

Current Privacy Issues in K-12 Education

Fred Carter

Senior Policy and Technology Advisor

Office of the Information and Privacy Commissioner of Ontario



Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

National Leadership
Conference

CAIS

08 April 2019

Overview

About Us

M/FIPPA

IPC Guidance

Digital Literacy / Citizenship

Online Educational Services



Who Is the Information and Privacy Commissioner?

- Established in 1987, the Office of the Information and Privacy Commissioner of Ontario (IPC) oversees the province's access and privacy laws
- **Brian Beamish** appointed by Ontario Legislature (March 2015)
- 5-year term
- Reports to **Legislature**, not government or minister
- Ensures independence as government “watchdog”



IPC Policy

- Conduct **research** into matters affecting access and privacy
- **Comment** on proposed legislation or government programs
- Develop **guidance** to help institutions understand their legislative obligations
- **Educate** public and stakeholders about access and privacy laws, rights and issues (e.g. research, publications, public speaking)

MFIPPA Obligations

Collection, use, and disclosure rules

No **collection** unless:

- authorized by statute
- Used for law enforcement, or
- Necessary to lawfully authorized activity

No **use** unless:

- Consistent with the purpose for which information was collected
- Written consent

No **disclosure** unless:

- consent
- consistent purpose
- comply with legislation
- law enforcement
- health or safety
- For compassionate reasons

Security rules

Information must be **retained**

if used by an institution, it must be retained for at least one year

No **use** unless

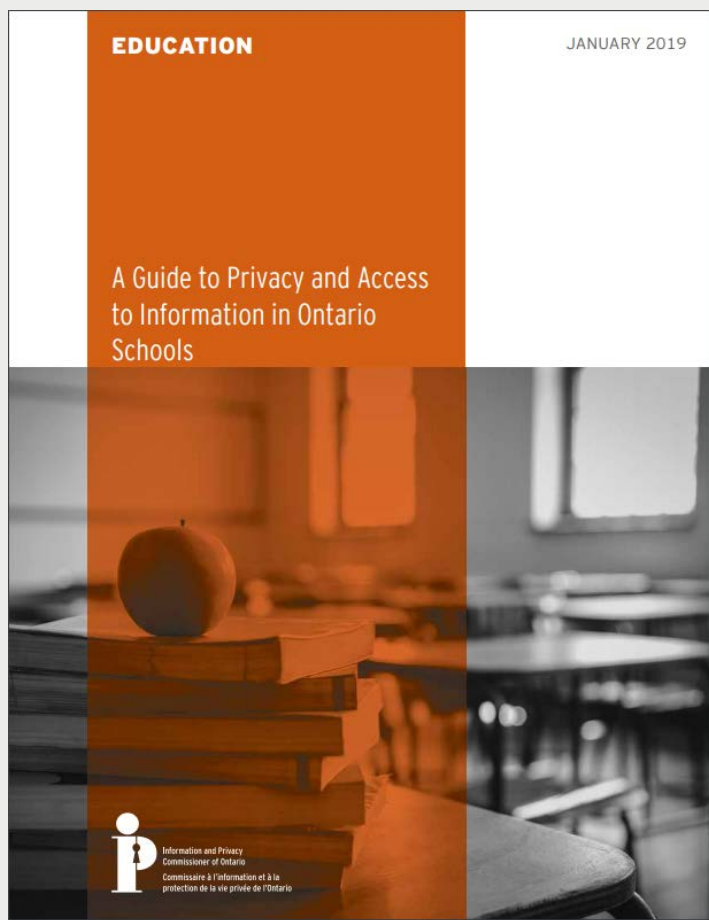
accurate
up to date

Information must be **protected**

from inadvertent disclosure and unauthorized access

IPC expects administrative, technical and physical measures to be in place to protect personal information

IPC Guidance for Ontario Schools



- Provides answers to common questions about privacy and access to information in the school system
- Goal to provide Ontario's school board officials and education professionals with an understanding of their rights and obligations in relation to the privacy of, and access to, students' personal information.

