectiveness of NetSafe, New Zealand's Department of Internal Affairs proposed the establishment of an independent statutory regulator. However, as of writing, this proposal has not been enacted.[61] In 2025, calls for meaningful reform grew amid criticism of NetSafe's close ties to digital platforms,[62] highlighting the challenges of ensuring online safety without sufficient authority.

Based on these international examples, five key elements emerge as essential for an effective Canadian online safety regulator:

1. **Independence** from political, governmental, or industry influence to ensure impartial and credible oversight

2. **Sufficient enforcement powers and appropriate resources** to meaningfully hold platforms accountable

3. **Deep expertise** in the digital sector, regulatory environment, and specific risks to children, including awareness of, and interoperability with, relevant international regulatory models and standards

4. **A requirement to uphold the specific best interests of children**, protecting their safety, well-being, and rights

5. **Adaptability** to keep pace with rapid technological change and evolving harms, including a broad scope of regulated entities and platform design features

Special Protections for Children and Youth

All peer jurisdictions recognize children as requiring special protections in their online safety frameworks. The EU's DSA requires that platforms uphold fundamental rights, including the "best interests of the child,"[2] and require a high level of privacy, safety, and security for services accessible by minors. Additional specific provisions include reducing exposure to harmful content and child-specific risk assessments. Similarly, the UK's *Online Safety Act* recognizes the need for a higher level of protection for children compared to adults, including a mandate to prevent children from accessing illegal, harmful, and age-inappropriate content, and a requirement to conduct child-specific risk assessments.

[2] The "best interests of the child" principle requires that all decisions affecting children prioritize their full rights and holistic development, with children's interests taking precedence over commercial or other external considerations.

Scope

In addition to variations in regulatory structure and function, international jurisdictions differ in the types of digital platforms included in their online protection frameworks, as highlighted in **Table 2**.

Table 2. Scope of digital platforms regulated by peer jurisdictions

Jurisdiction	Scope									
	Social media services[3]	Hosting and storage services	Gaming services	App distribution services	Internet service providers	Messaging services and dating apps	End-to-end encrypted services	Search engines	Websites	Gen AI
Australia	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
EU	Yes	Yes	Yes	Yes	Yes	Yes	Yes[4]	Yes	Yes	No
Fiji	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes
France	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	No
Germany	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
Ireland	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
New Zealand	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	No
Republic of Korea	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[5]
Slovakia	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
South Africa	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
UK	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes

[3] Social media services are defined as any online service that enables online social interaction between end-users. This includes services that allow users to interact with each other (user-to-user services) or post and view user-generated content (video-sharing platforms).

[4] End-to-end encrypted services aren't exempt, though the DSA does not mandate decryption or surveillance.

[5] The Korea Communications Standards Commission regulates content on AI platforms like DALL-E where content is publicly accessible. However, services such as ChatGPT are not regulated as they interact privately with individual users.

Most peer regulators have authority over a broad range of digital platforms and services, covering social media, online gaming, dating apps, search engines, and even emerging AI-driven systems. Recognizing that the digital environment continues to evolve rapidly, and that children can be present anywhere online, global precedent underscores the importance of defining the scope of regulated services broadly to ensure that they apply to all online products and services children are likely to access.

Funding

International models also illustrate options for financing an independent regulator. Both the **EU** and **UK** have adopted cost-recovery frameworks that require digital platforms to pay annual supervisory fees and use penalties paid from non-compliance to fund ongoing regulatory and enforcement activities. In the UK, these industry contributions are designed to fully offset the cost of regulation.[63]

Canadian federal and provincial jurisdictions have experience implementing effective cost-recovery regulatory models, including the Canadian Energy Regulator,[64] the Canadian Food Inspection Agency, and B.C.'s *Opioid Damages and Health Care Costs Recovery Act*. In the same way that existing models hold private companies accountable, digital platforms that generate billions in profit from online activity should bear a significant share of the financial responsibility for mitigating associated health harms. Canada's previous Bill C-63, the proposed *Online Harms Act,* also reflected this need through a reference to a cost-recovery model.

International Approaches: Harm Mitigation

Across peer jurisdictions, three distinct approaches to harm mitigation strategies have emerged based on a focus on content, age, or design.

Content-Based Approach

A content-based harm mitigation approach requires online service providers to remove illegal content (such as child sexual abuse material) as well as harmful but legal content, including pornography, any content promoting dangerous behaviour (e.g., self-harm, suicide, disordered eating), bullying, harassment, and misinformation. Viral social media challenges (e.g., risky online challenges such as consuming Tide Pods or "blackout") fall into this category because they encourage children and youth to perform dangerous acts online for attention, likes, or views, often across multiple platforms.[65] The obligations under the content-based approach include measures that limit the algorithmic amplification, recommendation, or repeated exposure to such harmful content. Some jurisdictions classify child-harmful content as a separate category, while others capture it more broadly under "harmful content."

Under a content-based approach, users can report harmful content to regulators, who may issue content-removal notices, or report directly to platform-operated reporting systems.

Platforms may be required to implement additional content-moderation systems, including automated screening and detection tools and human moderators that proactively remove illegal and harmful content. Importantly, content moderation should be carried out in consultation with relevant experts (e.g., mental health professionals) who can help establish standards for what constitutes harmful versus safe content, to ensure moderation is effective and evidence based. At minimum, many jurisdictions require platforms to remove illegal and harmful content reactively in response to user complaints.

Table 3 outlines the content-based harm mitigation obligations for both platforms and regulators across international jurisdictions.

