Ontario

Ministry of Public and Business Service Delivery and Procurement
Strategy, Artificial Intelligence, Data
Artificial Intelligence Division

Age-Appropriate Use of Digital Technology: Best Practices for Ontario Public Organizations

Table of Contents

Introduction 2

Who is this document for 2

Guidelines for age-appropriate technology use 2

1. Prioritize learning about digital safety 2

Technology that is age-appropriate 3

Understanding digital safety 3

Common risks 3

Respecting Indigenous data protocols 3

Recommended actions to consider 4

Useful resources 4

2. Protect children and youth's data and privacy 4

Data minimization practices 4

Be transparent about how data is collected, used and shared 4

Recommended actions to consider 5

Useful resources 5

3. Use safe applications and services 6

Manipulative design patterns 6

Recommended actions to consider 6

4. Use artificial intelligence (AI) responsibly 7

AI can reinforce bias 7

AI use may not be transparent 7

AI can generate misinformation and disinformation 7

Recommended actions to consider 7

Useful resources 8

Conclusion 8

Acknowledgements 8

Appendix A: Examples of nudging 9

Appendix B: Addictive feed patterns 10

Appendix C: Examples of predatory marketing 11

Introduction

These best practices are for organizations in Ontario's public sector, who are involved in helping children and youth to safely use digital technology. They complement the new O.Reg. 52/26 under Enhancing Digital Security and Trust Act, 2024, which establishes a foundation for government to strengthen **cyber security**, enhance **privacy safeguards for children** and support the responsible use of **artificial intelligence**. The information provided in this document should not be considered formal direction to the sectors and does not create legal obligations.

This document:

- Provides an **overview of key issues and concepts** relating to digital security.
- Outlines **resources** that support the assessment of current technology practices.
- Recommends **specific best practices** to avoid potential harm to children and youth.

This document is informed by four guiding principles:

1) Prioritize learning about digital safety
2) Protect children and youth's privacy and data
3) Use safe apps and services
4) Use artificial intelligence (AI) responsibly

The information and recommendations provided in this document are not mandatory. Some existing formal policies have been referenced below, however this is not an exhaustive list of applicable policies in Ontario and Canada.

Individual organizations are responsible for ensuring they are aware and following any legislation, regulation, directives or policies, which may apply to them when it comes to the privacy and protection of children and youth using digital technologies. Should these conflict with this guidance, the applicable legislation, regulation, directives and policies would prevail.

Examples of other existing policies which may apply, include:

- *Child, Youth and Family Services Act, 2017*
- *Education Act*
- *Freedom of Information and Protection of Privacy Act*
- *Municipal Freedom of Information and Protection of Privacy Act*

Intended Audience

The following is designed for organizations such as:

- School boards
- Children's Aid Societies and Indigenous Child and Family Well-being Agencies

However, this may be useful for anyone who want to understand and apply best practices for supporting children and youth in their use of digital technology.

Guidelines for age-appropriate technology use

1. Prioritize learning about digital safety

The first step in protecting children and youth is understanding the digital risks they face. This requires education for those who work with them, for parents and guardians, and for children and youth themselves.

A child or youth's "rights", as used in this document, refers to the guarantee of fundamental human rights and freedoms that a person under 18 have, ensuring protection from discrimination and harms (UN Convention on the Rights of the Child).

Public sector organizations should ensure their digital policies continue to uphold the rights of children and youth as technologies evolve. Policies should remain adaptable and be regularly reviewed and updated in collaboration with children, youth, families, communities, and subject-matter experts to maintain their relevance and effectiveness.

Technology that is age-appropriate

Children and youth should use digital technology that is developmentally suitable, proportionate to cognitive maturity, and aligned with their best interests.

Decisions about what digital applications children and youth use, including how and why they use them, should seek to support their best interests including their health and well-being, freedom of expression, safety, and privacy. Children and youth have diverse needs, contexts, capabilities and interests, and decisions about use of digital technology should seek to reflect and be inclusive of this diversity.

Organizations providing public services to children and youth should help parents/guardians, caregivers and educators understand how technology interacts with developmental milestones that children experience and how to protect their rights (Child Rights by Design, Digital Futures Commission). This can support differentiated approaches that can best nurture each child in their growth.

The Canadian Paediatric Society recommends limiting screen time for children over the age of five to less than two hours a day (and less than one hour for children two to five).

Understanding digital safety

While technology offers opportunities for learning and creativity, there are also significant risks. Researchers agree that excessive use of online tools such as social media and online games can have negative impacts on children and youth's health and well-being. Deepfakes, cyberbullying and other harmful online experiences can have an enormous impact on a child or youth mental health.

