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 make 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 Access guidelines for electronic security including cyber security awareness.

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 Privacy Office at Privacy@Brocku.ca 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 another Brock employee or 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 if upon disclosure notification thereof is mailed to the last known address of the individual to whom the information relates;

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. 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.

Note, the Course Calendars provide notice to students that their information on admission, registration and academic achievement may be disclosed and used for statistical and research purposes by the University, other post-secondary educational institutions, and the provincial government.

If you are uncertain if the use or disclosure of Personal Information is appropriate, you should consult with the Manager, Privacy & Records Management. For further details about each of these grounds, see below:

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.

Please note, if you wish to share Personal Information with another individual who is not a Brock employee, agent or consultant for the purpose of obtaining advice you should anonymize the Personal Information so that there is no personally identifiable information disclosed. For example, summarize the information without including names or redact the Personal Information from the documents you wish to share.

Even if you are sharing Personal Information with a Brock employee for a consistent purpose (e.g. with your union representative for the purpose of obtaining advice), you should limit the Personal Information shared to that which is strictly necessary and wherever possible anonymize the information.

Employees are expected to exercise their judgment and are accountable for any improper or unnecessary disclosures.

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 Manager, Privacy & Records Management (for all other requests) to respond.

c. To another Brock employee: If you wish to disclose Personal Information to another Brock employee, you should first consider whether the employee needs the information to perform their duties, or whether it can be provided on an anonymous or de-identified basis. In addition, you should only share as much information as is necessary for the purpose of performing their duties.

d. To an agent or consultant: If you wish to disclose Personal Information to an agent or consultant, you should contact the Manager, Privacy & Records Management to arrange a signed Confidentiality and Privacy Undertaking or confirm that appropriate confidentiality and privacy protections are in place with the agent or consultant.

e. 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.

f. Law enforcement: If you are asked by a law enforcement agency for Personal Information, refer the officer to the Director, Campus Safety Services or the Manager, Privacy & Records Management. 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 Safety Services. 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 Manager, Privacy & Records Management.

g. Emergencies: If there are compelling circumstances affecting the health or safety of an individual, contact the Student at Risk team who works with the Manager, Privacy & Records Management to determine the type of information that may be released in an emergency.

h. 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.

i. 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 Records Classification & Retention Schedule on the

University's Legal, Compliance & Privacy SharePoint site. If you have questions, contact your supervisor, or the Records Coordinator.

PART D

How to dispose of Personal Information securely

The Records Management Policy defines what is a University Record. The disposition of a University Record is listed in the Records Destruction Procedure. All dispositions must be authorized by the Record Steward listed in the Records Classification & Retention Schedule.

To dispose of University Records, please follow Brock's Records Destruction Procedure.

The Records Disposition and Authorization form serves as the documentation for all of Brock's Records dispositions.

June 2024