Table 3. Content-based harm mitigation obligations of peer jurisdictions

Jurisdiction	Content Obligation for Regulators	Content Obligations for Regulated Platforms			
	Run user-content reporting scheme[6]	Take steps to protect children from age-inappropriate content	Comply with content-removal notices from regulator	Run user-content reporting scheme	Proactively remove illegal and harmful content
Australia	Yes	Yes	Yes	Yes	Yes; only for illegal content
EU	No	Yes	Yes	Yes	Yes; only for illegal content
Fiji	Yes	Yes	Yes	Yes	No
France	Yes	Yes	Yes	Yes	Yes
Germany	Yes	Yes	Yes	Yes	Yes
Ireland	Yes	Yes	Yes	Yes	Yes
New Zealand	Yes	No	No	No	No
Republic of Korea	Yes	Yes	Yes	Yes	Yes
Slovakia	Yes	Yes	Yes	Yes	No
South Africa	Yes	Yes	No	Yes	Yes
UK	No	Yes	No	Yes	Yes

[6] A run user-content reporting scheme is a structured mechanism implemented by online platforms that allows users to flag or report content that violates community standards, terms of service, or legal guidelines.

> **Canada's digital environment is evolving faster than the safeguards designed to protect children and youth.**

In **Australia**, **New Zealand**, **Republic of Korea, South Africa**, and **Fiji,** regulators primarily rely on user-complaint mechanisms and the issuing of content-removal notices. In New Zealand, platform cooperation is voluntary, and unresolved cases can be escalated by users to the courts, which have binding takedown powers. In contrast, the EU and UK impose mandatory obligations on platforms to receive and respond to user reports. In the EU, platforms must notify law enforcement and judicial authorities if they become aware of a criminal offense involving the life or safety of a person. **Germany**, **Slovakia**, and **Ireland** also allow users to report platform violations of the DSA to national regulators, including issues with a platform's handling of user complaints.

Beyond reactive measures, both the **EU** and **UK** require platforms to remove certain content proactively including hate speech and child sexual abuse material. Both jurisdictions enforce robust obligations (under due diligence in the EU and duty of care in the UK) requiring platforms to mitigate risks associated with illegal and harmful content. Measures include user-reporting systems, automated detection tools, and human review. In the EU, member states designate expert third-party entities as "trusted flaggers," empowered to detect illegal content and notify online platforms of the need for prioritized content removal. In the UK, Ofcom explicitly requires child-accessible services to prevent children from accessing harmful content, categorized as "primary priority content," "priority content," and "non-designated content."[7]

Notably, all peer jurisdictions have adopted a form of content-based harm mitigation, with regulators either handling user complaints directly or requiring platforms to do so. Most can escalate unresolved complaints, issue binding takedown orders, and impose penalties for non-compliance.

Canada, by contrast, has no dedicated mechanism beyond law enforcement. Users may report illegal content only to local police or through Cybertip.ca,[66] which refers cases back to law enforcement. This reliance on law enforcement both delays intervention for affected children and creates a barrier to reporting, as those most at risk may be least likely to feel safe involving police. It also fails to address a wider range of harmful but legal content. To align with international best practice, Canada's online safety framework must include a content-based approach covering both illegal and legal content that may be harmful to children. However, such reactive measures are insufficient. To provide meaningful protection, Canada's framework must also adopt proactive design-based approaches to prevent children's exposure to illegal and harmful content online.

Age-Based Approach

An age-based harm mitigation approach involves implementing protective measures tailored to the specific needs of children and youth. This may include tailored platform design features by age range, default settings, or either de facto or explicit age requirements to access specific digital platforms or services (e.g., disabling voice/text chat and real-money purchases for younger users until parental consent is provided).[67]

In the context of online safety measures, the digital age of consent is the minimum age at which an individual can legally provide their own permission for the collection and processing of their personal information by online companies. This age varies across international jurisdictions. Operationalized through mechanisms including cookie consent banners, "click-wrap" agreements, and in-app permission requests, its effectiveness in protecting young people is limited. More fundamentally, consent frameworks assume levels of comprehension, voluntariness, and foresight that many children, specifically younger children, do not possess given their evolving cognitive development and critical thinking skills.[68] Complex privacy policies, "consent fatigue,"[69] and a lack of genuine user control compromise these age-based interventions.

[7] The UK's Online Safety Act and Ofcom define "primary priority content" as content such as pornography, suicide, self-harm, and eating-disorder material; "priority content" as harmful content including abusive, bullying, violent, and dangerous challenge material; and "non-designated content" as other content that presents a material risk of significant harm to children.

Table 4 highlights the age-based approaches being adopted in each jurisdiction studied.

Table 4. Age-based requirements of peer jurisdictions

Jurisdiction	Age of Consent		Age-Appropriate Design		Age Assurance Requirement
	Child consent	Parental consent if child under-age	Protect children from harmful content online	Age-appropriate design experience	
Australia	16	No	Yes	Yes	In development
EU	13–16	Yes	Yes	Yes	In development
Fiji	N/A	N/A	Yes	No	No requirement
France	15	Yes, jointly with child	Yes	Yes	In development
Germany	16	Yes	Yes	Yes	In development
Ireland	16	Yes	Yes	Yes	Age assurance or floor protection[8] for all users
New Zealand	N/A	N/A	Yes	No	No requirement
Republic of Korea	14	Yes	Yes	No	Includes government identification (ID), verifiable e-signature, personal ID, established accounts
Slovakia	16	Yes	Yes	Yes	In development
South Africa	18	Yes	Yes	No	In development
UK	13	Yes	Yes	Yes	Includes photo ID, credit card checks, email-based and facial-based age estimation

[8] Floor protection refers to applying baseline safety measures to all users when a service cannot reliably verify age, ensuring that children are still protected from harmful content.