Source: <https://bit.ly/2spVb7J>

IPC Fact Sheets

| | | | |
|---|--|--|--|
| <p>Protecting Your Students' Privacy Online</p> <p>Online educational tools and social media provide new opportunities for teachers to learn, enhance educational techniques and connect with students, parents, and the greater community. Protecting students' privacy in the age of technology has never been more important.</p> | <p>EDUCATION FACT SHEET</p> | <p>Your Child's Privacy in School</p> <p>Ontario's information and privacy laws set the rules for how your child's personal information is collected, used and disclosed.</p> | <p>EDUCATION FACT SHEET</p> |
| <p>Privacy and Access to Information in Ontario Schools: A Guide for Educators</p> <p>INTRODUCTION</p> <p>Public and separate school boards must follow various laws when dealing with students' personal information.</p> | <p>EDUCATION FACT SHEET</p> | <p>Privacy in the School</p> <p>Ontario's privacy laws set rules for how schools collect, use and disclose students' personal information.</p> | <p>EDUCATION FACT SHEET</p> |

Available at: <https://www.ipc.on.ca/education/download-the-guide/>



Digital Literacy: Lesson Plans

LESSON PLAN

Know the Deal: The Value of Privacy

Grades 6 to 8

60-90 minutes class time, plus time in class or at home to complete the evaluation task

Getting the Toothpaste Back into the Tube: A Lesson on Online Information

Grades 6 to 8

2 to 4 hours—Approximately two hours lesson time; work time for the assessment/evaluation task will vary.

Privacy Rights of Children and Teens

Grades 9 to 12

1.5 — 2 hours

Available for download at: www.ipc.on.ca/guidance-documents/

Digital Literacy: FPT WG Collaboration

Educational Poster

5 TIPS TO PROTECT YOUR PRIVACY ONLINE

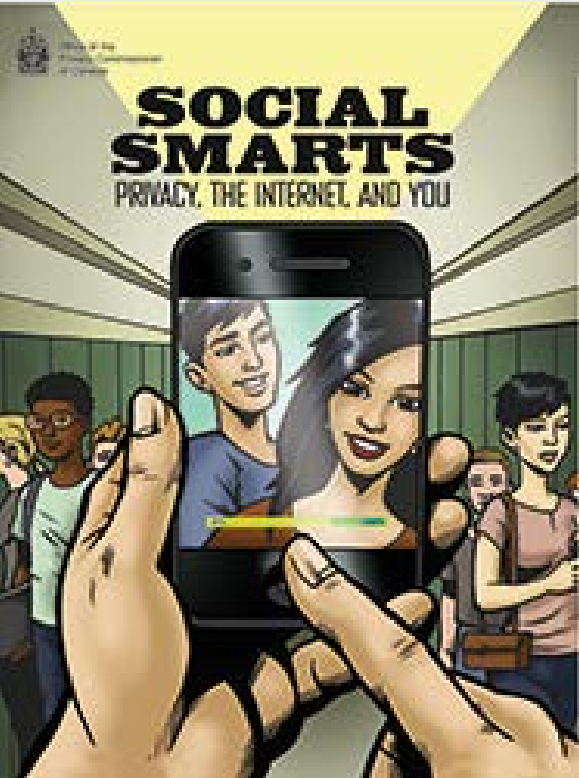
- 1 Think before you click!**
Really think about the photos, comments, messages and videos you want to post online, before you put them there.
- 2 Remember that things you post may not be private.**
Everything is shareable. People can copy comments, messages, photos and videos that you post online and send them to other people.
- 3 Know who your friends are.**
If you don't know someone in person, then you can't be sure who that person is online.
- 4 Protect your privacy with passwords**
It's important to password-protect your mobile device; use strong passwords on your accounts and don't share them with others.
- 5 Respect your friends' online footprints too.**
Before you post a photo or video with someone else in it, ask them if it's okay; and think carefully about what you say about others online.

If you're worried about something you see online, or have questions about how to protect your privacy, talk with an adult you trust.

Logos for various provincial privacy commissioners are listed at the bottom.

<https://bit.ly/2VP7JD9>

Graphic Novel



<https://bit.ly/2RDtBhP>

Discussion Guide

GRAPHIC NOVEL DISCUSSION GUIDE

Office of the Privacy Commissioner of Canada

Social Smarts: Privacy, the Internet, and You

You can use *Social Smarts* in your classroom to generate discussion about real-life situations to help young people learn to navigate online privacy risks. This graphic novel explores how a brother and sister start at a new school and learn about privacy risks related to social networking, mobile devices, texting and online gaming.

