Freedom of Information and Protection of Privacy

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY

a primer for employees of Ontario Universities and Colleges

MARION HANSEN, FREEDOM OF INFORMATION AND PRIVACY COORDINATOR

CONTENTS

Freedom of Information and Protection of Privacy

About the employee orientation

Who should take the employee orientation?

Regardless of your position, you need to understand your responsibilities with respect to access to information and the protection of privacy.

What does the orientation include?

- Part 1 – Privacy & Personal Information
- Part 2 – Disclosing Personal Information
- Part 3 – Privacy Breach Prevention & Response
- Part 4 – Records Management
- Part 5 – Your Working Environment
- Part 6 – Freedom of Information Requests

This training, including the quiz at the end, should take approximately 30 minutes.

How do I get started?

To get started, simply click here:

- Part 1 – Privacy & Personal Information

MODULES

PART 1 – PRIVACY & PERSONAL INFORMATION

All Ontario Universities and Colleges are responsible to fulfill the requirements of the Freedom of Information and Protection of Privacy Act (FIPPA for short).

- FIPPA was enacted to ensure that Ontario's publicly funded institutions are transparent and accountable to the people of Ontario through access to information and the protection of privacy
- FIPPA is enforced through the office of the Information and Privacy Commissioner of Ontario (IPC)

Two Key Principles of FIPPA:

Public access to information

- The public has a right to request records that the institution has in its custody or under its control.

The protection of personal privacy

- The institution has a responsibility to protect personal information and other kinds of sensitive records from unauthorized uses and disclosures.

A couple key points about FIPPA

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://ecampusontario.pressbooks.pub/fippaprimer/?p=22#h5p-1

An Institutional Record means any record:

- in the custody or under the control of the institution;
- created or received, and maintained as evidence of institutional decisions, transactions, and relationships; and,
- relevant to the administration and operation of institutional activities.

What is a Record?

An interactive H5P element has been excluded from this version of the text. You can view it online

here:
https://ecampusontario.pressbooks.pub/fippaprimer/?p=22#h5p-2

What is considered Personal Information?

- FIPPA defines Personal Information as information about an identifiable individual
- This includes, but is not limited to, such basic details as name, address, telephone number, gender, age and marital status, employee number, student number, health information, education and employment history, and financial data
- An individual's name on its own is not personal information unless it discloses other information, which if unauthorized, would be an invasion of privacy
- Personal Information does not include the name, title, business address, and business contact numbers of an employee

Key Points

- **Personal information is any information about an identifiable individual** (except employees' names and work contact details)
    - The names of students are personal information as they identify the individual as a student of the institution.

- **Record:** A record is any record of information however recorded, whether in printed form, on film, by electronic means or otherwise
- **FIPPA's rules** for the protection of personal information include:
    - Collect only the Personal Information (PI) that you need for the proper administration of the institution;
    - Inform people about the collection and about what you intend to do with their PI by including a Collection Notice whenever you collect PI;
    - Only use PI for the purpose(s) for which it was collected, or a consistent purpose;
    - Only share PI internally with other institutional employees if they need to know the information for the purpose of their role;
    - Don't disclose PI outside of the institution without consent, other than in limited circumstances as specified in FIPPA; and
    - Retain PI for a minimum of 1 year past last date of use.
- **Privacy breaches** must be reported to the institutional privacy office
    - Be mindful of privacy when handling records containing PI
- **Email:** Use institutional email address for all institution emails

Learn More

Institutions may have a policy detailing:

- Access to Information and Protection of Privacy

Check Your Understanding

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://ecampusontario.pressbooks.pub/fippaprimer/?p=22#h5p-3

What if I'm dealing with Personal Health Information?

Generally, even if you are handling records containing health information, FIPPA will continue to apply. The Personal Health Information Protection Act (PHIPA) only applies to the institution's units/departments that provide health care on the institution's behalf. Institutions will have health care providers who act as Health Information Custodians within the context of PHIPA, and may include the following:

- Student Health Services
- Personal Counselling Services

Employees of one of the above units should complete PHIPA Training.

Collection Notice Requirements

An institution must inform the individual to whom the information relates that a personal information collection has occurred. Whenever possible, the notice should be provided to an individual at the time of collection, or included on program forms and communications.

The notice to the individual must state:

- The legal authority for the collection;
- The principal purpose or purposes for which the personal information is intended to be used; and
- The title and business contact information of an official of the institution who can answer the individual's questions about the collection.

Notice must be provided each time there is a collection. The notice should address separate legal authorities or collections if a form is used for multiple purposes.

Example

Brock University's Collection Notice Template:

Brock University protects your privacy and your Personal Information. The Personal Information requested on this form is collected under the authority of *The Brock University Act, 1964*, and in accordance with the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). The information will be used to [specify purpose for collecting the Personal Information]. Direct any questions about this collection to the [contact position], of the [your department] at Brock University at (905) 688-5550, ext. [XXXX] or see www.brocku.ca/[your departmental website].