Common risks

Children and youth face some common risks when they are online, including:

- **Content risks**: exposure to inappropriate content such as sexual or violent images, some forms of harmful advertising and websites displaying dangerous behaviours.
- **Contact risk**: inappropriate interaction between a child and adult. This can include the adult seeking sexual favours from a child or trying influence them with radical or extremist ideologies.
- **Conduct risk**: negative behaviour resulting from exposure to negative content and contact. These behaviours negatively affect both the child and their peers, and may include bullying, self-harm or sharing of harmful material.
- **Contract risks**: when a child accepts an arrangement with conditions that can be exploitative with little control or means of escaping. This may include accepting the Terms of Service or Terms and Conditions of a commercial provider of a digital product or service.

In addition to these risks, barriers to digital access in children and youth may reduce digital literacy. This reduced digital literacy could potentially increase vulnerability to digital harms, such as online grooming.

Respecting Indigenous data protocols

First Nations, Inuit, Métis and urban Indigenous children and youth have unique physical, emotional, social, cultural, linguistic, and spiritual needs. These needs may include strong connections to their immediate and extended families, community, and people. Identifying the best interests and rights of Indigenous children and youth often requires a broader understanding of factors that may affect their health and well-being.

First Nations, Inuit and Métis communities are recommended to lead the management of data for their communities, land, people, and resources. Respecting the different expectations that First Nations, Métis, and Inuit peoples have about their privacy and information can help Indigenous children and youth use digital technology in a way that support health and well-being and respect culturally based practices.

Recommended actions to consider

- Promote digital literacy skills to help children and youth use digital technology safely and responsibly.
- Empower children and youth to have an authentic voice in their digital experiences. Let them share their opinions about how they use digital technology and inform digital policies.
- Support awareness amongst children, youth and parents/guardians about technology-related harms and cyberbullying (covered by the *Education Act* under PPM 144 *Bullying prevention and intervention*).
- Learn about distinction-based Indigenous data protocols. Engage with Indigenous organizations whenever possible to ensure that technology used in school settings does not undermine data principles, treaties or other important cultural values.

Useful resources

- For more about **making decisions on children's digital technology use**, refer to the Government of Canada's Child Rights Impact Assessment (CRIA).
  - The Information and Privacy Commissioner of Ontario's study guides to help children and youth learn about the importance of personal privacy.
  - The Office of the Privacy Commissioner of Canada's information, tools and other resources to help adults working in the public sector engage with children and youth about their privacy.
- For more on **distinction-based Indigenous data protocols**, refer to:
  - the First Nations principles of OCAP™ (ownership, control, access, possession).
  - the Métis principles of OCAS (ownership, control, access and stewardship).
  - the Inuit principles of Qaujimajatuqangit (traditional knowledge).
- For more on **recommended screen times**, refer to the Canadian Paediatric Society.
- For more on cyber security in the public sector, refer to the resources provided by the Cyber Security Centre of Excellence.

2. Protect children and youth's data and privacy

Privacy risks increase as children and youth increasingly use more digital technology, especially when they are required to share personal information.

For example, sharing information like a child's location could be used by others to find and target them. This is a particular concern for children and youth in care who are frequently targeted for human trafficking or may be estranged from family for their safety.

A balanced approach is recommended to leverage the benefits of the technologies that children, youth, educators, parents/guardians and/or caregivers enjoy while reducing privacy risks and harmful consequences.

Data minimization practices

"Data minimization" is the principle of limiting the collecting, processing, storing and sharing of personal information/ data to only what is necessary to deliver a specific service.

It is recommended to check how much access products or tools have to children and youth's personal information. Limiting access to children and youth's personal information reduces the risk of information being used in harmful contexts such as for predatory marketing, profiling or data monetization purposes.

For Children's Aid Societies, data minimization is outlined in the *Child, Youth and Family Services Act, 2017, Part X*.

Be transparent about how data is collected, used and shared

Be clear with children and youth, and their parents/guardians and caregivers about what they can expect from with respect to their personal information and data when using digital technology. It is recommended that children, youth and their parent or guardian are made aware of how their data is being used or processed and have control over what information is shared.

It is also considered a best practice to inform and potentially seek a person's agreement or consent when it comes to how their data is being used. Informed consent is when a person clearly understands how their data will be used and voluntarily agrees to it. Important parts of ensuring informed consent include the following.

