Privacy in the Networked Classroom: Current Trends and Developments

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

OASBO Annual General Meeting

Blue Mountain

9 May 2019

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 Mission and Mandate

MISSION:

We champion and uphold the public's right to know and right to privacy

MANDATE:

- Resolve access to information appeals and privacy complaints
- Review and approve information practices
- Conduct research, deliver education and guidance on access and privacy issues
- Comment on proposed legislation, programs and practices

IPC Policy Department

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

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

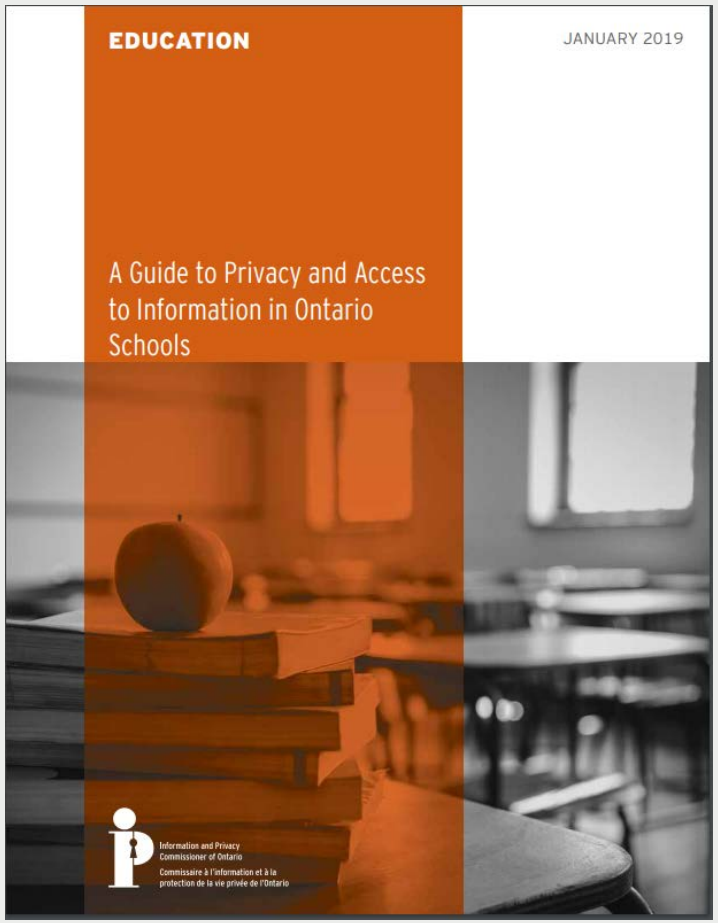
up to date

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

New IPC Guidance for Ontario Schools

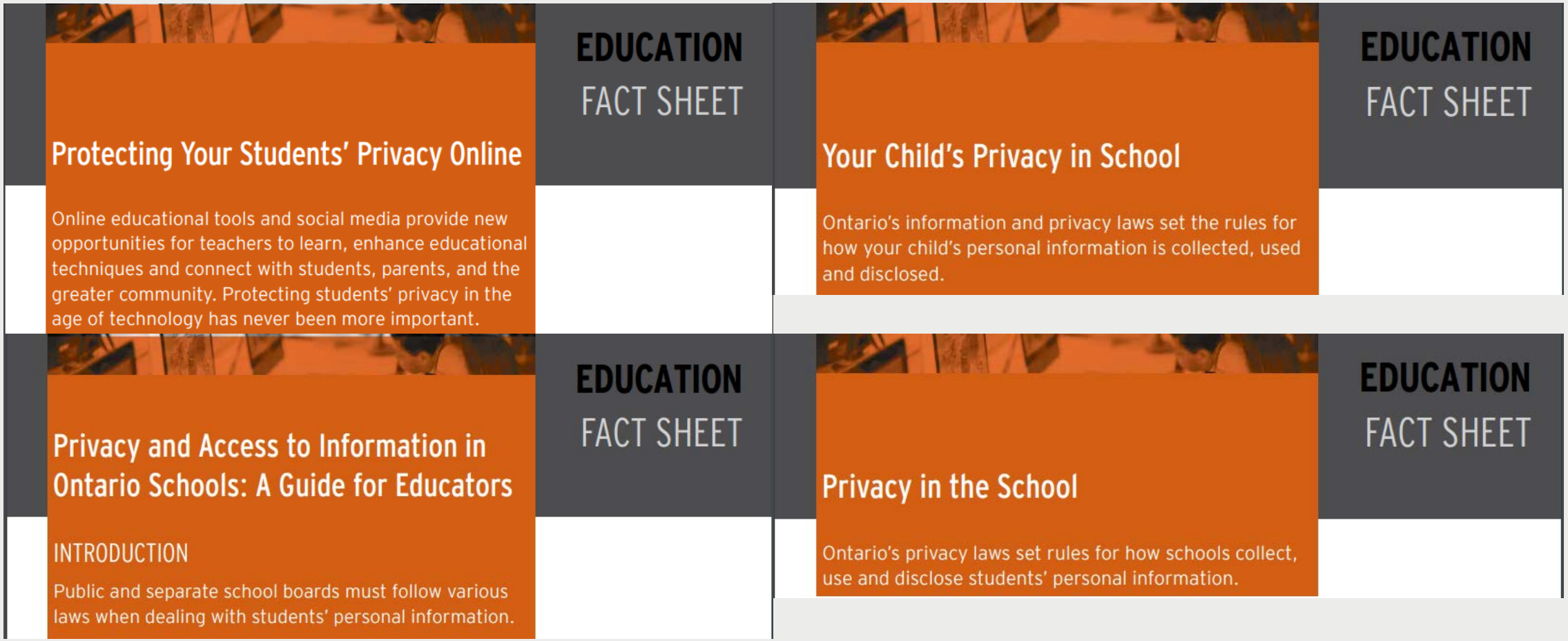


Source: https://bit.ly/2spVb7J

- 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.

New IPC Fact Sheets



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

International Collaboration

- ICDPPC has 120+ Members
- Digital Education Working Group (DEWG) (2013-present)
- DEWG Task Force on E-Learning Platforms (2018)
- 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

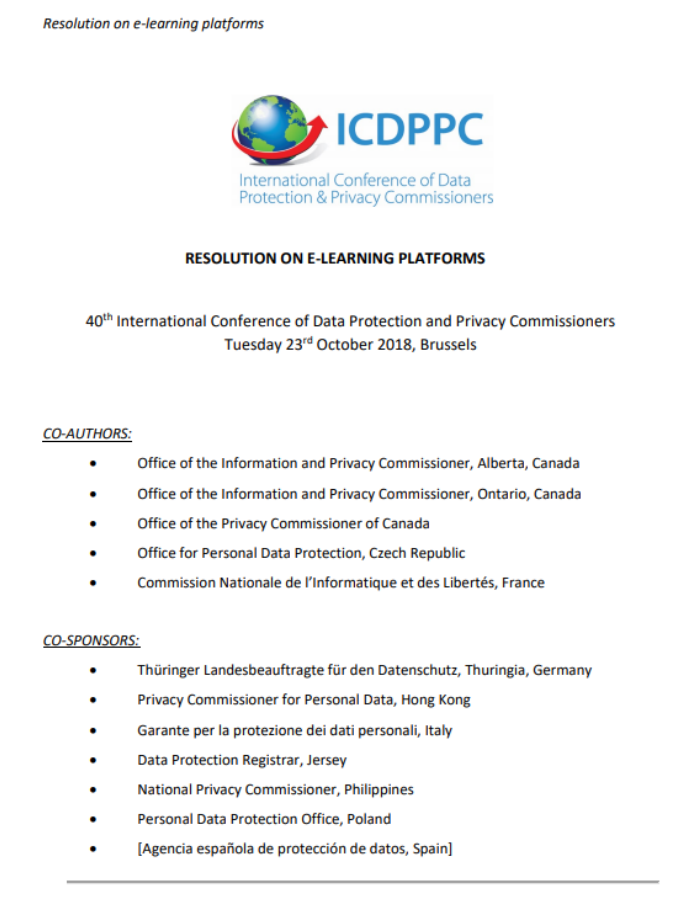
DEWG Task Force (Jan-Oct 2018)

Mandated to

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

Co-chaired by IPC and OPC

ICDPPC Resolution on e-Learning Platforms



Resolution on e-learning platforms