Learning goals / Big Ideas

Students will demonstrate the ability to:

- Explain why strategies like locking down privacy settings and using different passwords for different online sites can help mitigate risks to online privacy
- Understand how posting many little details can paint a big picture of who you are
- Explain why it can be impossible to delete a picture or comment once it has been posted online
- Suggest strategies to better protect privacy and navigate privacy issues in the online world
- Learn to be aware of the potential privacy risks of new digital communications technologies, such as those used for online gaming

Activity

Divide the class into 4 small groups, A, B, C and D, and have them read the graphic novel. When they have finished reading, give each group a piece of paper and a pencil. Have them put themselves in Dave and Amy's shoes – they are starting a new school and want to make sure that the kids at the school have the right picture of who they are.

Group A: Discuss what steps you can take to make sure that you have control of your online information. Why is it important to lock privacy settings and set strong passwords?

Group B: Discuss how you can make sure that the information you post doesn't give the wrong impression of who you are in real life. What sort of information is best left offline?

Group C: Discuss how you can learn about privacy risks of new technologies, such as online gaming devices, before you use them.

Group D: Discuss the importance of taking steps to protect your privacy on mobile devices.

1

<https://bit.ly/2soNM8X>



International Work



- ICDPPC has 120+ Members
- Digital Education Working Group (DEWG)
- DEWG Task Force on E-Learning Platforms
- Global Privacy Enforcement Network (GPEN) “Sweep”
- Common Thread Network

Digital Education Working Group (DEWG)



- ICDPPC subgroup
- Led by Privacy Commissioners of Canada and France
- Recent research / collaboration activities:
 - competency framework
 - train the trainers
 - youth consent
 - e-learning platforms
 - learning analytics*
- DEWG Task Force on E-learning platforms

DEWG Task Force (Jan-Oct 2018)

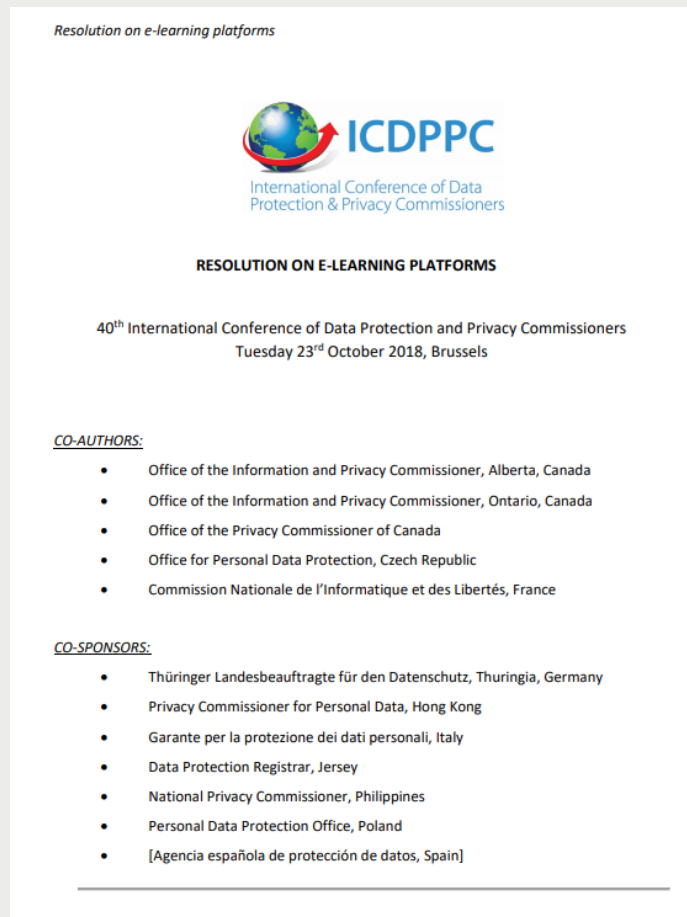


Mandate:

- review “e-learning platform” privacy issues
- develop resolution with recommendations
 - targeted at each stakeholder
 - plain language
 - actionable
 - implementation guidance

Co-chaired by IPC and OPC

ICDPPC Resolution on e-Learning Platforms



Source: <https://bit.ly/2RiXV5X>

Approved by ICDPPC Members Oct/18

- 24 recommendations for
 - educational authorities
 - e-learning platform providers
 - data protection authorities
- 24-page annex contains
 - complementary / explanatory notes
 - suggestions to assist Members with implementation

Notable Issues

What is an “e-learning platform”?

Who are “educational authorities”?

