JANUARY 2019

EDUCATION
FACT SHEET

Privacy and Access to Information in Ontario Schools: A Guide for Educators

INTRODUCTION

Public and separate school boards must follow various laws when dealing with students' personal information.

The Information and Privacy Commissioner of Ontario (IPC) oversees the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*). This law sets out rules that schools and school boards must follow regarding the collection, retention, use, and disclosure of personal information.

RESPONSIBILITIES

Staff at all levels within Ontario's public and separate school system have a responsibility to ensure the personal information of students is secure and kept confidential.

Principals and school board officials are responsible for:

- complying with *MFIPPA*, the *Education Act*, and other laws related to the privacy of and access to students' personal information, along with relevant guidelines and policies
- collecting personal information only where permitted under the law
- implementing reasonable security measures to protect student personal information
- ensuring that staff are aware of and adequately trained in their responsibilities

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

- ensuring that agreements with service providers, such as photographers, contain provisions to protect the privacy and security of personal information.

Teachers and staff are responsible for:

- complying with legislation, professional standards, guidelines, and school board policies when collecting, retaining, using, and disclosing personal information
- protecting personal information by following school policies and procedures
- reporting any suspected privacy or security breaches to the principal
- participating in training regarding their duties and obligations to protect personal information.

PERSONAL INFORMATION

Ontario's privacy laws define personal information as ***"recorded information about an identifiable individual."*** This includes a person's name, address, sex, age, education or medical history.

Recorded information includes personal information recorded in any format, such as:

- paper records, such as report cards, class lists and printed special education records including individual education plans, safety plans or behaviour plans
- electronic records, such as student information systems, Ontario Student Records (OSRs) and electronic student attendance records
- photographs, including yearbook images
- video footage including from surveillance cameras located in schools, or from video recorded in the classroom or school

For additional information, review the IPC fact sheet ***What is Personal Information*?**

COLLECTION AND USE OF PERSONAL INFORMATION

Under Ontario's access and privacy laws, a school or school board may collect personal information from a parent, guardian or student if at least one of the following applies:

- the collection is specifically authorized (permitted) by a law such as the *Education Act* (e.g., collecting information for the OSR)
- the information is used for law enforcement purposes
- it is necessary to deliver educational services or other related activities

DISCLOSURE OF PERSONAL INFORMATION

A school or school board may disclose personal information in some situations:

a. **Consistent Purpose**

   For the reason it was collected or for a consistent purpose.

b. **With Consent**

   If they have the permission of the individual or their parent or guardian in the case of a minor.-

c. **Required by law**

   To comply with a law, for example, the duty to report to a children's aid society.

d. **Law Enforcement**

   To aid an investigation by an institution or law enforcement agency in Canada, such as the police.

e. **Health and Safety**

   In compelling circumstances affecting the health or safety of an individual, where the disclosure is reasonably likely to reduce the risk of harm.

You can disclose personal information

- where necessary to deliver education services
- where you are permitted or required to by law
- where the individual has consented

COLLECTION, USE, AND DISCLOSURE OF PERSONAL HEALTH INFORMATION

The *Personal Health Information Protection Act* (*PHIPA*) sets the rules for the collection, use and disclosure of students' personal health information. These rules apply to health information custodians and those working on their behalf. Health information custodians include:

- physicians, nurses, psychologists, speech-language pathologists, dental hygienists and social workers providing health care
- anyone who operates a group practice of health care practitioners
- a centre, program or service for community health or mental health whose primary purpose is the provision of health care

For additional information, review the IPC document, ***A Guide to the Personal Health Information Protection Act***.

STORAGE AND RETENTION OF PERSONAL INFORMATION

Schools must retain and destroy personal information records according to the rules outlined in the OSR Guideline (for OSR records), *MFIPPA*, and the record retention schedules set by the school board. They must securely destroy information that is no longer needed.

Review the IPC fact sheet, ***Disposing of Your Electronic Media*** for information on how to destroy electronic media.

PRIVACY BREACHES

If a school does not comply with the law when they manage personal information, privacy breaches can occur. Some examples of privacy breaches, and their causes, include:

- lost or stolen flash drives containing student or staff information
- correspondence mailed or emailed to the wrong person
- disclosing information about a student without consent or without legal authority

All employees are responsible for protecting students' information, regardless of their role. If they become aware of a privacy breach (or potential privacy breach), they must:

- inform their supervisor, manager or principal
- take immediate steps to contain the breach (e.g., changing security passwords or retrieving copies of documents that were shared in error)
- participate in any resulting investigation.

After becoming aware of a breach, principals and managers are responsible for taking steps to contain the breach, advising the appropriate superintendent and Freedom of Information Officer where required, and participating in any resulting investigation.

> **Best Practice for Responding to a Privacy Breach**
>
> If an employee becomes aware of a privacy breach, they must immediately notify their supervisor so that immediate action can be taken to lessen its impact.

Review the IPC document, ***Privacy Breach Protocol Guidelines for Government Organizations***, for more information.

BEST PRACTICES FOR PROTECTING PERSONAL INFORMATION

- Familiarize yourself with your workplace policies.
- Treat all information about students as personal information that deserves protection under the law.
- Avoid casual sharing of students' personal information, even with colleagues.
- Provide privacy and security training to all staff.
- Restrict access to those employees that need the records or information to do their job.
- Ensure that sensitive and confidential information is not visible to the public.
- Encourage a clean desk policy to reduce the risk of exposing confidential information.
- Lock office and classroom doors and filing cabinets when not in use.
- Label filing cabinets, drawers, boxes and other storage containers to indicate they contain confidential information.
- Keep filing equipment or mailboxes behind a counter or other physical barrier separate from the public.
- Make sure fax machines and printers are in a secure area, and retrieve sensitive documents right away.
- When faxing sensitive information, double-check the recipient's number before dialing, and confirm receipt.
- Carefully read the school board's record retention schedule to find out how long to retain—and how to securely destroy—personal information.
- Use locked shredding boxes for the secure destruction of paper records.
- Position computer screens to prevent unauthorized viewing.
- Do not disclose passwords.
- Seek advice and direction from the school administrator if you are unsure about anything to do with personal information of students.

PRIVACY IN THE NETWORKED CLASSROOM: THE USE OF ONLINE EDUCATIONAL SERVICES

Ontario teachers often use online educational tools and services in their classrooms, sometimes without the knowledge or approval of school administrators and school boards.

School boards are accountable for the use of these tools in the classroom. They must ensure that these services do not improperly collect, use or disclose students' personal information.

Given these privacy risks, the IPC recommends that schools and school boards considering the use of online educational services take the following steps:

1. Assign responsibility for making decisions on the use of online educational tools.
2. Develop and implement policies and procedures to evaluate, approve and support the use of online educational services for use in the classroom.
3. Develop a list of approved apps and services.
4. Provide privacy and security training and ongoing support for teachers and staff
5. Work with other educational stakeholders to develop common criteria for engaging online educational services.
6. Notify students and parents that the service may collect personal data and explain how the information will be used.
7. Allow students or parents to opt out of services that collect, use, retain or disclose personal data.
8. Develop and implement a "Bring Your Own Device" (BYOD) policy for students who access services with their personal electronic devices.
9. Set and enforce retention periods for accounts and different categories of personal data.

Review the IPC's ***2017 GPEN Sweep Report*** for more information about online educational services.

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