USE AND DISCLOSURE OF PERSONAL INFORMATION PROCEDURE

PURPOSE

The purpose of this document is to provide instruction to members of the University community on how to use and disclose Personal Information in compliance with the University's Access to Information and Protection of Privacy Policy ("Access and Privacy Policy").

PART A

How to use Personal Information appropriately

1. **Use the information for an authorized purpose**
   You must only use Personal Information for the purpose for which it was collected or a consistent purpose. This means that if the individual was told the information would be used for a certain purpose, the information can only be used for that purpose and other uses which the individual might reasonably have expected. If you want to use the information for any other purpose, other than fundraising, you must obtain the consent of the individual. If using the information for fundraising purposes, comply with the Use of Personal Information for Fundraising Procedure.

2. **Share internally, on a need to know basis**
   You should only disclose Personal Information to a fellow Brock University employee if they need the information in the performance of their duties.

3. **Keep information secure**
   You must take reasonable efforts to prevent unauthorized access to Personal Information or inadvertent destruction or damage.
   See Best Practices for Security Measures for Protecting Personal Information. Also, see ITS Security and Antivirus guidelines for electronic security.

4. **Report any suspected privacy breaches**
   If you suspect that an individual's Personal Information has been accessed by a third party or disclosed to a third party other than as permitted under the Freedom of Information

and Protection of Privacy Act ("FIPPA"), you should immediately notify the University's Freedom of Information and Privacy Coordinator ("FIPPA Coordinator") and follow the Privacy Breach Notification Procedure.

PART B

When you can disclose Personal Information

1. When you can disclose Personal Information directly

You can disclose Personal Information to another person or organization in the following circumstances:

a. When you are disclosing Personal Information for the very purpose for which it was collected or a consistent purpose;
b. When the individual has consented to the disclosure;
c. When you are disclosing to a consultant or agent of the University who needs the Record to perform their duties and the disclosure is necessary and proper in the discharge of the University's functions;
d. When it is required by law;
e. When disclosure is to a law enforcement agency for law enforcement proceedings;
f. In compelling circumstances involving an individual's health or safety;
g. In compassionate circumstances when an individual is injured, ill or deceased;
h. To an MPP who has been authorized by the individual to make an inquiry on the individual's behalf;
i. To a member of the bargaining agent who has been authorized by an employee to make an inquiry on the employee's behalf; or
j. For research purposes, provided certain conditions have been met and a research agreement is in place.

For further details about each of these grounds, see below. If you are uncertain if the use or disclosure of Personal Information is appropriate, you should consult with the FIPPA Coordinator.

a. **For the purpose for which it was collected or a consistent purpose**: If the information was collected for a purpose which implicitly or explicitly included disclosure to a third party, you may disclose the information. The disclosure should be one which the individual would reasonably expect.

b. **Where the individual has consented to the disclosure**: If the individual to whom the information relates has identified that information in particular

and consented to its disclosure, you may disclose the information.

The consent should specify:

- The particular Personal Information to be used/disclosed;
- The use being consented to or the entity to whom the information is to be disclosed; and
- The date of the consent.

If you receive a written consent for the University to release an individual's Personal Information to their solicitor, forward the request to the Office of the Registrar (for undergraduate students) Faculty of Graduate Studies (for graduate students), or FIPPA Coordinator (for all other requests) to respond.

c. **To an agent or consultant**: If you wish to disclose Personal Information to an agent or consultant, you should contact the FIPPA Coordinator to arrange a signed Confidentiality and Privacy Agreement.

d. **Required by law**: If a statute requires you to disclose Personal Information, you may disclose the information. If you are required to release student Records to government agencies or professional licensing bodies, refer to the Access to Student Records and Disclosure of Information Policy.

e. **Law enforcement**: If you are asked by a law enforcement agency for Personal Information, refer the officer to the Director, Campus Security Services or the FIPPA Coordinator. For example, if a police officer wants to confirm a student's status, you can inform the officer that you cannot confirm or deny the status of a student, and refer them to the Director, Campus Security. If the officer is asking for a copy of attendance Records, you can inform the officer that you cannot confirm or deny the status of a student, and refer them to the FIPPA Coordinator.

f. **Emergencies**: If there are compelling circumstances affecting the health or safety of an individual, contact the Student at Risk team who works with the FIPPA Coordinator to determine the type of information that may be released in an emergency.

g. **Compassionate circumstances**: If an individual is injured, ill or deceased, you may release the individual's Personal Information to facilitate contact with the individual's spouse, close relative or friend.

h. **Research purposes**: If a researcher requests certain Personal Information for research purposes, it is permissible to disclose the information in certain circumstances (e.g. if the research cannot be reasonably accomplished unless the information is provided in individually identifiable form) provided the researcher signs a security and confidentiality agreement. Contact the Office of Research Services for a confidentiality agreement.

PART C

How long to keep Personal Information for

1. **Retain Personal Information for one year minimum**
FIPPA requires that University Records containing Personal Information be kept for at least one year after use unless the individual to whom the information relates consents to its earlier disposal. Some Records must be kept longer. For example, Records that contain both personal and financial information must by law be kept for seven years.

   If you are unsure of the retention period for Personal Information collected within your unit, consult the Personal Information Bank on the University's FIPPA website. If questions, contact your supervisor, or the FIPPA Coordinator.

PART D

How to dispose of Personal Information securely

1. **Disposal of print Records**
Print Records containing Personal Information may be disposed of by shredding the document yourself using a cross-cut shredder or placing in your unit's designated bin for shredding.

2. **Disposal of electronic Records**
If you have electronic Records that have met the minimum retention period, and no longer require the Records, you should either destroy the media and discard it or, if you wish to reuse the media, the media should be overwritten or demagnetized using reliable software. Contact Information Technology Services for further information.

3. **Log disposal**
   Once you have disposed of the Personal Information, log the category of Records containing Personal Information that was destroyed and the date of that destruction. Include the type of Record involved and not information about an identifiable individual. For example, note that 2013/2014 final exams for 'X' course in the 'X' program were destroyed on 'X' date and by whom.

   Documenting what Personal Information has been destroyed is a requirement of FIPPA.