

Frequently Asked Questions and Answers Regarding Personal Information



The Freedom of Information and Protection of Privacy Act (FIPPA) is provincial legislation that applies to Ontario Universities effective June 10, 2006. There are two fundamental principles to FIPPA:

1. Public access to information and,
2. The protection of personal privacy.

The above is to ensure that Ontario's publicly funded post-secondary institutions are transparent and accountable to the people of Ontario.

The following are answers to some Frequently Asked Questions regarding personal information.

Q1. What is Personal Information?

A. Personal Information means recorded information about an identifiable individual, including, but is not limited to such basic details as name, home addresses, telephone numbers, gender, age and marital or family status, race, national or ethnic origin, colour, religious or political affiliations, employee history, employee number, student number, health information, educational history, disabilities, blood type, financial history, criminal history, other persons' opinions about an individual, an individual's private views or opinions, and name, address and phone number of parent, guardian, spouse or next of kin.

Personal information does not include the name, title, business address, and business contact numbers of an employee. The personal information exemption expires for individuals deceased more than 30 years.

COLLECTION OF PERSONAL INFORMATION

Q1. How is personal information collected?

A. There is no restriction on how personal information is collected. All personal information collected must remain confidential.

Q2. Do I need to inform individuals that I'm collecting personal information about them?

A. Yes. Where an employee collects personal information on any individual (including faculty, staff, students and other community members) FIPPA requires us to notify that individual of the collection. That their personal information is necessary for the University to properly run programs or activities. This notification is called a Collection Notice.

Q3. What is included in a Collection Notice?

A. There are three parts to the Collection Notice which states:

- 1) *The Brock University Act* provides the legal authority to collect personal information.
- 2) The purpose for which the information is collected.
- 3) A contact in case the individual has questions about the collection of their personal information.

Here is the standard Collection Notice that can be copied and pasted to forms that are used to collect personal information, and originate from your department:

3<

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)* for the administration of the University and its programs and services. Direct any questions about this collection to the [contact title], of the [your department] at Brock University at (905) 688-5550, ext. [XXXX] or see [www.brocku.ca/\[your departmental website\]](http://www.brocku.ca/[your departmental website])

Q4. Where is the Collection Notice to appear?

- A.** According to FIPPA, a Collection Notice needs to be provided where personal information is collected. Below are some examples of where departments can place Collection Notices:
- a) Paper format: The Collection Notice need only appear on one page of a multiple paged document, usually appearing at the bottom of the last page.
 - b) Electronic format: The Collection Notice can be added to an electronic document where best suited. Research Support and Web Services can be of assistance with any modification needed to meet this FIPPA requirement, by calling ext. 4760 or emailing webdev@brocku.ca
 - c) Posters: Hang a Collection Notice poster where personal information is obtained (e.g. “front desk”). This quick reference is ideal for registration desks, and circulation desks.

You may have other ways of informing individuals that you are collecting personal information about them. This is fine providing the above three parts to the Collection Notice are satisfied.

Q5. Our department has a large supply of forms. What is the best method of adding the required Collection Notice to this supply of forms? Where do I add the Collection Notice if there is no space at the bottom of the form?

- A.** If your department currently has a large supply of forms for the purpose of collecting personal information, you can add the Collection Notice to the form(s) by either:
- a) Photocopying the Collection Notice on the back of the supply of forms, or
 - b) Copying and pasting the Collection Notice on to labels, and adhering the labels on to the forms.
 - c) Prepare a supply of photocopied Collection Notices and attach to the form being completed.

Please add the Collection Notice to a form before reprinting.

NOTE: The department where a form originated is the department who is responsible for adding the Collection Notice to future forms, as required.

USE OF PERSONAL INFORMATION

Q.1 Can I post or publish a photo of a student(s)?

- A.** Generally, a verbal consent to post or publish a photo, by the individual being photographed, will suffice. For those wishing to obtain a written consent, a “Photography Release Form” is available from University Communications for completion.

Q.2. Is there an access restriction regarding students’ personal information?

