



INTRODUCTION

This procedure outlines the general rules regarding the collection, use, disclosure, retention and disposal of personal information in the custody or under the control of Brock University. Brock University recognizes that an individual's right to privacy includes the right to know how his/her personal information is being used. All Brock employees who handle personal information on behalf of the University have a responsibility to ensure that the information remains confidential and secure. These procedures are intended to comply with the requirements of the *Freedom of Information and Protection of Privacy Act* (FIPPA).

DEFINITION OF PERSONAL INFORMATION

Personal Information, as defined by FIPPA, means recorded information about an identifiable individual, including, but is not limited to such basic details as name, home address, 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.

COLLECTION OF PERSONAL INFORMATION

1. Collect only the personal information necessary in order to fulfill the purpose for which the information was collected.
2. Personal information is to be collected directly from the individual whom the information is about, with few exceptions. (See number 11 for the exceptions.) This ensures that the information collected is up-to-date, complete and accurate.
3. Personal information includes activities where individuals respond through interviews, questionnaires, surveys, polls, or by completing forms in order to provide information to the University.
4. There is no restriction on how personal information is collected. The means of collection may be writing, audio- or videotaping, electronic data entry or by other means.
5. All personal information, as defined above, must remain confidential.

6. Where collecting personal information from an individual Brock University is required by FIPPA to notify individuals that:
 - a. The Brock University Act provides the legal authority to collect personal information.
 - b. The purpose for which the information is collected.
 - c. A contact position who can answer questions about the collection
7. In order to meet the above requirements, copy and paste the wording from the following standard **Collection Notice** to the bottom of each form originating from the department, where personal information is collected.

Collection Notice:

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/\[your departmental website\]](http://www.brocku.ca/[your departmental website])

8. Insert departmental information in place of the information in square brackets. See above.
9. Add the above Collection Notice to hard copy and electronic forms that require personal information. The Collection Notice need only appear on one page of a multiple paged form.
10. Departments must ensure that all departmental forms have a Collection Notice when collecting personal information from employees, students, alumni, clients, and members of the general public.
11. You do not need to obtain consent to collect personal information if the information is being collected, as per FIPPA, to:
 - a. Determine suitability for an honour or award;
 - b. Recognize outstanding achievement or distinguished service;
 - c. Conduct a proceeding or possible proceeding before a court or tribunal, or;
 - d. For law enforcement purposes.

USE OF PERSONAL INFORMATION

1. Take reasonable steps to ensure the personal information collected is accurate, up to date and secure.
2. Only use personal information for the purpose for which it was obtained or for a consistent purpose.

A consistent purpose means that the individual could reasonably expect this use/disclosure of his/her personal information. Where personal information is collected other than directly from the individual, a consistent purpose is determined by considering whether the proposed use/disclosure of this information is reasonably compatible with the purpose for which it was collected.

3. Only use personal information where the individual to whom the information relates has consented to the use proposed by Brock in the Collection Notice. When personal information is to be used for a new purpose, outside of the parameters of the Collection Notice, then further consent needs to be obtained from the individual which includes the new purpose for which consent is given, the date, and the personal information to be used.
4. 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.
5. Employees and third parties whom Brock University authorizes to handle personal information must protect the personal information and records they use by following appropriate security arrangements. This will help to ensure there is no unauthorized access, collection, use, disclosure, correction, retention or disposal of personal information and records.

Before personal information is provided to any third party service provider, the University's Confidentiality and Privacy Agreement is to be signed by the third party. For more information, please contact the Freedom of Information and Privacy Coordinator.

6. Departments are responsible to self monitor compliance with security standards to ensure that physical and procedural security precautions are established and maintained.

DISCLOSURE OF PERSONAL INFORMATION

1. Individuals have a right to ask to review or obtain a copy of their own personal information and to request a correction of the record containing their own personal information. FIPPA outlines exemptions and exclusions whereby individuals will not be given access to personal information.
2. Student records are only to be disclosed by the Office of the Registrar or Graduate Studies Office where appropriate. For more information, see the Access to Student Records and Disclosure of Information Policy.
3. Records regarding faculty, staff, and other members of the University community, should not be disclosed unless such a disclosure is in keeping with the University wide Access to Information and Protection of Privacy Policy.
4. An individual has the right to make a formal request for personal information, if the information requested is not provided through the above routine processes. All formal requests for information under FIPPA, are to be in writing and addressed to the Freedom of Information and Privacy Coordinator.

RETENTION OF PERSONAL INFORMATION

1. FIPPA requires that personal information that is used is to be kept for a minimum of one year. There may also be internal and legal considerations that require a longer retention period, for example, the Income Tax Act.

2. When information is updated the outdated information must be retained in some form so that it is available for the prescribed retention period of one year. The outdated documentation does not necessarily need to be stored in the same location as the current information.
3. It is the responsibility of each unit head to ensure that the appropriate retention periods are observed.
4. The prescribed minimum retention period for records containing personal information is noted in the Personal Information Banks. Unit heads may, at their discretion, keep the records for a longer period of time if it is deemed necessary.

DISPOSAL OF PERSONAL INFORMATION

1. Ensure material for shredding has completed its scheduled retention period according to FIPPA and the department's records retention schedule. Disposal of records should occur routinely and in keeping with retention policies and procedures.
2. Check with the unit head to confirm that there is no active legal investigation, freedom of information reviews or audits relating to the records that are scheduled for disposal.
3. Personal information is to be destroyed in such a way that it cannot be reconstructed or retrieved. Paper and other hard copy records such as microfiche for instance, should be burned, pulped, or shredded and not discarded or disposed of as garbage.
4. Personal information on magnetic media such as tape or disk should be disposed of by magnetic erasure or by destruction of the medium. When the medium is retained and re-used within a secure environment, reformat or clear prior to re-using. For further information contact Brock University User Services.
5. Take all reasonable steps to protect the security and confidentiality of personal information that is to be disposed.
6. Maintain a disposal record setting out the category of records containing personal information that was destroyed and the date of that destruction. Include the type of record involved (e.g. ABC Program Files) and not information about an identifiable individual.
7. Note that documenting what personal information has been destroyed is a requirement of FIPPA. Documenting all other records destroyed is good practice.

PERSONAL INFORMATION BANKS

1. Brock University maintains Personal Information Banks in keeping with FIPPA. These are available on the University's Freedom of Information and Protection of Privacy website.
2. A Personal Information Bank lists the types of personal information that the University collects. It is important that the University protects the personal privacy of individuals and, in keeping with FIPPA, access to information is subject to limited and specific exemptions.

DIRECTORY OF RECORDS

1. Brock University maintains a Directory of Records in keeping with FIPPA. This is available on the University's Freedom of Information and Protection of Privacy website.
2. A Directory of Records lists the general classes or types of records held by the University.

RELATED POLICIES

- Access to Information and Protection of Privacy Policy
- Access to Student Records and Disclosure of Information Policy

For more information about the application of these procedures, please see Brock University's Freedom of Information and Protection of Privacy website at www.brocku.ca/accessandprivacy or contact the Freedom of Information and Privacy Coordinator at 905-688-5550, ext. 5380.

Revised: July 8, 2010