Click here for the next module: Part 2 – Disclosing Personal Information

PART 2 – DISCLOSING PERSONAL INFORMATION

When is it appropriate to share Personal Information (PI)?

Sharing PI – INTERNALLY

Sharing PI internally:

- You should only disclose PI to a fellow employee if they need the information in the performance of their duties.

Share PI – EXTERNALLY in Limited Circumstances (as permitted by FIPPA)

Personal information can be shared externally:

- For the purpose collected
- With the consent of the individual to whom it relates
- Compelling circumstances affecting health and safety
- Other limited circumstances (e.g. law enforcement proceedings)

While it is important to recognize that personal information is protected by Ontario's privacy and access laws, it is also important to realize that these protections are not intended to stand

in the way of the disclosure of vital – and in some cases, life-saving- information in emergency or other urgent situations.

Compassionate Circumstances – In situations calling for compassion, when there is a need to notify the spouse, close relative, or a friend about an individual who is injured, ill or deceased, you may disclose personal information without consent in order to facilitate this contact. FIPPA allows this discretionary disclosure, as permitted under FIPPA section 42(1)(i).

FIPPA requires we must notify the individual to whom the information relates, if it is practicable to do so. (i.e., mail to last known address).

Key Points

Only disclose the minimum amount of personal information necessary to achieve the University's or College's objectives:

- Limit what you share to what is needed.
- Disclosure to a fellow employee is on a "need to know" basis.
- Disclosure outside of the institution to third parties is generally only permitted with consent.
- Confirm consent in advance where possible.
- Personal information must be protected with reasonable security arrangements.
- De-identify if generic inquiry. (Do not automatically blanket copy / forward entire email.)
- Use secure institution-endorsed services to share PI, such as Workday or SharePoint.
- Avoid using your institutional email to share sensitive information (e.g., SIN#) unless the information is encrypted — and don't use your personal email account for institutional business!
- In emergency situations, FIPPA may permit the institution to disclose a student's personal information, including information about their mental health, or other health conditions, to parents or others who may be able to help in a crisis.

Where the individual has consented to the disclosure

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://ecampusontario.pressbooks.pub/fippaprimer/?p=25#h5p-4

If you need consent to share personal information outside of the institution, there are consent templates for this purpose. Generally, it is the institution's preference to release directly to the individual and the individual can then share their own information as needed.

Learn More

Institutions may have policies detailing:

- Use and Disclosure of Personal Information
- Use of Personal Information for Fundraising
- Protecting Students Health Privacy
- Best Practices for Security Measures for Protecting Personal Information

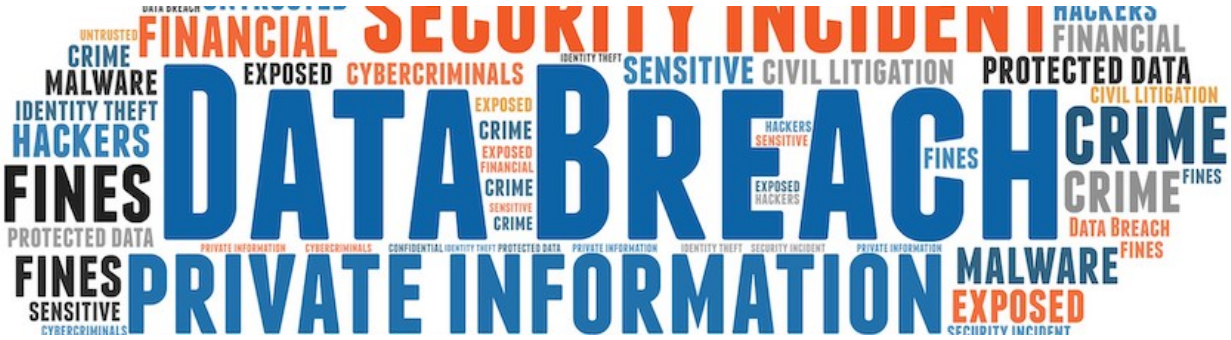
---

Check Your Understanding

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://ecampusontario.pressbooks.pub/fippaprimer/?p=25#h5p-5

Click here for the next module: Part 3 – Privacy Breach Prevention & Response

PART 3 – PRIVACY BREACH PREVENTION & RESPONSE



What is a privacy breach?

- A privacy breach occurs when personal information (PI) is disclosed in contravention of the FIPPA.