Most jurisdictions have established a minimum age for accessing digital services, typically ranging from 13 to 16. In 2025, **Australia** raised the minimum age for social media accounts to 16; **New Zealand**[70] has proposed similar age restrictions. Within the **EU**, several member states (including Spain, France, and Greece) are exploring a harmonized higher minimum age for social media services.[71]

Some jurisdictions require platforms to implement an "age-appropriate design experience," including restricted access to specific features. For example, **France** prohibits users under 18 from accessing monetizable features in online games, while the **Republic of Korea** requires users to be at least 16 to create an online gaming account.

Existing self-declaration methods used by platforms to verify user age are proven to be inadequate, as shown by the widespread presence of users under the current minimum age on social media.[72] Instead, age-based protection systems require the development, implementation, and regulation of effective age-assurance systems. Efforts to support more robust age-assurance include the EU's "white-label age verification app" that reads official IDs and confirms age for websites and apps without gathering any other personal details. Member states, including Denmark, France, Greece, Italy, and Spain, were set to pilot the solution in July 2025.[73] Australia launched its Age Assurance Technology Trial in November 2024, with preliminary findings confirming technical feasibility of age assurance and further guidance is expected.[74] The **UK** has also recently released guidelines outlining acceptable verification methods.[75]

In **Canada**, the digital age of consent is 13.[76] In May 2025, Quebec recommended raising it to 14.[77,78] The Office of the Privacy Commissioner of Canada signalled growing national attention to age-assurance requirements by conducting an exploratory consultation on age-assurance technologies.[79]

While age-based approaches and age-assurance mechanisms can support the enforcement of the digital age of consent and facilitate precise child-specific protections, raising the minimum age to effectively ban children from digital spaces is a potentially counterproductive strategy. It risks excluding youth from beneficial online spaces, such as for education, entertainment, and positive social interaction, removes the responsibility of platforms to create safer digital environments, and may risk driving young people toward unregulated and less safe online spaces. Moreover, age-assurance mechanisms may have inherent limitations and, if poorly designed, may undermine children's right to privacy, participation, and access to information, or become a superficial "box-checking" exercise focused on age-gating rather than safety.[80] Real safety improvements require design changes, including platform accountability for safety-by-design measures, with age-assurance mechanisms that meet privacy protective standards serving as one tool for harm reduction in the online world.

Design-Based Approach

A design-based approach to online harm mitigation requires digital platforms to embed child-protective measures directly into the architecture of their platforms and processes. This approach aims to ensure that children and youth are proactively shielded from online harms, while still being able to benefit from the opportunities of the digital environment. The principle of "safety-by-design," long established in the regulation of physical products used by children, including car seats and toys, is increasingly recognized as a necessary standard for digital platforms.[81] Applying this established regulatory expectation to the online environment is essential to ensuring equivalent protections for children across physical and digital contexts.

Peer jurisdictions adopt this approach through statutory duty of care (UK), due diligence obligations (EU), enforceable codes (EU, UK, Ireland, Australia), and voluntary guidelines (South Africa, New Zealand). The EU's and UK's legislated due diligence obligations and duties of care respectively require platforms to conduct risk assessments, implement mitigation measures, and report to regulators. Platform non-compliance can result in significant penalties including 5 per cent of global annual turnover (EU) or 10 per cent of qualifying worldwide revenue (UK). Similarly, Australia's *Online Safety Act* mandates risk assessments and "reasonable safety steps," though penalties only apply for non-reporting.

Table 5 outlines key safety-by-design protections for children in legislation, regulation, codes, and guidelines across five jurisdictions; the other jurisdictions do not contain explicit safety-by-design provisions.

Table 5. Safety-by-design provisions of peer jurisdictions

Safety-by-Design Provision	Jurisdiction				
	EU	UK	Australia	South Africa	New Zealand
Risk Assessments					
Assess and mitigate systemic risks posed to children	✓	✓	✓		
Assess a child's likelihood of accessing the service	✓	✓	✓		
Follow regulators for guidance on risk-assessment standards	✓	✓	✓		
Assess risks against regulators released risk profiles	✓	✓	✓		
Internal Policies					
Involve children in the design of the platform	✓				
Assign dedicated staff (audit committee, accountable persons) for mitigation of risks to children	✓	✓	✓	✓	
Train staff in compliance duties to protect children	✓	✓			
Collaborate with external stakeholders	✓	✓	✓		✓
Transparency and Accountability					
Outline child risks, protection measures, and tools in terms of service	✓	✓	✓	✓	
Uphold set community guidelines and policies	✓	✓	✓		
Present information in an engaging, child-friendly format	✓	✓	✓	✓	✓
Alert children when features or behaviours pose a risk (e.g., changing default settings, geolocation, processing of personal data)	✓	✓	✓		

	EU	UK	Australia	South Africa	New Zealand
Privacy					
Set children's accounts to private by default and restrict interaction outside of connected accounts	✓	✓	✓	✓	
Conduct data protection assessments	✓	✓			
Minimize data collection to essential activities a child is engaged in	✓	✓			
Do not disclose children's data to third parties		✓			
Implement effective age-assurance	✓	✓	✓	✓	
Functionalities					
Acknowledge children's evolving capacities through age-appropriate design	✓	✓		✓	
Modify recommender systems9 to reduce exposure to harmful content and loops	✓	✓	✓		
Encourage user's agency over content and interactions (e.g., category selection, recommendation feed resets, negative feedback)	✓	✓	✓	✓	✓
Avoid features that extend engagement (e.g., reward loops, continuous scrolling, push notifications, auto-play features, streaks, ephemeral content, read receipts)	✓	✓			
Avoid profiling advertising	✓	✓			
Avoid geolocation tracking	✓	✓			
Limit commercial practices that lead to unwanted spending or addictive behaviours (e.g., virtual currencies, loot boxes, aggressive advertising)	✓	✓			