- A.** Employees of the University are permitted access to information contained in student records, if they need to know the information to perform their official duties. As a general rule, only employees involved in some aspect of academic administration or student affairs are given access to the contents of student records.

DISCLOSURE OF PERSONAL INFORMATION

Q1. Am I permitted to confirm the registration status of a current student, to someone other than a Brock employee or service provider?

- A.** No. Refer the requester to the Registrar’s Office, or Graduate Studies as appropriate.

Q2. Who is permitted to answer questions about degrees conferred?

- A.** Only the Registrar’s Office, or Graduate Studies as appropriate, are to disclose information about students who have graduated, which is considered to be public information, as follows:
- a) degree(s) obtained and the dates conferred by the University, and in most circumstances,
 - b) scholarships and the dates awarded.

Q3. What should I do if I am asked to provide information that I believe is protected under FIPPA?

- A.** If questioning whether or not you should be releasing certain personal information, contact Brock’s Freedom of Information and Privacy Coordinator at mhansen@brocku.ca or at extension 5380. To learn more about FIPPA, and the practices of the Freedom of Information and Privacy Office please visit the following website: www.brocku.ca/accessandprivacy/

- Q4. What do I tell a student who is asking that a correction be made to their student record?**
A. Refer the student to the Registrar's Office, or Graduate Studies as appropriate.
- Q.5 Our department is required to provide third parties (e.g. potential Co-op placement employers) with student's personal information (e.g. grades). What privacy practices apply?**
A. Personal information should only be disclosed when the individual to whom the information is about, is aware of the specific information to be disclosed. If there becomes a new use for personal information on file, that is not consistent with the original Collection Notice provided, you will need to obtain consent from the individual in order to use their personal information for a new purpose. The consent is to outline the new use of the information and of the terms of agreeing or refusing to the disclosure. By giving consent, the person acknowledges that she or he knows and understands how and to whom the information is to be disclosed.
- Q6. How does FIPPA define unauthorized disclosure?**
A. Unauthorized disclosure means revealing, exposing, showing, providing copies of, selling, giving or telling personal information in ways that are not permitted by the privacy law.

RETENTION OF PERSONAL INFORMATION

- Q1. How long do I have to keep personal information?**
A. The retention period for personal information under FIPPA is at least one year after use, unless the individual concerned consents to earlier disposal. There may also be internal and legal considerations that require a longer retention period, for example the Income Tax Act.
- Q2. How long do I have to keep student exams, essays and other assignments?**
A. All unclaimed student work, including exams, essays and other assignments are to be kept for six months in accordance with the Faculty Handbook III. 9.2.4.
- Q3. What do I do with the old copies of the personal information, once I've updated information?**
A. When information is updated the outdated information must be retained in some format so that it is available for the prescribed retention period of a minimum of one year. The outdated documentation does not necessarily need to be stored in the same location as the current information.
- Q4. What is the e-mail protocol and retention period in regard to correspondence, regarding personal information, with students?**
A. Generally speaking, all e-mails from and to students that contain personal information and that you **use** for purposes such as evaluating their contributions during a course or for advising regarding their educational path should be retained for a minimum of one year under FIPPA.
- Q5. What is the e-mail protocol and retention period in regard to correspondence, regarding personal information, with other faculty and administration?**
A. The same general advice applies in regards to e-mails with students. E-mail is generally not considered secure or an appropriate vehicle for the transmission of highly sensitive information. E-mails that contain personal information need to be retained for a minimum of one year.
- Q6. Is there a list of measures to secure personal information that I should follow?**
A. Yes. Please refer to *Best Practices for Security Measures* in the following website:
www.brocku.ca/accessandprivacy/ For electronic security measures, please refer to ITS'
www.brocku.ca/its/security/

DISPOSAL OF PERSONAL INFORMATION

- Q.1 Is it necessary to log all personal information that has been, or is about to be, disposed of?**
A. No, as long as departmental procedures state that certain personal information will be destroyed at certain times.

The Procedure regarding Handling Personal Information is available at this link: www.brocku.ca/accessandprivacy. Please contact Marion Hansen at mhansen@brocku.ca if you have further questions.