Setting the Standard: A Children's Code for the Safe Social Media Act



SickKids
Child Health Policy Accelerator

Key Recommendation: Canada's proposed Digital Safety and Data Protection Commission should prioritize the development and implementation of a children's digital safety code ("children's code") to help fulfill the Safe Social Media Act's primary objective of reducing the risks digital platforms pose to children.

Background

The online environment poses serious risks to the mental and physical health of children and youth.[1] Across digital services, children encounter diverse and evolving risks, including harmful content, persuasive platform design, unsolicited contact from strangers and commercial practices that prioritize revenue generation over children's best interests.[2,3]

Recognizing these risks, many jurisdictions comparable to Canada have introduced legislation to enhance digital safety. Canada now has a critical opportunity to establish a similarly robust framework through Bill C-34, the Safe Social Media Act. Introduced in Parliament in June 2026, the Bill explicitly identifies the protection of children's physical and mental health as one of its purposes. If enacted, the legislation would establish an independent regulator, the Digital Safety and Data Protection Commission of Canada (the "Commission"), and impose a specific statutory duty on regulated service providers to protect children.[4] The Commission would also be empowered to develop codes and standards to support the implementation and enforcement of the Act.

A strong legislative framework, as proposed in Bill C-34, is an important first step for Canada. However, its effectiveness will depend not only on the obligations established in the legislation but also on how those legislative obligations are translated into specific, meaningful, measurable and enforceable requirements.

The role of a children's code

A children's code is a powerful vehicle for translating broad legislative obligations into specific, enforceable standards to protect children online. By establishing clear expectations for digital services, a children's code can help platforms understand what compliance requires while providing regulators with a practical framework for assessing and enforcing those obligations. In doing so, **a children's code translates legislative intent into consistent, measurable protections for children that must be embedded in the design, operation and governance of digital platforms**.

For ease of reference, this brief uses "children's code" as an umbrella term for child-specific regulatory documents, recognizing that jurisdictions differ in how these protections are labelled, structured, developed and implemented.

Across digital services, children encounter diverse and evolving risks, including harmful content, persuasive platform design, unsolicited contact from strangers and commercial practices that prioritize revenue generation over children's best interests.[2,3]

Children's codes in other jurisdictions

Internationally, other jurisdictions have adopted diverse regulatory approaches to online safety. Where child-focused legislation exists, or where regulators have a clear mandate and sufficient resources, standalone children's codes have been developed.[5,6] In other jurisdictions, child-specific provisions have been incorporated into broader regulatory codes or standards.[7-12]

While both approaches can establish meaningful protections for children, **Bill C-34's explicit focus on child safety warrants the development of a dedicated children's code to provide a clear mechanism for establishing and enforcing comprehensive, child-specific requirements.**

Once developed and given legal effect, child safety codes become an integral part of regulatory enforcement. In Australia, for example, platforms' actions and inaction are expressly assessed against applicable codes and standards[13] and non-compliance has triggered multiple investigations.[14] Similarly, the United Kingdom's digital regulator, Ofcom, has indicated that its new Protection of Children Codes of Practice will inform its review of platforms' annual risk assessments.[15] These examples demonstrate that a children's code can serve as the bridge between legislative intent and practical protection: translating a statutory duty to protect young people from harm into specific child-centred expectations for digital services and establishing a clear basis for regulatory accountability when those expectations are not met.

Table 1: Online Safety Legislative Structure in Other Jurisdictions

Jurisdiction	Legislation	Regulatory Document	Dedicated Children's Code	Legal Status	Developer
Australia	Online Safety Act (2021)	Online Safety Codes and Standards	No	Registered industry codes and standards under legislation	eSafety Commissioner and industry partners
European Union	Digital Services Act (2022)	DSA Guidelines on Protection of Minors	Yes	Regulatory guidance*	European Commission
Ireland	Online Safety and Media Regulation Act (2022)	Online Safety Code	No	Statutory regulatory code	Coimisiún na Meán
United Kingdom	Online Safety Act (2023)	Ofcom Protection of Children Codes of Practice	Yes	Statutory regulatory code	Ofcom

**Regulatory guidance is not enforceable, but carries significant interpretive weight by the European Commission.*

Common elements of children's codes

Across jurisdictions, several common regulatory approaches emerge. Together, they demonstrate how **broad legislative duties can be translated into concrete requirements for the design, operation and oversight of digital services.**

Age Assurance

A child-safe digital environment requires digital services to know when their users are children. Age assurance is therefore a foundational component of child-safety regulation.