[9] Recommender systems, also known as content curation systems, are systems that prioritize content or make personalized content suggestions to users of online services. In the context of safety-by-design, modifying recommender systems may involve embedding safety measures directly into the algorithm architecture to proactively mitigate risks. (eSafety Commissioner)

	EU	UK	Australia	South Africa	New Zealand
User Empowerment					
Empower children to easily block and mute users	✓	✓	✓		
Enable users to issue complaints easily, respond swiftly, and communicate process and timeframe clearly	✓	✓	✓	✓	
Offer parental control tools	✓	✓	✓	✓	
Use of AI					
Put safeguards around AI chatbots (e.g., assess risks, restrict access, warning labels)	✓	✓			
Limit use of support tools based on AI interacting with children	✓				
Limit children's exposure to AI that influences children for commercial purposes	✓				

As seen above, leading jurisdictions like the **EU** and **UK** have outlined safety-by-design measures for children that span all aspects of platform design. Similar measures appear in voluntary guidelines such as in **New Zealand** and **South Africa**, reflecting a global shift towards safety-by-design. Notably, **Australia**'s guidelines closely mirror those of the EU and UK but lack enforceability as obligations are primarily set out in non-binding guidance. In 2025, Australia's statutory review of its *Online Safety Act* recommended introducing a legislated duty of care to strengthen enforcement, which, at time of writing, the government had committed to advancing.[82]

In line with international best practice, **Canada** should prioritize a design-based approach to online safety legislation that requires platforms to build digital environments centred on the safety, well-being, and best interests of children and youth. These requirements must be enforceable, such as through a statutory duty of care.

Additionally, the regulator should be mandated to develop a comprehensive children's code, outlining specific safety-by-design provisions for services accessible by children and grounded in a binding legal framework.

Conclusion

Screens have become ubiquitous in the lives of children and youth, and in most places they live, learn, and play. The impact of the unregulated digital environment on child development is undoubtedly one of the most significant and unpredictable issues facing child health today. While Canadian children face profound mental and physical health harms from online spaces that are designed and operated counter to children's best interests, industry giants continue to operate in Canada without meaningful accountability and exert widespread influence over young Canadians without adequate safeguards. The global momentum towards online safety legislation, coupled with robust science and overwhelming public support, underscores a growing international consensus on the need for federal oversight. To protect children and youth, and the well-being of future generations, it is critical that federal policymakers in Canada catch up to international best practice and implement robust, child-centred online safety regulations. **As such, Canada's priority should be to establish an independent online safety regulator. This authority should enforce a statutory duty of care on online platforms and services, with an emphasis on obliging them to implement proactive, safety-by-design measures. To guide its work and to ensure children's rights and well-being, Canada should also develop and apply a comprehensive children's code.**

References

1. Cornelius S, Leidner D. Acceptance of Anthropomorphic Technology: A Literature Review. Proceedings of the 54th Hawaii International Conference on System Sciences; 2021. doi: 10.24251/HICSS.2021.774

2. Jang Y, Ko B. Online Safety for Children and Youth under the 4Cs Framework—A Focus on Digital Policies in Australia, Canada, and the UK. Children. 2023;10(8):1415. doi: 10.3390/children10081415

3. Chiu M, Gatov E, Fung K, Kurdyak P, Guttmann A. Deconstructing The Rise In Mental Health–Related ED Visits Among Children And Youth In Ontario, Canada. Health Aff. 2020;39(10):1728-1736. doi: 10.1377/hlthaff.2020.00232

4. UNICEF Canada. Worlds Apart Canadian Companion to UNICEF Report Card 16 [Internet]. Toronto: UNICEF Canada; 2020 [cited 2026 Feb 12]. Available from: www.unicef.ca/irc16

5. Lockhart A, Laghaei M, Andrey S. Survey of Online Harms in Canada 2024 [Internet]. Toronto: The Dais; 2024. [cited 2025 Nov 25]. Available from: https://dais.ca/wp-content/uploads/2024/08/Survey-of-Online-Harms-in-Canada-2024.pdf

6. Memon AM, Sharma SG, Mohite SS, Jain S. The role of online social networking on deliberate self-harm and suicidality in adolescents: A systematized review of literature. Indian J Psychiatry. 2018;60(4):384-392. doi: 10.4103/psychiatry.IndianJPsychiatry_414_17

7. Madriaza P, Hassan G, Brouillette-Alarie S, et al. Exposure to hate in online and traditional media: A systematic review and meta-analysis of the impact of this exposure on individuals and communities. Campbell Syst Rev. 2025 Jan 16;21(1):e70018. doi: 10.1002/cl2.70018

8. Abi-Jaoude E, Naylor KT, Pignatiello A. Smartphones, social media use and youth mental health. CMAJ. 2020 Feb 10;192(6):E136-E141. doi: 10.1503/cmaj.190434

9. Davis CG, Goldfield GS. Limiting Social Media Use Decreases Depression, Anxiety, and Fear of Missing Out in Youth With Emotional Distress: A Randomized Controlled Trial. Psychology of Popular Media. 2024;14(1):1-11. doi: 10.1037/ppm0000536

