David Young Law
Compliance Bulletin

November 2026

OPC's Children's Privacy Code – precursor to a statutory design code for platforms?

At the end of September, following a stakeholder consultation over the summer of 2025, the Office of the Privacy Commissioner of Canada published its *Children's Privacy Code*, a guidance document for organizations interacting with children and youth through online platforms. The Code can be viewed as the latest instalment in the evolving worldwide environment to protect children and youth from online harms. Its origins may be traced back to the UK Information Commissioner's Office's 2022 statutory code of practice for online communications with children, titled *Age appropriate design: a code of practice for online services*. Since the publication of the UK Code, its precedent has been followed in diverse international jurisdictions.[1] More critically, events and legal developments have overtaken the specific focus of protective rules for the protection of children's privacy.

In Canada, the Tumbler Ridge tragedy, involving the interaction of the ChatGPT AI tool with a youth contemplating gun violence, has pushed to the top of the federal government's legislative agenda re-introduction of an online harms law with a primary focus of protecting children from online risks, as well as the continuing attempt to modernize the private sector privacy law with legislation that will strengthen children's protections.[2] Furthermore, the government's initiatives in these areas must be viewed in the context of its proposed transferring of privacy oversight to a new regulator, the Digital Safety and Data Protection Commission of Canada, which will have jurisdiction for both privacy and online harms.

In the US, significant judicial developments over the course of 2026 have seen court cases and settlements resulting in multi-billion dollar awards against social media platforms for injury caused to youth through addiction to social media and for otherwise endangering the safety of youth.[3]

In the face of these developments, much of the regulatory focus is now on preventing harm to children and youth through online interactions as opposed to the arguably narrower focus of protecting their personal information. Consistent with the government's proposed online harms law, other governments both domestic and international have enacted or are proposing: social media bans for children and youth, legislation banning addictive social media features

---

[1] See: Data Protection Commission (Ireland), *The fundamentals for a child-oriented approach to data processing*, December 2020; Australian Information Commissioner, *Privacy (Children's Online Privacy) Code 2026* (Exposure Draft); *The California Age-Appropriate Design Code Act*.

[2] Bill C-34, *Digital Safety Act*; Bill C-36, *Protecting Privacy and Consumer Data Act* (PPCDA).

[3] In March, Meta and You Tube were found liable in California for substantial damages caused to youth by addiction to social media and, in New Mexico, Meta was found liable for misleading consumers and endangering children respect to the safety of its platforms. In August Meta settled a court case with 47 states, the District of Columbia and U.S. territories, agreeing to pay up to $17.1 billion in penalties for claims that it posed dangerous risks to children by its addictive social media platforms.

 © David Young Law 2026

directed at children, and rules regulating or prohibiting chat bot interactions with children.[4]

However, as articulated by the UK Commissioner in her introduction to the ICO Code, privacy protection is at the heart of risks to children when they interact online:

> [Personal] Data sits at the heart of the digital services children use every day. From the moment a young person opens an app, plays a game or loads a website, data begins to be gathered. Who's using the service? How are they using it? How frequently? Where from? On what device?
>
> That information may then inform techniques used to persuade young people to spend more time using services, to shape the content they are encouraged to engage with, and to tailor the advertisements they see.

Therefore, it is timely for the OPC to publish the *Children's Privacy Code* now, understanding that it should be read in this broader context of protecting children and youth online.

Code as a guidance document

Unlike the UK Code and similar initiatives in a number of US states which have the force of law, [5] the OPC's Code is a guidance document. While it includes what may be characterized as "bright-line" rules or standards as are found in the UK Code, the thrust of the Code is to provide guidance or reference points for organizations considering interactions with children online, all in the context of ensuring compliance with the operative private sector privacy law, PIPEDA.[6] The Code sets out what it describes as robust privacy-protective expectations for organizations that collect, use or disclose children's personal information, to be grounded in privacy rights deserving of enhanced protection and that such protection should be embedded into the design practices of all online interactions with children and youth.

In sum, the Code is broader than simply a compendium of "black letter" rules and should be treated as guidance regarding how the OPC interprets the relevant statutory provisions – specifically PIPEDA – and what it expects from organizations in terms of compliance with those provisions.

Application and scope

The Code is intended to apply to all interactions with children under the age of 18 and to all organizations governed by

[4] See, for example, *Davis & Gilbert Alert*, Sept. 26, 2026: California has signed into law the nation's most far-reaching package of online child safety legislation, including a ban on addictive social media features for users under 16, the strongest companion chatbot regulations for children, and enhanced civil penalties for platforms that harm children. The law significantly expands the obligations of chatbot operators to conduct risk assessments and prevent harm and introduces both public enforcement mechanisms and a private right of action.

[5] For example, *The California Age-Appropriate Design Code Act*; similar legislation is now law in New Jersey, South Carolina, Nebraska, Vermont and Maryland and has been proposed in various forms in other states including Connecticut, Illinois, Georgia, Kansas, Michigan, Minnesota, New Mexico, Rhode Island, and Washington.

[6] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5.

PIPEDA that collect, use or disclose personal information – specifically those involving an online commercial service (including websites, applications, platforms and digital tools) that is directed at children or is likely to be accessed by children.

The Code makes clear that it applies irrespective of whether an organization intends to direct its service to children – in other words even if not intended to be so directed, if the service is likely to be accessed by children, the Code will apply. The Code provides guidance indicators to assist organizations in determining whether either of these criteria apply to a particular service.

Key principles – best interests of the child and their evolving capacities

The Code articulates certain "Foundational Principles", which it describes as the overarching values and considerations that underpin the Code, as opposed to specific obligations. These principles are intended to communicate the intent of the Code and are to be considered by organizations when interpreting its specific rules, and in exercising judgement and determining how the requirements apply in any specific context.