To achieve this, digital services are required to implement age-verification or age-estimation tools. Children's codes and regulatory guidance documents identify high-level characteristics constituting effective age assurance, commonly citing accuracy, reliability, robustness, fairness and non-intrusiveness as important criteria.[5-7,11] Regulatory frameworks also establish expectations regarding when age assurance should be applied, which technologies or practices are considered acceptable and what assessments are required to ensure that an age assurance tool is proportionate to the level of risk. For example, there is broad recognition across existing codes that self-declaration alone is insufficient to meet age-assurance objectives.[6-9]

Measures to Mitigate Harmful Content

Children's codes and related regulatory standards add specificity to the broad definitions of illegal and harmful content contained in their respective legislative frameworks and clarify the circumstances in which digital services must take action. Codes provide guidance on how platforms should develop content-classification processes so that different content-removal obligations can be applied effectively and consistently. They also establish expectations for the development and implementation of user complaint systems.[6,8,11,16]

Existing codes set clear expectations regarding the measures platforms should implement to mitigate users' exposure to harmful content. These measures include proactive content moderation requirements[6,7,9,10] and the use of technology-assisted methods such as hash matching[i], URL detection and machine learning.[6,7,11]

Addressing Persuasive Design

The attention economy underpinning many digital platforms has led to the widespread deployment of platform features intentionally designed to maximize user engagement and prolong use.[17] Children and adolescents are known to be particularly vulnerable to many of the persuasive design mechanisms currently employed by platforms because of their developmental stage and evolving capacity for self-regulation.[3]

Among existing children's codes, the European Union's (EU) approach provides particularly detailed guidance on persuasive and otherwise harmful design.[6] Other jurisdictions have recognized gaps in their existing frameworks or faced criticism for failing to adequately address harmful design.[18,19] Children's codes provide regulators with a critical mechanism to address risks to children at the level of platform design by restricting existing harmful features, requiring safer defaults and establishing expectations for the introduction of new safety features.

Children's codes provide regulators with a critical mechanism to address risks to children at the level of platform design by restricting existing harmful features, requiring safer defaults and establishing expectations for the introduction of new safety features.

[i] Hash matching is a digital process that helps platforms proactively detect and prevent the spread of known harmful content by comparing uploaded files against a database of digital fingerprints.[26]

Modification of Existing Features – Account Discoverability
The EU's code requires platforms to prevent children's accounts from being discoverable by unknown users, particularly adults, by excluding them from account recommender systems and ensuring that their personal information and account activity are not visible to users they do not know. Privacy-sensitive features, including geolocation, microphone, camera and unnecessary tracking functions, are also disabled by default.[6]

Modification of Existing Features – Compulsive Use
The EU's code further directs platforms to protect children from design features that encourage excessive use. Several features are identified for disabling by default, while retaining the regulatory authority to require that persistently harmful design features be removed altogether. These features include infinite scroll, push notifications, "is typing" notifications, filters associated with negative body image, streaks and autoplay.[6] The EU's code also provides that, where a minor chooses to enable one of these features, they should receive a clear warning about the associated risks, be given the option to enable the feature only temporarily and receive periodic reminders of the option to reverse the setting.[6]

Integration of New Features
The EU's code specifies that minors should have access to customizable time-management tools to deter excessive use, nudge safer behavioural choices and remind children how long they have spent on a platform.[6] The code mandates that the content an algorithm serves to children should be determined primarily by a child's explicit choices, rather than inferred from their activity on a platform.[6] Codes also require platforms to introduce user controls, such as the ability for children to accept or reject whether they are tagged in content, while some introduce parental-control requirements for managing screen time, account settings and user activity.[6,7] **Importantly, the EU's code makes it clear that digital services should not rely exclusively on parental tools to ensure the privacy, safety and security of minors. Rather, such tools are intended to complement platforms' responsibility to ensure that their products are safe by design**.[6]

MULTI-STAKEHOLDER DEVELOPMENT

The development of a children's code must be informed by an evidence-led and consultative process. Regulators across the jurisdictions considered in this brief have drawn on empirical evidence,[19] consulted with children to better understand their online experiences[20-22] and sought input from industry, civil society, child safety experts, parents and caregivers.[23-25]

RECOMMENDATION

Given Bill C-34's focus on child safety and platforms' responsibility to protect children who use their services, if the Bill is enacted, the Digital Safety and Data Protection Commission should prioritize the development of a dedicated, comprehensive children's code. The Commission should develop this code in consultation with youth, caregivers and child health experts, ensuring that child safety and privacy by design are central to the Safe Social Media Act's regulatory framework.

