

The IPC, Privacy and Education in the Digital Age

Brian Beamish - Commissioner

Renee Barrette – Director of Policy

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

TDSB Unleashing
Learning 2018

April 3, 2018

Our Office

- Information and Privacy Commissioner (IPC) provides **independent** review of government decisions and practices on access and privacy
- Commissioner appointed by, reports to the Legislative Assembly, to ensure **impartiality**

What We Do

- Provide an **independent** review of provincial and municipal government and public sector decisions and practices concerning access and privacy
- Oversee **compliance** with provincial and municipal access and privacy legislation
- Conduct **research** and deliver **education** and **guidance** on access and privacy issues

IPC's Mandate

- *Freedom of Information and Protection of Privacy Act (FIPPA)*
- *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*
- *Personal Health Information Protection Act (PHIPA)*
- Expanded Mandate:
 - *Child Youth and Family Services Act*
 - *Anti-Racism Act*

MFIPPA

The purposes of *MFIPPA* are:

- To provide a **right of access to information** under the control of institutions in accordance with the principles that
 - information should be available to the public
 - access exemptions should be limited and specific
 - access decisions should be reviewed independently of government
- To **protect the privacy of individuals** with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information

Institutions

- *MFIPPA* applies to **“institutions”** regarding the general records and records of personal information in their custody and control
- Institutions under *MFIPPA* include **school boards**
- School boards remain responsible for the information practices of their educators and **third party service providers**



Access Basics

Access Rights

- *MFIPPA* gives every person a **right** to access a record or part of a record in the **custody or under the control** of an institution unless:
 - contents fall within exemptions
 - the request is frivolous or vexatious
 - the record is specifically excluded or
 - another act overrides the legislation
- Right of access applies to **records** which is broadly defined to include:
 - correspondence, working notes (notebooks), photos,
 - expense accounts, videos, e-mails, appointment books and schedules,
 - draft documents, voicemails and texts

Exemptions: Limited and Specific

There are two separate categories of exemptions under Ontario's access laws:

1. mandatory exemption – Head of an institution **must** withhold the record
2. discretionary exemption – Head of an institution **may** choose to withhold the records

Discretionary Exemptions

- Record of closed meetings (*MFIPPA* only)
- Advice or recommendations
- Law enforcement
- Economic and other interests
- Solicitor-client privilege
- Danger to safety or health
- Species at risk (*FIPPA* only)
- Information soon to be published

Mandatory Exemptions

- Relations with other governments
- Cabinet records (*FIPPA* only)
- Third-party information
- Someone else's personal information

Access Requests

- Requests can be made by anyone, for any reason – no obligations on the requester to provide a reason for making the request
- Once an access request is received **all responsive records must be retained** – they cannot be altered, deleted or shredded
- Requesters who are not satisfied with the response they receive from the institution have a right to file an appeal with our office



Privacy Basics

Fair Information Practices

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

Privacy

- *MFIPPA* protects the **privacy** of individuals concerning their personal information, provides them with the **right to access** that information
- It includes rules for the **collection, use, disclosure** of personal information
- To qualify as **personal information** it must be reasonable to expect that an individual may be **identified** if the information is disclosed

Examples of Personal Information

- Race, national or ethnic origin, religion, age, sexual orientation or marital or family status
- Education or medical, criminal, employment history
- Identifying number, symbol or other particular assigned to the individual
- Address, phone number, fingerprints, blood type
- Individual's name, where it appears with other information about the individual

MFIPPA Privacy Rules

- Head is **accountable** for access decisions, privacy protection and annual reporting
- Individual has a right to know the principal **purposes** of CUD
- CUD **limited** by rules prohibiting CUD unless exceptions apply
- PI collected for one purpose can be used and disclosed for that purpose or a **consistent purpose**
- Cannot use PI unless it is **accurate and up-to-date**

MFIPPA Privacy Rules

- Requirement to ensure that PI is **safeguarded** against unauthorized uses and disclosures
- Requirement to be **open** by providing notice and maintaining PI bank
- Individuals have a right of **access and correction** to their own PI
- Individuals can **challenge compliance** by filing a complaint and under *M/FIPPA* Commissioner has the authority to **order** institution to:
 - cease a collection practice and destroy collections of PI
- Commissioner can also make **recommendations** regarding the privacy implications of a legislative scheme or program