Issue #1: Organizational Capability and Readiness

Issue #2: Transparency and Notice

Issue #3: Consent and Opt-Out

Issue #4: Secondary Purposes and Uses

Issue #5: Use of Personal Devices

Resolution on e-Learning Platforms

Issue #1: Organizational Capability and Readiness

- 1(b) “**Develop policies and procedures** to evaluate, approve and support the use of e-learning platforms and, where feasible or required, conduct ... privacy impact assessments...”
- 1(c) “Provide **training and on-going support for educators**. Educators must be equipped with up-to-date, relevant and sufficient information on data protection and privacy rights to be able to implement effective e-learning platforms...”

Resolution on e-Learning Platforms

Issue #1: Organizational Capability and Readiness

Discussion:

- How capable and ready are educational authorities to engage online educational services and to ensure compliance with applicable laws and internal policies?
- Are PIAs feasible or are there other methods of evaluation and risk management?
- What resources, training and support do teachers need?

Resolution on e-Learning Platforms

Issue #2: Transparency and Notice

2(d) “**Before** collecting personal data, **notify** individuals about the personal data to be processed by the e-learning platform and the **reasons for processing**. The notice should be provided in a **timely, age-appropriate, clear and concise** fashion... More detailed information should be easily **accessible**. The notice needs to enable individuals to **make informed decisions**. Further, notices should **explain uses and disclosures to third parties**, the **risks of harm** arising from processing personal data, a **summary of protections and assurances** in place, and an **account of existing privacy rights and options available**”

Resolution on e-Learning Platforms

Issue #2: Transparency and Notice

Discussion:

- What notices should be provided to parents and students above and beyond MFIPPA?
- Who should provide the notices – school or online educational services provider?

Resolution on e-Learning Platforms

Issue #3: Consent and Opt-Out

1(e) “Where required or appropriate, seek **valid, informed** and **meaningful consent** from individuals. The **legal basis** for the processing of student data by an e-learning platform commissioned by an educational institution should be determined by law or rules established by competent regulatory authorities, wherever available. If no such legal basis is available, parental consent, student consent or both, as appropriate, must be obtained. The validity of this consent presumes that its **withholding leads to no disadvantage** of the student compared to their consenting peers. The decision, at any time, to **opt out or withdraw consent** should allow individuals to opt out of all or some of the data processing, if practical.”

Resolution on e-Learning Platforms

Issue #3: Consent and Opt-Out

Discussion:

- When is student or parental consent needed under MFIPPA?
- Who collects consent – educational-tech providers or schools / boards?
- When can students / parents / guardians opt out?

Resolution on e-Learning Platforms

Issue #4: Secondary Purposes and Uses

2(b) Make sure that the **purposes** for which personal data are being collected, processed and used are **legitimate**, suited to the context and **authorized** by law. All **collection** of student data should be **limited** to what is needed for educational purposes. By default, no other use of this data should take place, including for **commercial or marketing purposes**. Student data must **never be repurposed or used for non-educational purposes** without freely given express consent, unless there is legislation allowing for re-purposing. Secondary processing should proceed with **de-identified data** whenever possible, including for statistical and research purposes.

Resolution on e-Learning Platforms

Issue #4: Secondary Purposes and Uses

Discussion:

- What secondary purposes and uses of student data may be authorized or (un)acceptable?
- What uses are typically “required” to provide a requested service
 - testing / quality control?
 - security / fraud prevention?
 - statistical reporting / analytics?
 - profiling / personalization?
 - marketing / advertising?!
- Are there clear no-go zones?

Resolution on e-Learning Platforms

Issue #5: Use of Personal Devices

1(f) Consistent with domestic law, **implement a policy** for individuals who access the e-learning platform with their personal electronic devices. This policy should **clarify appropriate uses** of the e-learning platform and any consequences of using a personal device – especially when **installing software or mobile applications**.

Resolution on e-Learning Platforms

Issue #5: Use of Personal Devices

Discussion:

- What personal devices do schools allow (or encourage) students to access online educational services?
- What steps are taken to prevent excessive tracking or collection of student personal data beyond the school environment?
- If schools provide Wi-Fi connectivity, what personal information do their routers/networks collect?

Resolution on e-Learning Platforms

What is to be done?

1(d) Work with other educational authorities and, in cooperation with local data protection authorities, to **agree on common standards** for engaging e-learning platforms....

Discussion

- What obstacles exist to greater collaboration and consistency of practices among educational authorities?
- What standards are needed or even possible?
- How can privacy commissioners help?



HOW TO CONTACT US

Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

TDD/TTY: 416-325-7539

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965