This Issue Brief was prepared with the generous support of the Waltons Trust, One Child Every Child, the McConnell Foundation and ResetTech. We are grateful for their ongoing partnership.

Date of Publication
October 30, 2026

Recommended Citation
Healey, C., Hall, C., & Moore Hepburn C. (2026) Setting the Standard: A Children's Code for the Safe Social Media Act. [Issue Brief] Hospital for Sick Children/Child Health Policy Accelerator.

References

1. Abi-Jaoude E, Naylor KT, Pignatiello A. Smartphones, social media use, and youth mental health. ***CMAJ***. 2020;192(6):E136-E141. doi:10.1503/cmaj.190434
2. Ofcom. ***Exploring the relationship between persuasive design on online platforms and the time that children spend on them***. Ofcom; 2026. Accessed July 31, 2026. https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/childrens-online-experiences/exploring-the-relationship-between-persuasive-design-on-online-platforms-and-the-time-that-children-spend-on-them/exploring-the-relationship-between-persuasive-design-on-online-platforms-and-the-time-that-children-spend-on-them.pdf?v=418215
3. Patel R, Hall C, LeBel L, Moore Hepburn C. ***The Architecture of Attention: Persuasive Design Features and Child Well-being on Digital Platforms*** [Issue Brief]. The Hospital for Sick Children, Child Health Policy Accelerator; 2026. https://www.sickkids.ca/contentassets/bd08c50e557247ab87eb3e4ed07894e1/persuasive-design-brief.pdf
4. Bill C-34, An Act to enact the Digital Safety Act and the Digital Safety Commission of Canada Act and to make consequential amendments to other Acts (Safe Social Media Act). 1st Sess. 45th Parl. First reading June 10, 2026. Accessed June 23, 2026. https://www.parl.ca/Content/Bills/451/Government/C-34/C-34_1/C-34_1.PDF
5. Ofcom. ***Protection of Children Code of Practice for User-to-User Services***. 2025. Accessed July 20, 2026. https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-protecting-children-from-harms-online/main-document/protection-of-children-code-of-practice-for-user-to-user-services.pdf
6. European Commission. 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. ***Official Journal of the European Union***. 2025. Accessed July 20, 2026. https://eur-lex.europa.eu/eli/C/2025/5519/oj/eng
7. Coimisiún na Meán. ***Online Safety Code***. Coimisiún na Meán; 2024. Accessed July 31, 2026. https://www.cnam.ie/app/uploads/2024/11/Coimisiun-na-Mean-Online-Safety-Code.pdf
8. eSafety Commissioner. ***Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material): Head Terms***. Australian Government; 2023. Accessed July 20, 2026. https://www.esafety.gov.au/sites/default/files/2023-09/Consolidated-Industry-Codes-of-Practice-Head-Terms-12-September-23.pdf?v=1784811744765
9. eSafety Commissioner. ***Consolidated Industry Codes of Practice for the Online Industry (Class 1C and 2 Material): Head Terms***. Australian Government; 2025. Accessed July 20, 2026. https://www.esafety.gov.au/sites/default/files/2025-09/Consolidated-Industry-Codes-of-Practice-for-the-Online-Industry-%28Class-1C-and-Class-2-Material%29-Head-Terms-9-September-2025.pdf?v=1784811744765
10. eSafety Commissioner. ***Schedule 1—Social Media Services Online Safety Code (Class 1A and Class 1B Material)***. Australian Government; 2023. Accessed July 20, 2026. https://www.esafety.gov.au/sites/default/files/2023-06/Schedule-1%E2%80%93Social-Media-Services-Online-Safety-Code-%28Class-1A-and-Class-1B-Material%29.pdf
11. eSafety Commissioner. ***Schedule 4—Social Media Services (Core Features) Online Safety Code (Class 1C and Class 2 Material)***. Australian Government; 2025. Accessed July 20, 2026. https://www.esafety.gov.au/sites/default/files/2026-03/Schedule-4-Social-Media-Services-Core-Features-Online-Safety-Code-Class-1C-and-Class-2-Material.pdf
12. eSafety Commissioner. ***Schedule 4A—Social Media Services (Messaging Features) Online Safety Code (Class 1C and Class 2 Material)***. Australian Government; 2025. Accessed July 20, 2026. https://www.esafety.gov.au/sites/default/files/2025-09/Schedule-4A-Social-Media-Services-Messaging-Features-Online-Safety-Code-Class-1C-and-Class-2-Material.pdf