Privacy Breach

- A privacy breach occurs when personal information is collected, retained, and used or disclosed in ways that are not in accordance with *MFIPPA*
- Among the most common breaches of personal privacy are:
 - sending communications to the wrong recipient due to human error
 - improper records destruction procedures
 - loss or theft of unsecured electronic devices, such as laptop computers, digital cameras, or portable storage devices (USB sticks)
 - unauthorized access (snooping, hacking)

IPC Privacy Investigations

The IPC may:

- receive privacy complaints from the public or investigate on its own accord
- investigate privacy complaints and report publicly on them
- order the institution to cease and destroy a collection of personal information
- make recommendations to safeguard privacy

Reducing Risk of Privacy Breaches Best Practices

Administrative	Technical	Physical
<ul style="list-style-type: none">• privacy and security policies• auditing compliance with rules• privacy and security training• data minimization• confidentiality agreements• Privacy Impact Assessments	<ul style="list-style-type: none">• strong authentication and access controls• detailed logging, auditing, monitoring• strong passwords, encryption• patch and change management• firewalls, anti-virus, anti-spam, anti-spyware• protection against malicious code• Threat Risk Assessments, ethical hacks	<ul style="list-style-type: none">• controlled access to premises• controlled access to locations within premises where PI is stored• access cards and keys• ID, screening, supervision of visitors <div data-bbox="1290 911 1858 1196" style="border: 1px solid black; padding: 5px;"><p>NOTE – when determining appropriate safeguards consider</p><ul style="list-style-type: none">• sensitivity and amount of information• number and nature of people with access to the information• threats and risks associated with the information</div>



Privacy – An Absolute?

Yes, You Can.

- Some professionals do not report suspicions about a child at risk of harm to a children's aid society (CAS) on the unfounded belief that “privacy” prevents them from doing so
- The Ontario Child Advocate and the Information and Privacy Commissioner of Ontario have developed a resource to clarify some common misunderstandings about privacy and the duty to report
- If a person has **reasonable** grounds to suspect that a child is in need of protection, the person **must** immediately report the suspicion and the information on which it is based to a CAS
- The **duty** applies to any person, including a person who performs professional or official duties with respect to children

Yes, you can share
information with a
Children's Aid Society to
protect a child.

YES,

YOU

CAN.

**DISPELLING THE MYTHS ABOUT
SHARING INFORMATION WITH
CHILDREN'S AID SOCIETIES.**

Find out more at www.ipc.on.ca

 Information and Privacy
Commissioner of Ontario

Provincial Advocate
for Children & Youth

The Philadelphia Model

- Annual meeting of advocates and representatives from the Women’s Law Project who search through police sexual assault files — alongside high-ranking officers — to look for deficiencies and biases
- Since it was implemented 17 years ago, the “unfounded rape” rate has dropped to four per cent, in contrast with the national average of seven per cent



UNFOUNDED
**WHY POLICE DISMISS
1 IN 5 SEXUAL
ASSAULT CLAIMS AS
BASELESS**

Globe and Mail Series:
“Unfounded”

Working with Police on an Ontario-based Philadelphia Model

- Identify external partners with the experience to assist with the review of sexual assault files and appoint them agents
- Ensure external reviewers have been subject to a background check, signed an oath of confidentiality and received privacy and confidentiality training
- Require external reviewers to see names of principals so they can recuse themselves if needed
- Permit external reviewers to review complete closed files, subject only to redactions or restrictions required by law
- Ensure reviews take place at police facilities and no identifying information is copied, retained or removed by agents

MOU For Use By Ontario Police

- IPC worked with police to develop a model Memorandum of Understanding and Confidentiality Agreement
- Used to set the terms for the review of sexual assault cases by police and external reviewers
- Kingston Police are the first to put into practice

MEMORANDUM OF UNDERSTANDING respecting the External Sexual Assault Case Review Program made this 1st day of November, 2017 (the "Effective Date").