Key among these principles are the recognition that decisions regarding operationalizing any child-related interaction must take into account the *best interests of the child*, that such decisions must address child-specific risks that are distinct from those affecting adults, and that as children grow they have an evolving capacity to understand and make privacy-related decisions.

With respect to this last-mentioned principle, the Code applies an age-based sliding scale of criteria and requirements for parental assistance and a child's independent capacity to understand and make privacy-related decisions, in particular those related to consent. Consistent with this age-related decision sliding scale, the Code further articulates a principle of parental support and guided autonomy in relation to a child's understanding and exercise of judgement, also applied on a sliding scale basis, reflecting increasingly complex online activities, with increasing levels of risk. In this latter regard, the Code states that where parental controls are offered, they should be age-appropriate, support children's agency, and respect children's rights, evolving capacities, and the best interests of the child.

A key precept advanced by the Code, consistent with these sliding scale rules, is that where an organization has sufficient information to reasonably conclude that a user is, or is likely to be, a child, it should apply privacy protections appropriate to the child's age and developmental stage.

Expectations and prohibited practices – the key rules

The core of the Code is contained within its sections that set out "Expectations" and "Prohibited Practices". These provisions articulate what can be considered the key compliance rules of the Code, analogous to the "standards" set out in the UK Code, although in certain instances they are articulated as simply expectations or best practices as opposed to hard and fast rules. In each of these instances of compliance standards, the Code includes useful and, in some instances illustrative, examples of non-compliance and of how the expected compliance should be executed.

These rules are as follows.

Consent - Organizations must obtain meaningful consent for the collection, use and disclosure of children's personal information, calibrated to the child's evolving capacity. Non-essential data uses should require express, opt-in consent with separate choices offered for each optional feature or enhancement. Organizations should allow children and their parents or guardians to withdraw consent at any time.

Privacy impact assessments - Organizations are encouraged to conduct a privacy impact assessment, especially when offering higher-risk products or services.

Default high privacy settings - Services covered by the Code should be configured to the highest available privacy setting by default. The collection and use of location data, and the public visibility of profiles should be off by default.

Data minimization - Organizations must limit the collection of children's personal information to what is directly necessary for the service. Personal information collected from children must not be retained for longer than is necessary for the purpose for which it was collected.

Transparency - Organizations should provide privacy information that is clear, accessible and age appropriate.

Correction and deletion - Children should have practical means of correcting personal information that is inaccurate or incomplete as well as of deleting their personal information.

Avoiding profiling - Organizations should not use children's personal information to build profiles on them or for purposes that could harm them. Where profiling informs automated decisions about children, the best interests of the child should be the primary consideration.

Prohibited practices – Organizations must not use practices such as deceptive design patterns that are incompatible with the protection of children's privacy and their best interests. Specifically, organizations must not use such practices to deceive children into disclosing more personal information than they would otherwise choose to share or undermine their ability to exercise meaningful privacy choices. Deceptive design patterns in web interfaces may be used to influence, manipulate, or coerce youth users to make decisions that are not in their best interests, by exploiting psychological and behavioural characteristics through engagement mechanisms.

The Code also identifies as prohibited, practices that introduce or amplify privacy harms, which it describes as privacy harms that can arise from practices that, regardless of intent, create conditions in which children's personal information is exposed to risks that they may not understand or be able to anticipate.

As a general proposition, the Code states that organizations should take particular care where their data practices rely on information about a child's age, developmental stage, behaviour, emotional state or other characteristics, to make decisions about how the child's personal information is collected, used or disclosed. In this regard, organizations should not use such information to exploit a child's vulnerabilities or to expand the collection or use of their personal information in ways that are inconsistent with the child's reasonable expectations or best interests.

The Code in the context law reform and other developments

As noted, the government has introduced legislation to update the current privacy law, PIPEDA, as well as to establish a framework for protection of children and youth from online harms. In regard to the privacy law reform, the proposed PPCDA echoes certain of the themes found in the OPC's Code – in particular the precepts of the best interests of the child and the that children require special protections in regard to the collection, use and disclosure of their personal information. The PPCDA also stipulates a definition of a child as a person under the age of 18, consistent with the Code. However the proposed law does not provide for any statutory recognition of a children's code, containing specific rules as are found in the OPC's document. Further to be noted, there is no reference in the Code to alignment with the proposed PPCDA, or even reference to its provisions as may impact children. Presumably, the Code will need to be revised to reflect these if that legislation becomes law.

Additionally, the Code must be viewed in the context of the evolving legislative and judicial developments regarding children's online harms generally. In particular, a key focus of the government's proposed *Digital Safety Act* is the protection of children and youth from harmful online content, victimization and exploitation. As can be appreciated, any such activity inherently involves the obtaining and use of personal information about an individual.

Significantly, the *Digital Safety Act* contemplates the potential for a statutory code of practice for online platforms. The requirement for platforms to adopt child-protective design features may be seen as a vehicle for the proposed Digital Safety and Data Protection Commission to articulate in effect a mandatory design code that addresses not only online harms but also the related protection of children's online privacy. In the context of the projected transfer of the OPC's private sector oversight role to the Commission, it may be surmised that the Code could inform the development of such a statutorily-mandated children's online design code. In this regard, it is pertinent to note the GDPR's recognition of the risks to the rights and freedoms of children that may result from processing their personal data potentially leading to physical, material or non-material injury.[7]

The OPC is soliciting comments on the Code until January 20, 2027, after which it may publish an updated version of the Code.

For more information please contact: David Young 416-968-6286 david@davidyounglaw.ca
Note: The foregoing does not constitute legal advice. © David Young

[7] *General Data Protection Regulation*, Recital 75.