10. Jusienė R, Pakalniškienė V, Wu JCL, Sebre SB. Compulsive Internet Use Scale for assessment of self-reported problematic internet use in primary school-aged children. Front Psychiatry. 2023 Jun 30;14 :1173585. doi: 10.3389/fpsyt.2023.1173585

11. Canadian Internet Use Survey (CIUS) – Detailed information for 2022 [Internet]. Ottawa: Statistics Canada; 2023 Nov 2. [cited 2026 Feb 12]. Available from: https://www23.statcan.gc.ca/imdb/p2SV.pl?Function=getSurvey&SDDS=4432

12. Colley RC, Saunders TJ. The ongoing impact of the COVID-19 pandemic on physical activity and screen time among Canadian youth. Health Rep. 2023;34(10):3-12. doi: 10.25318/82-003-x202301000001-eng

13. Donelle L, Facca D, Burke S, Hiebert B, Bender E, Ling S. Exploring Canadian Children's Social Media Use, Digital Literacy, and Quality of Life: Pilot Cross-sectional Survey Study. JMIR Form Res. 2021;5(5):e18771. doi: 10.2196/18771

14. Statistics Canada [Internet]. Young people and exposure to harmful online content in 2022. Ottawa: Government of Canada; 2024 Feb 27. [cited 2026 Feb 12]. Available from: https://www150.statcan.gc.ca/n1/pub/11-627-m/11-627-m2024005-eng.htm

15. Kardefelt Winther D, Stoilova M, Büchi M, et al. Children's exposure to hate messages and violent images online. Florence: UNICEF Innocenti – Global Office of Research and Foresight; 2023 Jul. Available from: https://www.unicef.org/innocenti/media/2621/file/UNICEF-Children-Exposure-Hate-Violence-Online.pdf

16. Statistics Canada [Internet]. The Daily — Online hate and aggression among young people in Canada. Ottawa: Government of Canada; 2024 Feb 27. [cited 2026 Feb 12]. Available from: https://www150.statcan.gc.ca/n1/daily-quotidien/240227/dq240227b-eng.htm

17. Finkelhor D, Turner H, Colburn D. Which dynamics make online child sexual abuse and cyberstalking more emotionally impactful: Perpetrator identity and images? Child Abuse Negl. 2023;137:1-10. doi: 10.1016/j.chiabu.2023.106020

18. Riehm KE, Feder KA, Tormohlen KN, et al. Associations Between Time Spent Using Social Media and Internalizing and Externalizing Problems Among US Youth. JAMA Psychiatry. 2019;76(12):1266-1273. doi: 10.1001/JAMAPSYCHIATRY.2019.2325

19. Ioannidis K, Taylor C, Holt L, et al. Problematic usage of the internet and eating disorder and related psychopathology: A multifaceted, systematic review and meta-analysis. Neurosci Biobehav Rev. 2021;125:569-581. doi: 10.1016/J.NEUBIOREV.2021.03.005

20. Gardner W, Pajer K, Cloutier P, et al. Changing Rates of Self-Harm and Mental Disorders by Sex in Youths Presenting to Ontario Emergency Departments: Repeated Cross-Sectional Study. Can J Psychiatry. 2019;64(11):789-797. doi: 10.1177/0706743719854070

21. Van Bavel JJ, Robertson CE, del Rosario K, Rasmussen J, Rathje S. Social Media and Morality. Annu Rev Psychol. 2024;75:311-340. doi: 10.1146/ANNUREV-PSYCH-022123-110258

22. Williams D, Mcintosh A, Farthing R. Profiling Children for Advertising: Facebook's Monetisation of Young People's Personal Data [Internet]. Reset Australia; 2021 Apr. [cited 2026 Feb 12]. Available from: https://au.reset.tech/uploads/resettechaustralia_profiling-children-for-advertising-1.pdf

23. Derevensky JL, Hayman V, Lynette Gilbeau. Behavioral Addictions: Excessive Gambling, Gaming, Internet, and Smartphone Use Among Children and Adolescents. Pediatr Clin North Am. 2019;66(6):1163-1182. doi: 10.1016/j.pcl.2019.08.008

24. Raghuvanshi A. Hooked by Design: How Social Media Makes and Breaks Us [Internet]. CMC Senior Theses; 2025. [cited 2026 Feb 12]. Available from: https://scholarship.claremont.edu/cmc_theses/3953

25. Raffoul A, Ward ZJ, Santoso M, Kavanaugh JR, Austin SB. Social media platforms generate billions of dollars in revenue from U.S. youth: Findings from a simulated revenue model. PLoS One. 2023;18(12):e0295337. doi: 10.1371/JOURNAL.PONE.0295337

26. 5Rights Foundation. Disrupted Childhood: The cost of persuasive design. London (UK): The Foundation; 2023 Apr. Available from: https://5rightsfoundation.com/wp-content/uploads/2024/08/5rights_DisruptedChildhood_G.pdf

27. Bradshaw S, Vaillancourt T. Freedom of Thought, Social Media and the Teen Brain. Waterloo: Centre for International Governance Innovation; 2024 Feb 12. [cited on 2026 Feb 13]. Available from: https://www.cigionline.org/publications/freedom-of-thought-social-media-and-the-teen-brain/

28. Common Sense Media [Internet]. Most Apps and Online Platforms Used by Kids Are Likely Sharing and Selling Their Data, According to a New Report from Common Sense Media. San Francisco: Common Sense Media; 2023 Jun 28. [cited on 2026 Feb 12]. Available from: https://www.commonsensemedia.org/press-releases/most-apps-used-by-kids-are-likely-sharing-and-selling-their-data