BETWEEN:

SEXUAL ASSAULT CENTRE KINGSTON
(Hereinafter referred to as "SACK")

-AND-

PAMELA CROSS, BA, LLB
(Hereinafter referred to as "Pamela Cross")

-AND-

OTTAWA RAPE CRISIS CENTRE
(Hereinafter referred to as "ORCC")

COLLECTIVELY REFERRED TO AS THE "KINGSTON VAW ADVOCACY GROUPS"

-AND-

KINGSTON POLICE
(Hereinafter referred to as "Kingston Police")

COLLECTIVELY REFERRED TO AS THE "PARTIES"

WHEREAS the Kingston Police as a municipal police service are governed by the *Police Services Act*, R.S.O. 1990, c. P. 15 (*PSA*) and the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M. 56 (*MFIPPA*);

WHEREAS, under section 1 of the *PSA*, police services shall be provided in accordance with principles, including the need for co-operation between the providers of police services and the communities they serve; the importance of respect for victims of crime and understanding of their needs; the need for sensitivity to the pluralistic, multiracial and multicultural character of Ontario society; and the need to ensure that police forces are representative of the communities they serve;

WHEREAS, under section 4(2) of the *PSA*, core police services include crime prevention, law enforcement, and providing assistance to victims of crime;

WHEREAS, under section 41(1) of the *PSA*, the duties of the Chief of the Kingston Police include ensuring that the Kingston Police provide community-oriented police services and that its members carry out their duties in a manner that reflects the needs of the community;

WHEREAS the duties and functions of the Kingston Police include investigating reports of sexual assault and supervising and monitoring those investigations, including for the purpose of identifying deficiencies, errors and anomalies in and improving the efficiency of individual sexual assault investigations and the sexual assault investigative process as a whole;



Access and Privacy in the Education Sector

Access and Privacy Education at the IPC

*What Students Need to Know
about Freedom of Information
and Protection of Privacy*



A Study Guide for Elementary Schools
Grade 5 Teacher's Guide
September 2005

Educational Resources for Youth

- IPC worked with frontline teachers
- Created tools / resources on access & privacy issues for use in teaching plans
- Based on Ontario Ministry of Education curriculum policy
- Three study guides produced for grades 5, 10 and 11/12
- School boards distributed the guides to teachers

Access and Privacy Education at the IPC

Educational Resources: Approach Taken

- Separate materials developed based on age group
- Variety of learning tools, including:
 - Powerpoint presentations
 - Online research activities:
 - “webquests”
 - Quizzes
 - Quick reference infographics
 - Group discussion aids
 - Case studies
 - Privacy in the news

YOU, ONLINE

Personal Branding and Online Privacy:
A Primer
(Appendix 3.1)

This PowerPoint presentation is on the accompanying CD.

The image displays a grid of 11 PowerPoint slides from the 'YOU, ONLINE' presentation. The slides are arranged in three rows:

- Row 1:**
 - Slide 1: Title slide 'YOU, ONLINE: Personal Branding and Online Privacy: A Primer'.
 - Slide 2: 'ONLINE PRIVACY: WHY DOES IT MATTER?' with bullet points: 'Online postings, by you or others, can take control of your brand out of your hands', 'Wide audience', 'Long-lasting', 'Able to be viewed, copied, downloaded, reposted by virtually anyone', 'Predators, Parents, Professors, Prospective Employers, Police'.
 - Slide 3: 'WHAT'S IN A BRAND?' with a word cloud including: TIMELESS, Professional, TRUSTWORTHY, Eco-friendly, ELITE, Playful, Traditional, Cool, Reliable, Innovative, Cutting-edge, Elegant, MODERN.
- Row 2:**
 - Slide 4: 'YOUR PERSONAL BRAND' with text: 'What you say + What you do + What others say about you = Your Reputation'.
 - Slide 5: 'FREE YOUR HANDS' with an image of a hand holding a smartphone and a laptop.
 - Slide 6: 'FREE YOUR HANDS' with an image of a hand holding a smartphone and a laptop.
- Row 3:**
 - Slide 7: 'MEMBERS STAY ON THE LOOP' with an image of a group of people.
 - Slide 8: 'YOUR PERSONAL BRAND' with an image of a hand holding a smartphone and a laptop.
 - Slide 9: 'PRIVACY: PROTECT IT, RESPECT IT' with bullet points: 'Protect: Adjust your privacy settings; Use a pseudonym or post anonymously where appropriate; Control private details.'; 'Respect: Don't post compromising photos of others; Ask before you tag; Don't post intimate details on walls or other applications.'; 'THINK BEFORE YOU POST!'.