Examples of real breaches:

- Lost or misplaced information (e.g., lost laptop)
- Stolen information (through hacking or physical theft)
- Unauthorized use (including viewing) or disclosure of information, whether accidentally or deliberately

---

Key Point

All Institutions will have policies detailing the following: faculty, staff, contractors and volunteers have a duty to report suspected privacy breaches to their supervisor or manager, who will then initiate an investigation by reporting it to the Privacy Office.

When you suspect a privacy breach

What do you do?

Immediately inform:

- Your supervisor
- Privacy Office

What does the institution do?

- Contains the breach
- Determines the severity of the breach
- Investigates the cause of the breach
- Notifies the appropriate people
- Implements any recommendations to prevent another breach

A privacy breach may cause substantial personal harm to the affected individuals and may also result in financial and reputational harm to the institution. So when you handle any Personal Information remember to do so appropriately.

If information is released or accessed without consent and when the disclosure is not permitted by FIPPA, this is considered a breach.

Tips to prevent a privacy breach

—

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://ecampusontario.pressbooks.pub/fippaprimer/?p=28#h5p-6

Learn More

Institutions may have policies detailing:

- Privacy Breach Notification
- Breach Form
- IT Encryption Tools

Check Your Understanding

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://ecampusontario.pressbooks.pub/fippaprimer/?p=28#h5p-7

Click here for the next module: Part 4 – Records Management

PART 4 – RECORDS MANAGEMENT

What is an Institutional Record?

An institutional record is **evidence of work activity, capturing decisions made and actions taken**, which exist in any formats (paper and digital information/data).

As an example, Brock's Records Policy uses the following definition:

University Record means any record:

- in the custody or under the control of the University,
- created or received, and maintained as evidence of University decisions, transactions, and relationships; and,
- relevant to the administration and operation of University activities.
- The Freedom of Information and Protection of Privacy Act (FIPPA), Section 2, defines a record as "any record of information, however recorded", and then gives many possible examples of types of records

What is NOT an Institutional Record?

Research records created by faculty does not fall under the definition of a University Record. Records related to activities planned and implemented by student run groups also do not constitute University Records. In addition, **Transitory Records** are not considered institutional records. These are records that are generated in the day-to-day work of staff.

Transitory records have a temporary utility and are not required for statutory, legal, fiscal, administrative, operational, or archival purposes. Despite their short-term value they may contain sensitive and confidential or

personal information and should be disposed of in a secure manner. Electronic formats should be permanently deleted, while paper should be shredded.

Examples of transitory records include:

- Convenience copies retained for reference (e.g., digital copies of the official record in paper form and filed as the official record; "cc," "bcc," or FYI copies.
- Copies of records retained when the original or primary record has been sent to another unit.
- Routine emails to schedule or confirm meetings or events
- Announcements and notices of a general nature

Where to store records?

Wherever possible, institutional records should be stored in secure locations, such as:

- Shared drive
- SharePoint
- Other departmental applications (such as Workday, etc.)

Records stored in temporary storage locations should be transferred to these secure locations as soon as possible. Temporary storage locations include:

- Laptop hard drive
- Removable media (USB sticks)
- OneDrive (good intermediate step)
- Microsoft Teams
- Paper records

These locations are not suitable for the long-term keeping of records as they are not readily accessible to other employees who may have a legitimate need to access them. Additionally, there are no controls or safeguards to these documents.

Key Points

- Check the University or College's records retention schedule for information on how long to keep records
- Have reasonable measures in place to preserve records
- Store final versions of documents in an institutional system (e.g., SharePoint)
- Dispose of records securely

Records Retention

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://ecampusontario.pressbooks.pub/fippaprimer/?p=31#h5p-8

Learn More...

Institutions may have policies detailing:

- Records Management Policy

- Records Retention Schedule
- Disposition Procedure & Forms

Check Your Understanding

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://ecampusontario.pressbooks.pub/fippaprimer/?p=31#h5p-9

Click here for the next module: Part 5 – Your Working Environment

PART 5 – YOUR WORKING ENVIRONMENT

While working in the office, or remotely/from home, employees should remember that the documents and other information they create and use in their work are institutional records.

You must still follow the institution's Access to Information and Protection of Privacy Policy and its supporting Procedures[1] as you create, use, store and manage institutional records at home. This applies to all institutional records including those containing personal information.

More about records and working from home

If you won the lottery...

- What records and information would your replacement and your colleagues need to continue your work?
    - Would they be able to access your files and information?
    - Would they be able to find your files and information?
- Best Practice: keep institutional records in an appropriate shared repository
    - When convenient (Monthly? Weekly?), systematically transfer Records to a shared storage location

1. e.g.https://brocku.ca/university-secretariat/fippa/

Example:

- You get emails to institutional email that have important information in them.
- If you won the lottery, your team wouldn't know what is in these emails, or even that these emails existed.

Suggestion:

Once a week, transfer these emails to (for example) a team SharePoint site, and file them in a way that makes it easy to find them.