29. eSafety Commissioner [Internet]. [cited 2026 Feb 13]. Available from: https://www.esafety.gov.au

30. Coimisiún na Meán [Internet]. Dublin; c2026 [cited 2026 Feb 13]. Available from: https://www.cnam.ie

31. Arcom [Internet]. [cited 2026 Feb 13]. Available from: https://www.arcom.fr

32. Ofcom [Internet]. [cited 2026 Feb 13]. Available from: https://www.ofcom.org.uk

33. Broadcasting Media and Communications Deliberation Committee [Internet}. Soeul; c2024 [cited 2026 Feb 13]. Available from: https://www. /mainPage.do

34. Canadian Centre for Child Protection [Internet]. Canada needs online safety laws. Winnipeg: C3P; c2026 [cited 2026 Feb 12]. Available from: https://protegeonsnosenfants.ca/en/resources-research/safe-spaces-online/?utm_campaign=sl&utm_term=/en/resources-research/online-harms-bill

35. Lockhart A. Survey of Online Harms in Canada 2025. Toronto: The Dais; 2025. Available from: https://dais.ca/wp-content/uploads/2024/08/Survey-of-Online-Harms-in-Canada-2024.pdf

36. Zapata K. Calgary advocate leads national push for revival of Online Harms Act to protect kids. CBC News [Internet]. 2025 Nov 20 [cited 2026 Feb 12]. Available from: https://www.cbc.ca/news/canada/calgary/online-harms-act-revival-9.6985654

37. Innovation, Science and Economic Development Canada [Internet]. Government of Canada orders the wind up of TikTok Technology Canada, Inc. following a national security review under the Investment Canada Act. Ottawa: Government of Canada; 2024 Nov 6 [cited on 2026 Feb 12]. Available from: https://www.canada.ca/en/innovation-science-economic-development/news/2024/11/government-of-canada-orders-the-wind-up-of-tiktok-technology-canada-inc-following-a-national-security-review-under-the-investment-canada-act.html

38. Canada Revenue Agency [Internet]. Digital services tax. Ottawa: Government of Canada; 2025 Sep 15 [cited 2026 Feb 12]. Available from: https://www.canada.ca/en/services/taxes/excise-taxes-duties-and-levies/digital-services-tax.html

39. Department of Justice Canada [Internet]. Bill C-63: An Act to enact the Online Harms Act, to amend the Criminal Code, the Canadian Human Rights Act and An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service and to make consequential an and related amendments to other Acts. Ottawa: Government of Canada; 2024 Jun 4 [cited 2026 Feb 12]. Available from: https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c63.html

40. Zimonjic P. Liberals split online harms bill to postpone debate over policing hate speech. CBC News [Internet]. 2024 Dec 4 [cited 2026 Feb 12]. Available from: https://www.cbc.ca/news/politics/liberal-government-split-online-harms-bill-1.7400882

41. Bill C-412: An Act to enact the Protection of Minors in the Digital Age Act and to amend the Criminal Code, 44th Parl., 1st Sess. (2024) [cited 2026 Feb 12]. Available from: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-412/first-reading

42. Department of Justice Canada [Internet]. Bill C-27: An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts. Ottawa: Government of Canada; 2023 Nov 27 [cited 2026 Feb]. Available from: https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c27_1.html

43. Bill 12 – 2024: Public Health Accountability and Cost Recovery Act, 42nd Parl., 5th Sess. [cited 2026 Feb 12]. Available from: https://www.bclaws.gov.bc.ca/civix/document/id/bills/billsprevious/5th42nd:gov12-1

44. Office of the Premier. Joint statement on Bill 12: B.C. to convene online safety action table. BC Gov News [Internet]. 2024 Apr 23 [cited 2026 Feb 12]. Available from: https://news.gov.bc.ca/releases/2024PREM0029-000617

45. Office of Attorney General, Ministry of Public Safety and Solicitor General. Online Safety Action Table – Progress Report. Victoria: B.C. Government; 2024 Sep. Available from: https://www2.gov.bc.ca/assets/gov/law-crime-and-justice/about-bc-justice-system/legislation-policy/osat/online_safety_action_table__progress_report.pdf

46. Lim R. Ontario school boards clear hurdle in lawsuits against Meta, Snapchat, TikTok. CBC News [Internet]. 2025 Mar 11 [cited 2026 Feb 12]. Available from: https://www.cbc.ca/news/canada/toronto/ontario-school-boards-social-media-lawsuit-1.7480402

47. Schools For Social Media Change [Internet]. About Us. c2024–2026 [cited 2026 Feb 12]. Available from: https://schoolsforsocialmediachange.ca/about-us/

48. Centre for Healthy Screen Use [Internet]. Provincial and Territorial Policies. Ottawa: Canadian Paediatric Society; c2026 [cited 2026 Feb 12]. Available from: https://healthyscreenuse.cps.ca/policy-and-advocacy/provincial-territorial-policies

49. Subdhan A, Shah M. The cellphone rules for the 2024-2025 school year in every Canadian province and territory. The Globe and Mail [Internet]. 2024 Aug 29 [cited 2026 Feb 12]. Available from: https://www.theglobeandmail.com/canada/article-cellphone-bans-are-coming-to-a-canadian-classroom-near-you-here-are/

50. Baig F. A for effort: First year of cellphone bans in Canadian schools gets mostly positive marks. CBC News [Internet]. 2025 Jun 9 [cited 2026 Feb 12]. Available from: https://www.cbc.ca/news/canada/edmonton/general-acceptance-one-year-cell-phone-ban-canadian-schools-1.7556549