ICDPPC
International Conference of Data Protection & Privacy Commissioners

RESOLUTION ON E-LEARNING PLATFORMS

40th International Conference of Data Protection and Privacy Commissioners
Tuesday 23rd October 2018, Brussels

CO-AUTHORS:

- Office of the Information and Privacy Commissioner, Alberta, Canada
- Office of the Information and Privacy Commissioner, Ontario, Canada
- Office of the Privacy Commissioner of Canada
- Office for Personal Data Protection, Czech Republic
- Commission Nationale de l'Informatique et des Libertés, France

CO-SPONSORS:

- Thüringer Landesbeauftragte für den Datenschutz, Thuringia, Germany
- Privacy Commissioner for Personal Data, Hong Kong
- Garante per la protezione dei dati personali, Italy
- Data Protection Registrar, Jersey
- National Privacy Commissioner, Philippines
- Personal Data Protection Office, Poland
- [Agencia española de protección de datos, Spain]

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

Agreed 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 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 - ed 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 wifi 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 off practices among educational authorities?
- What standards are needed or even possible?
- How can privacy commissioners help?


QUESTIONS
PRIVACY
???
&5DF?W$
SYBASE
IP
LOGIN
ORACLE
SSL
105254
28

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

Overview

IPC and MFIPPA

New IPC Guidance

Digital Literacy / Citizenship

Online Educational Services