13. eSafety Commissioner. Online Safety Codes and Standards compliance. Australian Government; 2025. Accessed October 8, 2026. https://www.esafety.gov.au/industry/codes/compliance
14. eSafety Commissioner. Enforcement actions and outcomes. Australian Government; 2026. Accessed October 8, 2026. https://www.esafety.gov.au/industry/codes/enforcement-action
15. Ofcom. ***Year 1 Online Safety Risk Assessments: Report on standards and improvements***. Office of Communications; 2025. Accessed October 8, 2026. https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/research-statistics-and-data/os-standards/online-safety-risk-assessments-report-year-one.pdf?v=408834
16. Coimisiún na Meán. Online Safety Code. Coimisiún na Meán; 2024. Accessed October 8, 2026. https://www.cnam.ie/app/uploads/2024/11/Coimisiun-na-Mean-Online-Safety-Code.pdf
17. 5Rights Foundation. ***Disrupted Childhood: The Cost of Persuasive Design***. 5Rights Foundation; 2024. Accessed July 23, 2026. https://5rightsfoundation.com/wp-content/uploads/2024/08/5rights_DisruptedChildhood_G.pdf
18. Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts. ***A Digital Duty of Care for Australia: Developing a Duty of Care Framework for Online Services Used by Australians***. Australian Government; 2026. Accessed October 8, 2026. https://www.infrastructure.gov.au/sites/default/files/documents/digital-duty-of-care-for-australia-developing-duty-of-care-framework-for-online-services-used-by-australians-may2026.pdf
19. Wood S. Impact of regulation of children's digital lives: phase II. Digital Futures for Children Centre, London School of Economics, and 5Rights Foundation; 2026. Accessed August 4, 2026. https://researchonline.lse.ac.uk/id/eprint/138377/
20. Coimisiún na Meán. ***Video-Sharing Platform Services Online Harms Evidence Review***. PA Consulting; 2024. Accessed July 31, 2026. https://www.cnam.ie/app/uploads/2024/11/PAConsulting_Online-Harms-Evidence-Review.pdf
21. Ofcom. ***Consulting Children on Protection of Children Online Safety Proposals***. Revealing Reality, Ofcom; 2025. Accessed July 31, 2026. https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/research-statistics-and-data/protecting-children/consulting-children-on-protection-of-children-online-safety-proposals.pdf
22. Moody L, Marsden L, Nguyen B, Third A. ***Consultations With Young People to Inform the eSafety Commissioner's Engagement Strategy for Young People: A Report on the Findings***. Young and Resilient Research Centre, Western Sydney University; 2021. Accessed July 31, 2026. https://www.esafety.gov.au/sites/default/files/2022-01/YRRC%20Research%20Report%20eSafety%202021_web%20V06%20-%20publishing_1.pdf
23. Coimisiún na Meán. ***Youth Advisory Committee Report on Consultation on the Draft Online Safety Code; the Draft Statutory Guidance Material and the proposed application of the Online Safety Code to the Category of Video-Sharing Platform Services***. Coimisiún na Meán; 2024. Accessed July 31, 2026. https://www.cnam.ie/app/uploads/2024/11/Youth-Advisory-Committee-Report.pdf
24. Shaffique MR. ***Digital Services Act: Summary Report on the Targeted Public Consultation on the Protection of Minors Guidelines***. European Union. Accessed October 8, 2026. https://digital-strategy.ec.europa.eu/en/library/digital-services-act-summary-report-targeted-public-consultation-protection-minors-guidelines
25. Ofcom. ***Protecting Children from Harms Online***. Office of Communications. Accessed October 8, 2026. https://www.ofcom.org.uk/online-safety/protecting-children/protecting-children-from-harms-online
26. Thorn. How Hashing and Matching Can Help Prevent Revictimization. Thorn; 2023. Accessed October 8, 2026. https://www.thorn.org/blog/hashing-detect-child-sex-abuse-imagery/