51. Goodyear VA, Randhawa A, Adab P, et al. School phone policies and their association with mental wellbeing, phone use, and social media use (SMART Schools): a cross-sectional observational study. Lancet Reg Health Eur. 2025;51:101211. doi: 10.1016/j.lanepe.2025.101211

52. Lockhart A, Singh R, Côté A. Phone Restrictions in K-12 Schools: National Survey on Canadian Sentiment. Toronto: The Dais; 2025 [cited 2026 Feb 12]. Available from: https://dais.ca/wp-content/uploads/2025/05/Phone-Restrictions-in-K-12-Schools-Survey-Brief.pdf

53. Youth Victims and Accused of Cybercrime – Uniform Crime Reporting Survey 2022. Ottawa: Government of Canada; 2024 Dec 24 [cited 2026 Feb 12]. Available from: https://open.canada.ca/data/en/dataset/802c713f-5b98-4b66-8787-4cf4ced5962f/resource/1299c9b1-98e4-49c5-853f-a48647470443

54. Public Safety Canada [Internet]. About Online Child Sexual Exploitation. Ottawa: Government of Canada; 2026 Jan 14 [cited 2026 Feb 12]. Available from: https://www.publicsafety.gc.ca/cnt/cntrng-crm/chld-sxl-xplttn-ntrnt/abt-nln-chld-sxl-xplttn-en.aspx

55. Public Safety Canada [Internet]. Government of Canada invests in protecting children and youth from online sexual exploitation. Ottawa: Government of Canada; 2025 Mar 20 [cited 2026 Feb 12]. Available from: https://www.canada.ca/en/public-safety-canada/news/2025/03/government-of-canada-invests-in-protecting-children-and-youth-from-online-sexual-exploitation.html

56. Young Politicians of Canada [Internet]. The Internet Delegation's Input. Toronto: Young Politicians of Canada; c2026 [cited 2026 Feb 12]. Available from: https://www.youngpoliticians.org/get-involved/leadership-groups/online-harms/input

57. The Dais [Internet]. Heads Up. Toronto: The Dais; c2026 [cited 2026 Feb 12]. Available from: https://dais.ca/headsup

58. References re Greenhouse Gas Pollution Pricing Act, 2021 SCC 11, [2021] 1 S.C.R. 175 CanLII. [cited 2026 Feb 12]. Available from: https://www.canlii.org/en/ca/scc/doc/2021/2021scc11/2021scc11.html

59. eSafety Commissioner [Internet]. The Global Online Safety Regulators Network. Australian Government; c2025 [cited 2026 Feb 12]. Available from: https://www.esafety.gov.au/about-us/consultation-cooperation/international-engagement/the-global-online-safety-regulators-network

60. Global Online Safety Regulators Network [Internet]. Regulatory Index: Comparing international approaches and perspectives to online safety regulations. 2024 Oct 24 [cited 2026 Feb 12]. Available from: https://www.ofcom.org.uk/siteassets/resources/documents/about-ofcom/international/other/global-online-safety-regulators-network-regulatory-index.pdf?v=383839

61. Bickerton S, Mudgway C. NZ has no clear direction on online safety regulation. Newsroom. [Internet]. 2025 Mar 6 [cited 2026 Feb 12]. Available from: https://newsroom.co.nz/2025/03/06/nz-has-no-clear-direction-on-online-safety-regulation

62. Espiner G. Netsafe's tech ties spark calls for independent regulator. RNZ News [Internet]. 2025 Feb 20 [cited 2026 Feb 12]. Available from: https://www.rnz.co.nz/news/in-depth/542415/netsafe-s-tech-ties-spark-calls-for-independent-regulator

63. Department for Science, Innovation, and Technology. Guidance to the regulator about fees relating to the Online Safety Act 2023. GOV.UK; 2024 May 24 [cited 2026 Feb 12]. Available from: https://www.gov.uk/government/publications/online-safety-act-2023-guidance-to-the-regulator-about-fees/guidance-to-the-regulator-about-fees-relating-to-the-online-safety-act-2023

64. Canada Energy Regulator [Internet]. Cost Recovery. Ottawa: Government of Canada; 2024 Dec 10 [cited 2026 Feb 12]. Available from: https://www.cer-rec.gc.ca/en/about/who-we-are-what-we-do/cost-recovery/index.html

65. Smart Social [Internet]. 25+ Dangerous Social Media Challenges Parents and Teachers Need to Know. Smart Social; c2026 [cited 2026 Feb 12]. Available from: https://www.smartsocial.com/dangerous-challenges

66. Cybertip.ca [Internet]. Canadian Centre for Child Protection; c2026 [cited 2026 Feb 12]. Available from: https://cybertip.ca/en

67. Epic Games [Internet]. Parental Controls. c2026 [cited 2026 Feb 12]. Available from: https://safety.epicgames.com/en-US/parental-controls

68. Canadian Paediatric Society. Written Submission to the Office of the Privacy Commissioner of Canada: Exploratory Consultation on the Development of a Children's Privacy Code. Ottawa: CPS; 2025 Aug. Available from: https://cps.ca/uploads/advocacy/CPS_Submission.OPC_.pdf

69. Centre for Information Policy Leadership and Bae, Kim & Lee. The Limitations of Consent as a Legal Basis for Data Processing in the Digital Society. 2024. Available from: https://www.informationpolicycentre.com/wp-content/uploads/2024/12/cipl_bkl_limitations_of_consent_legal_basis_data_processing_dec24-4.pdf