- the purpose of the technology or application being used
- what information is being collected
- how their information will be used
- the risks of sharing their information

Recommended actions to consider

- Give children and youth tools and resources to help them understand and feel empowered to assert their privacy rights.
- Apply the strongest privacy and security settings possible to digital tools and applications used by children and youth in public sector settings to help keep personal information safe. These settings should be implemented as the default setting.
  - Keep geolocation tracking off by default. When geolocation is needed, ensure software clearly says when a user's location is being tracked.
  - Use depersonalized or generic accounts where possible.
  - Assess the risks of using connected devices before giving them to children and youth. Monitor connected devices to ensure that Wi-Fi, Bluetooth, cameras and microphones are turned off when not in use.
- If a digital tool or application is being considered, it is important to review how data is used in the applications and assess if there are any potential risks. Conduct a Privacy Impact Assessment (PIA) when:
  - Implementing a new system that collects, uses or discloses personal information.
  - Making changes to an existing system that collects, uses or discloses personal information.
  - Refer to the PIA to regularly monitor and review the use of data in the system.
- Make sure applications communicate clearly, in plain language, how information is collected. Where possible, translate notices into languages used in the child's communities.
- Where possible, share the terms of use or end user license agreements of applications to support transparency on the use of personal information.
- Establish procedures to notify parents/guardians and caregivers when you become aware of incidents or harms such as cyberbullying or deepfakes.
- Introduce contractual provisions with third-party vendors to support children and youth's privacy and data minimization in applications or services, which may be in addition to any provisions required by law. For example:
  - allowing students to access and correct their personal information
  - agreeing to only collect data for the purposes outlined in the agreement
  - including easily accessible privacy tools such as "see all my data", "download my data", "delete all my data;" etc.

Useful resources

- For more information on **how to protect students' privacy** when using digital technology, refer to the Information and Privacy Commissioner's Digital Privacy Charter for Ontario Schools.
- For more information on **how to be transparent about the technology** used in schools, refer to the Ontario Association of School Business Officials (OASBO)'s Guidance on Notification and Consent Requirements When Using Digital Tools.

3. Use safe applications and services

Digital products are increasingly designed to shape a user's behaviour in subtle ways. Design practices intended to increase engagement can negatively impact users, especially children and youth. Educating parents/guardians, caregivers, children and youth about safer digital practices can help support more informed choices and reduce potential risks.

Manipulative design patterns

Manipulative design patterns in technology intentionally lead users into taking actions they otherwise would not do, for example:

- signing up for email notifications
- buying something
- staying online for longer than intended

Examples of these patterns to be aware of include **nudging, addictive feeds** and **predatory marketing**.

Nudging is an application or software design feature that encourages users to make choices that follow a path that a designer or developer wants them to follow.

Nudging can be used positively and negatively:

- A neutral nudge presents users with a bias-free choice to make.
- A positive nudge can guide users to seek help when needed.
- A negative nudge may present users with choices but favour one over another.

Nudging may encourage children and youth to remove privacy protection features in the application. Applications used by children and youth should not have any nudging techniques that lower privacy protections.

See appendix A for some examples of nudging types.

Addictive feeds are often found on social media and digital applications, including those that use AI. They are designed to keep users engaged with content for extended periods of time. These feeds often contribute to excessive use.

Addictive feeds may use:

- **personalized algorithms**: showing content tailored for specific users to keep them engaged.
- **infinite scrolling**: no "end" to the content, making it difficult to stop using the application.
- **endless novelty**: notifications and constantly pushing new content to bring users back into an application.

See appendix B for more information on addictive feeds.

Predatory marketing can profile children and youth and show them targeted advertisements that may not be beneficial to their health (for example, snacks high in sugar) or wellbeing (for example, addictive free-to-play games with microtransactions).

See appendix C for more information on predatory marketing.

Recommended actions to consider

- Ensure that digital applications used by children and youth in public sector settings are ad-free.
- Be aware of and avoid technology that employs manipulative design patterns.
- Learn about the negative health impacts of addictive feeds.
- Limit predatory marketing by using anonymous accounts with limited personal information.

4. Use artificial intelligence (AI) responsibly

Artificial intelligence (AI) is being used more and more by children and youth and the organizations that support them. In public services, AI can help with learning, reduce time spent on routine tasks, and make programs run more smoothly. Teaching children and youth how AI works can help them use it safely and responsibly.

Generative AI (Gen AI) is increasingly used to process data, produce text, and generate media like images, videos or audio.