International Partnerships

International Resolution on Privacy Education

- IPC is a signatory to the 2016 Resolution for the Adoption of an International Competency Framework on Privacy Education
- To meet our commitment to digital education promotion, IPC consulted with the Ministry of Education
- We were pleased to find that all elements of the International Competency Framework on Privacy Education have been integrated into the existing curriculum for Ontario's students
- In addition, specific requirements for privacy and digital education are present in numerous courses and at all grade levels

ICDPPC Resolution: <https://icdppc.org/wp-content/uploads/2015/02/Resolution-2016-on-Privacy-education.pdf>

National Partnerships

FPT Working Group on Youth Education

- Ontario is working with IPCs across the country to develop lesson plans for youth on a variety of privacy matters, including:
 - digital economy and personal information
 - permanence of online information
 - rights and responsibilities for online privacy
 - understanding online privacy policies / terms and conditions

National Partnerships

FPT WG Joint Letter to Council of Education Ministers (Nov 2017)

- Annual Media Literacy Week, which takes place every November, highlights the importance of teaching children and teens digital and media literacy skills
- Open letter calls for privacy education to become a “clear and concrete component in digital literacy curricula across the country”
- Letter notes that:
 - online risks are growing (cyberbullying, sexting and child luring, tracking, hacking and email scams)
 - personal information has become a hot commodity as businesses seek to monetize our data
 - everyone, regardless of age, must weigh benefits and risks of each product and service they use, each time they use it

The Canadian Teachers' Federation and the FPT

- A collaboration between Privacy Commissioners across Canada and the Canadian Teachers' Federation to raise awareness among youth about the importance of privacy protection
- The poster can also be used as a tool to support education about privacy in the online world

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. **POST**
- 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: Information and Privacy Commissioner of Ontario, Commission d'accès à l'information / Commission de l'accès à l'information du Québec, Office of the Information & Privacy Commissioner, Office of the Language Commissioner, Manitoba Ombudsman, Office of the Information & Privacy Commissioner of the Prince Edward Island, Office of the Information Commissioner and Privacy Commissioner, Office of the Information and Privacy Commissioner of Alberta, Office of the Information and Privacy Commissioner of British Columbia, Office of the Information and Privacy Commissioner of Saskatchewan, Office of the Information and Privacy Commissioner of Yukon, Office of the Information and Privacy Commissioner of Nunavut.

Office of the Privacy Commissioner of Canada

Find out more at youthprivacy.ca

Online Educational Tools and Services


- Growing use in Ontario classrooms
- Often used without knowledge or approval of school boards
- Under *MFIPPA*, school boards are responsible for information management practices of educators and service providers


Think Before You
CLICK

I accept all terms
and conditions

Could the
online education
tool you are using
expose your students
and school to privacy
risks?

**TALK TO YOUR
PRINCIPAL**

 Information and Privacy
Commissioner of Ontario
Commissionnaire à l'information et à la
protection de la vie privée de l'Ontario

 **OASBO**
ONTARIO ASSOCIATION OF
SCHOOL BOARDS OF ONTARIO

Online Educational Tools and Services

Privacy and Access Risks:

Improper Collection

- personal information of students, parents
- online activities, interactions with others

Unauthorized Use

- performance evaluations, learning profiles which may be used for marketing purposes

Unauthorized Disclosure

- sale of personal information to third parties for marketing purposes

Online Educational Services

What Educators Need to Know



Online Educational Tools and Services

Potential Consequences:

- breaches
- complaints
- IPC investigations
- public reports
- notification requirements
- disciplinary procedures
- reputational impacts
- financial impacts

Online Educational Services

What Educators Need to Know

<http://www.>





2017 GPEN “Sweep”

- GPEN established to foster cooperation among privacy regulators
- Annual GPEN “Sweep” is a coordinated review of the privacy risks of websites and mobile applications
- 2017 Sweep theme: “User Control over Personal Information”
- IPC collaborated with Office of Privacy Commissioner of Canada to review free online educational services in use across Ontario
- Goal to identify potential areas of concern to guide future awareness and outreach efforts

2017 GPEN Report

Lessons Learned:

- Privacy policies and terms of service were often lengthy, challenging to understand
- Collection and disclosure of student personal information could occur via mobile apps, social login, and browser tracking cookies
- Two-thirds of online services did not have a clear policy on deleting dormant or inactive accounts

2017 GPEN Sweep Report Online Educational Services



2017 GPEN Report Recommendations

Best Privacy Protection Practices for School Boards and Educators:

- Consult before selecting online services
- Understand privacy policies and terms of service
- Minimize identifiability of students
- Seek involvement of parents & guardians
- Provide guidance to students on appropriate uses



Questions?

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