70. Sharma S. New Zealand's prime minister proposes social media ban for children under 16. The Independent [Internet]. 2025 May 6 [cited 2026 Feb 12]. Available from: https://www.independent.co.uk/news/world/australasia/new-zealand-social-media-ban-children-b2745512.html

71. Villamor J. Six EU Countries Plan to Ban Social Media for Minors. The European Conservative [Internet]. 2025 Jun 3 [cited 2026 Feb 12]. Available from: https://europeanconservative.com/articles/news/eu-countries-plan-ban-social-media-for-minors-restriction-control-protection

72. eSafety Commissioner [Internet]. eSafety report shows widespread underage use of social media and minimal measures to prevent kids signing up. Australian Government; 2025 Feb 20 [cited 2026 Feb 13]. Available from: https://www.esafety.gov.au/newsroom/media-releases/esafety-report-shows-widespread-underage-use-of-social-media-and-minimal-measures-to-prevent-kids-signing-up

73. European Union Commission [Internet]. Commission makes available an age-verification blueprint. EU Commission; 2025 Jul 14 [cited 2026 Feb 12]. Available from: https://digital-strategy.ec.europa.eu/en/news/commission-makes-available-age-verification-blueprint

74. Age Assurance Technology Trial [Internet]. News Release: Age Assurance Technology Trial Publishes Twelve Preliminary Findings Ahead of Full Report. Canberra: The Trial; 2025 June 20 [cited 2026 Feb 12]. Available from: https://ageassurance.com.au/wp-content/uploads/2025/06/News-Release-Preliminary-Findings-for-publication-20250620.pdf

75. Ofcom [Internet]. Statement: Age Assurance and Children's Access. Ofcom; 2025 Jan 16 [cited 2026 Feb 12]. Available from: https://www.ofcom.org.uk/online-safety/protecting-children/statement-age-assurance-and-childrens-access

76. Office of the Privacy Commissioner of Canada [Internet]. Protecting the privacy rights of young people. OPC; 2023 Nov 28 [cited 2026 Feb 12]. Available from: https://www.priv.gc.ca/en/for-federal-institutions/privacy-act-bulletins/pab_20231128

77. Assemblée nationale du Québec [Internet]. Commission spéciale sur les impacts des écrans et des réseaux sociaux sur la santé et le développement des jeunes. Québec: Assemblée nationale. [cited 2026 Feb 12]. Available from: https://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/csesj-43-1/index.html

78. Fournier C. Young people, health and screens: Supporting action in Indigenous contexts. Québec: Institut national de santé publique du Québec; 2024. Available from: https://www.inspq.qc.ca/sites/default/files/2024-06/3485-young-people-health-screens-supporting-action-Indigenous-contexts.pdf

79. Office of the Privacy Commissioner of Canada [Internet]. Consultation on age assurance – What We Heard. OPC; 2025 Mar 21 [cited 2026 Feb 12]. Available from: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-age/report_age_2025

80. 5Rights Foundation [Internet]. What happens once you know it's a child? Rethinking age assurance for a rights-respecting digital world. The Foundation; 2025 Apr 16 [cited 2026 Feb 12]. Available from: https://5rightsfoundation.com/what-happens-once-you-know-its-a-child-rethinking-age-assurance-for-a-rights-respecting-digital-world

81. OECD. Towards digital safety by design for children. OECD Digital Economy Papers. 2024;363. doi:10.1787/c167b650-en

82. The Hon Michelle Rowland MP [Internet]. New Duty of Care obligations on platforms will keep Australians safer online Department of Infrastructure, Transport, Regional Development, Communications; 2024 Nov 14 [cited 2026 Feb 12]. Available from: https://minister.infrastructure.gov.au/rowland/media-release/new-duty-care-obligations-platforms-will-keep-australians-safer-online

Appendix

Jurisdiction	Digital Safety Legislation
Australia (eSafety Commissioner)	Basic Online Safety Expectations (2022) Online Safety Act (2021) Industry Codes and Standards
European Union (European Commission)	Guidelines on the Protection of Minors (2025) Digital Services Act (2022) Regulation to address the dissemination of terrorist content online (2021) Audio-Visual Media Services Directive (2018) General Data Protection Regulation (2016)
Fiji (Online Safety Commission)	Online Safety Regulations (2019) Online Safety Act (2018)
France (Arcom)	Securing and Regulating the Digital Space (2024)
Germany (Bundesnetzagentur)	Digital Services Act (2024) Second Act Amending the Youth Protection Act (2021) Telecommunication Digital Services Data Protection Act (2021)
Ireland (Coimisiún na Meán)	Online Safety Code (2024) Online Safety and Media Regulation Act (2022) The Fundamentals for a Child-Oriented Approach to Data Processing (2020)
New Zealand (NetSafe)	Voluntary Code of Practice for Online Safety and Harms (2022) Harmful Digital Communications Act (2015)
Republic of Korea (Korea Communications and Standards Commission)	Act on Promotion of Information and Communications Network Utilization and Information Protection (2024) Telecommunication Business Act (2023)
Slovakia (Council for Media Services)	The Media Services Act (2022)
South Africa (Film and Publications Board)	Industry Code on Prevention of Online Harm (2023) Films and Publications Act (amended in 2022)
United Kingdom (Ofcom)	Protection of Children Code of Practice (2025) Online Safety Act (2023) Age-Appropriate Design Code (2020) UK Data Protection Act (2018) UK General Data Protection Regulation (2016)

Canadian
Paediatric
Society

SickKids® | Child Health
Policy Accelerator