Commonly used Gen AI tools include:

- ChatGPT
- Microsoft Copilot
- Google Gemini
- Midjourney
- Claude
- DALL-E

Because AI is a new and evolving quickly, it is important to keep up to date when it comes to the specific risks associated with it:

AI can reinforce bias

Children and youth should be made aware that AI can sometimes be biased. Because AI learns from large datasets that may include human biases, it can accidentally reinforce stereotypes. For example:

- AI tools may be unfair to marginalized groups if the data they were trained on is incomplete or unbalanced.
- AI can repeat or strengthen racial or cultural biases, which may lead to unfair outcomes.

AI use may not be transparent

Whenever youth are using AI tools, it should be clear how the technology works and how their information is being used. Being transparent helps to protect their information, helps them to understand what data is being collected, and notice when something does not seem safe.

There should be a clear understanding of the limitations and risks of transparency in AI, for example:

- Some AI tools may store the personal information shared with them, or use data and original content to train models without clear consent.
- AI models often do not explain how their outputs are generated, which makes it less transparent.

AI can generate misinformation and disinformation

AI can create content that is misleading or completely false. This can be harmful to children and youth, but it can be opportunity to teach them about digital literacy.

Harmful false content includes:

- **Misinformation**: any false, inaccurate or subjective information presented as facts.
- **Disinformation**: intentionally false information meant to mislead or manipulate (for example, hoaxes and propaganda).
- **Deepfakes**: highly realistic but fake images, videos or audio that can cause confusion or reputational harm to a person.

Recommended actions to consider

- Set clear rules with children and youth on how to safely use AI, including the risks of using AI, circumstances where AI tools should not be used, and how they can protect their personal information and privacy when using AI.

- Create clear AI-use policies that address legal, ethical and privacy risks. Review policies with children, youth, parents, educators and the community to ensure AI use does not harm a child or youth.
- Build children and youth's AI literacy and critical thinking so they can judge whether AI-generated content is accurate and trustworthy.
- Apply an AI risk management process when giving children and youth access to AI tools.
- Use previously approved AI tools where possible to make sure they meet minimum safety and quality standards.

Useful resources

- To understand guidelines for ministries and provincial agencies on the transparent, responsible and accountable use of AI, refer to Ontario's Responsible Use of Artificial Intelligence Directive (which is part of the Ontario's Trustworthy AI Framework).
    - The directive only applies to ministries and provincial agencies but can be used as a helpful resource for information about the responsible use of AI.

Conclusion

Technology is continually evolving, and we recognize the need for this guidance to continually evolve as well. This is a living document that will be continuously reviewed and updated.

The ministry would be interested in feedback on this guidance. If you have any questions or feedback for this guidance, please email us at Digital.Government@ontario.ca.

Acknowledgements

Below is a list of ministries and program areas that reviewed and provided feedback on this guidance to date:

Ministry	Division
Ministry of Children, Community and Social Services	Child Welfare and Protection Division Strategic Policy Division
Ministry of Education	Strategic Policy and Planning Division
Ministry of Indigenous Affairs and First Nations Economic Reconciliation	Strategic Policy and Planning Division
Ministry of Public and Business Service Delivery and Procurement	Archives and Privacy Division Artificial Intelligence Division GovTechON Legal Services Branch

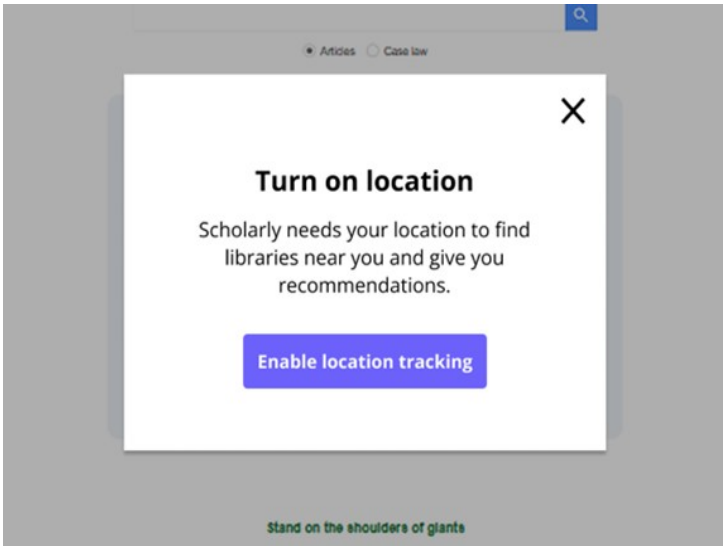
Appendix A: Examples of nudging

The table below shows three different examples of nudging types for one scenario: an app requesting location access.