- Name the file something that indicates what the email is about
- Be sure to store attachments separately

*Alternative idea: transfer important emails to a shared email account, and make folders in Outlook to sort emails.

Example:

You create or receive files (pdfs, word docs, presentations, or anything else) that need to be kept. These are stored on your computer, then uploaded to OneDrive. Your team doesn't have access to your OneDrive, or even know that the files are there.

Suggestion:

Set up a regular schedule to transfer your files to shared storage such as Shared drive, or SharePoint. Some departments might have a system that has document storage, or a different shared storage location that is appropriate.

- Name the file something that clearly indicates what the file is about
- Include dates at the end of the file so the latest version can be found easily
    - Use the format YYYY MM DD (i.e. 2022 12 08) so that all files with the same name fall chronologically
- Have a folder structure that will make it easy for someone else to find the right file.

Key Points

Minimize the amount of paper records you create to save having to dispose of them while working from home or remotely. Even hand-written notes concerning your work, or preliminary versions of documents which you might normally print for proof-reading, are confidential institutional records requiring secure storage and secure destruction when you no longer need them.

- Don't leave devices unattended in public places
- Don't use public computers to access Personal Information
- Personal information stored on mobile devices must be encrypted
- Have reasonable measures in place to preserve records
- Find a quiet & secure location to limit unintended access to PI (e.g., close door, wear earbuds)
- Use your work email account for work related emails

Learn More

Institutions may have policies detailing:

- Access to Information and Privacy
- Records Management

Check Your Understanding

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://ecampusontario.pressbooks.pub/fippaprimer/?p=34#h5p-10

Click here for the next module: Part 6 – Freedom of Information Requests

PART 6 – FREEDOM OF INFORMATION REQUESTS

The public has a right to request/access most records by making a Freedom of Information (FOI) request. Freedom of Information (FOI) requests may be filed for any records produced in the course of your work at the institution, including records stored in personal use systems. Examples of records are emails, letters, reports, notes, photographs, and audio and video recordings. If it relates to University business, it can be requested!

When a FOI request is filed, you are legally required to produce any requested records that are in the institution's custody or under its control. Time is of the essence, as FOI requests must be responded to under strictly legislated timelines.

The Privacy Office coordinates FOI requests, and is able to help you through the process.

Requests for information:

All FIPPA requests are to be submitted to and processed by the Freedom of Information and Privacy Office. If there is a request for information affecting records in your area, the request is processed by the Freedom of Information and Privacy Office.

The Freedom of Information and Privacy Office employee(s) will process all FIPPA requests, and may contact the unit/department in order to the meet FIPPA's requirements as follows:

- assist in locating records requested;
- determine if the requested record might contain personal information or third party information that affects the interests of someone other than the requester and, if so, allow the affected third party to make representations about the disclosure of this information;
- within 30 calendar days of receipt of a request, make records available, deny access or cite extraordinary circumstances resulting in a delay;
- give a written reason for denial; and
- inform the person being denied access of his or her right to appeal to the Information and Privacy Commissioner of Ontario (IPC) within 30 calendar days of receiving the institution's response.

Records excluded:

FIPPA applies to all records, regardless of medium, in the custody or control of the institution, except for the following records (subject to certain limitations):

- Private donations to Archives;
- Labour relations and employment related records;
- Research records; and
- Teaching materials.

Subject to certain limitations, the institution may withhold records that contain:

- Advice or recommendations of a institutional employee or consultant;
- Information where the disclosure could reasonably be expected to prejudice the economic interests or competitive position of the institution;
- Plans relating to the administration of the institution that have not yet been put into operation or made public;
- Third party information if supplied in confidence and where disclosure could prejudice the interests of a third party; and
- Personal Information about individuals other than the requester where disclosure would constitute an unjustified invasion of personal privacy.

Key Points

Knowing that most records are releasable under FIPPA if requested, here are some tips for excellent records:

- Keep records factual / objective / concise.
- Maintain professional tone – *always assume records will be released.*
- Minimize the amount of personal information included to what is strictly necessary

---

Learn More

Institutions may have policies detailing:

- Access to Information and Protection of Privacy Policy
- Access to University Records
- Making a Request for Information

Check Your Understanding

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://ecampusontario.pressbooks.pub/fippaprimer/?p=37#h5p-11

Click here to access the Final Quiz.

FINAL QUIZ

Quiz Introduction

Here is how it works:

- All of the answers are included in the presentation. Feel free to backtrack through the presentation before selecting your answer.
- Your user identity and answers are anonymous.
- When you are ready to start the quiz click on the “Next” arrow below.

FINAL QUIZ

Final Quiz

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://ecampusontario.pressbooks.pub/fippaprimer/?p=121#h5p-13