Negative, neutral and positive nudging examples for location access request

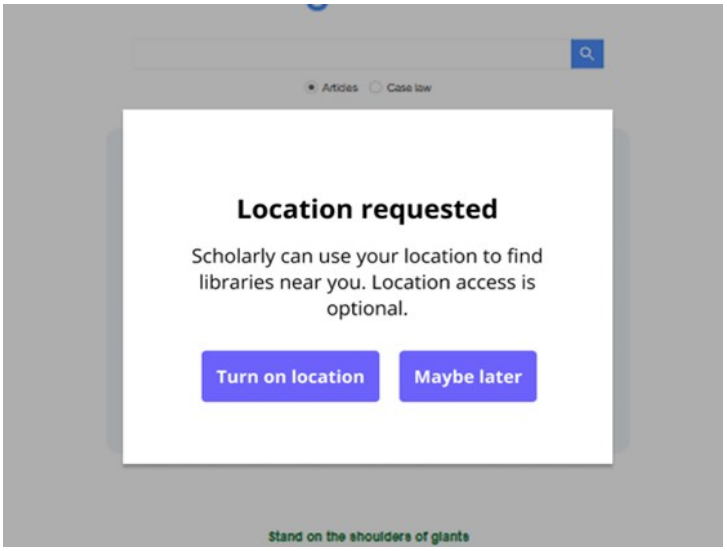
Negative nudging

- The single button makes it look like Enable is the only option.
- It's not clear that users can skip the request by clicking the "x" icon.
- Language makes it sound like location is needed for the app to work.



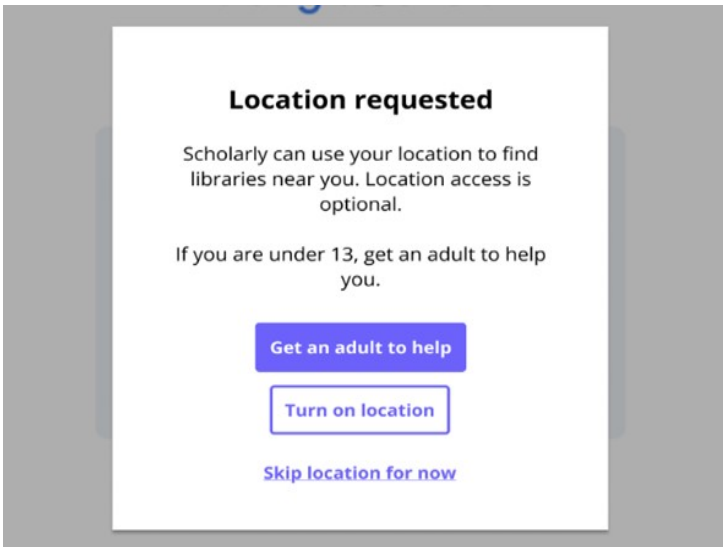
Neutral nudging

- Explains what location enabling will do and is clear that it's not mandatory
- Gives two options weighted equally: turn on location or skip and decide later.



Positive nudging

- Explains what location enabling will do and is clear that it's not mandatory
- Guides (nudges) younger users to get help from an adult as before making a choice.



Appendix B: Addictive feed patterns

Addictive feeds are used by different social media applications to maximize engagement of children and youth. These applications use different patterns to keep children and youth coming back to use these applications. Examples of these patterns include:

Tailored content: Applications collect data about interest, moods, habits to personalize content children and youth see. This data feeds into an algorithm to decides what a user sees based on these patterns, which causes them to stay on the application for a longer time.

Instant gratification: Due to its easy access and speedy rewarding, social media applications instantly provide children and youth with dopamine. Common actions such as, likes, comments and notifications provide small bursts of dopamine causing users to return for more validation.

Manufactured social connection: Feeling that a child is socially connected to a community. A brain releases dopamine when people make human connections, incentivising people to do it again (Addictive potential of social media, explained, Stanford Medicine). The sense of community causes users to stay connected through social media to avoid missing out on social interactions or community news.

Appendix C: Examples of predatory marketing

Predatory marketing is when a third-party application uses information to identify what a child or youth's interests are, and shares targeted advertisements based on those interests. These practices include deception, coercion and manipulation to expose vulnerabilities among youth.

Examples of predatory marketing include:

- **Data harvesting**: Gathering information of a child or youth's interests and shares advertisements based on those interests.
- **Social media manipulation**: Getting social media influencers to advertise a product that blends seamlessly with their content, making it difficult to distinguish what is an ad and what is content
- **Gamification**: Using gaming principles (such as competition with others, awarding points and badges) to encourage and motivate children and youth to interact with the application including encouraging in-app purchases for additional benefits
- **Pester power marketing**: Encouraging children and youth to continuously ask their parents or guardians to purchase a product or service