Privacy Breach Procedure

Introduction

Part 3 of the British Columbia *Freedom of Information and Protection of Privacy Act* (the Act) establishes protection of privacy rules with which the University must comply. The Act governs the collection, accuracy, correction, protection, storage, retention, disposal, use and disclosure of personal information.

Purpose

This procedure outlines the steps to be taken as soon as the University learns of a privacy breach. Following this procedure will help the University: 1) implement immediate remedial measures to mitigate any harm caused by the breach; and 2) take steps to prevent a similar breach from happening again.

Scope

This procedure applies to all University employees, volunteers and service providers engaged in a sanctioned University activity that involves the handling of personal information in the custody or under the control of the University. With respect to service providers, this procedure applies only during the term of their contract with the University.

Definitions

“Access” means disclosure of personal information by the provision of access to personal information.

“Custody or control” means personal information contained in records belonging to the University, but does not apply to the following:

1. A record containing teaching materials or research information of:
   (i) A faculty member, as defined in the *University Act*, of a post-secondary educational body,
   (ii) A teaching assistant or research assistant employed at a post-secondary educational body, or
   (iii) Other persons teaching or carrying out research at a post-secondary educational body;
2. Material placed in the University Archives or University Library by or for a person or agency other than a public body; and
3. A record of a Service Provider that is not related to the provision of services for a public body.

“Disclose” and “disclosure” means to reveal, show, expose, provide copies of, sell, give or tell personal information.

“Employee” means a person employed for wages or salary by the University, including staff, faculty, instructors and administrators.
“Personal information” means recorded information about an identifiable individual, other than employees’ business contact information, such as:

- names, home addresses and telephone numbers;
- age/birthdate;
- sex;
- marital or family status;
- identifying number (e.g., student or employee number, personal education number, social insurance number, personal health care number, driver’s license number);
- race, national or ethnic origin;
- colour;
- religious or political beliefs or associations;
- educational history (e.g., personal data maintained on any undergraduate or graduate student file or stored in a student information system such as SIMS, SERA, OASIS and/or a learning management system such as Canvas or LON-CAPA, including applications; references and evaluations; admission; enrolment; academic advising, assignments, grades, transcripts and test scores; coop work placements; career counseling; volunteer activities; finances and financial assistance; academic dishonesty and misconduct investigations and discipline; extra-curricular activities; etc.);
- medical history (e.g., personal data maintained on any patient, student, employee or disability case file describing medical conditions, diagnoses, treatment and procedures; prescribed drugs; psychological and psychiatric evaluations; occupational health and safety; etc.);
- disabilities (e.g., personal data maintained on any patient, student, employee or disability case file describing physical and cognitive assessments, abilities, treatment and accommodation; etc.);
- blood type;
- employment history (e.g., personal data maintained on any employee file or stored in administrative information systems such as HAPS and FINS, including applications; CVs, references; recruitment and hiring; performance evaluations; renewal, tenure, promotion and salary review; work schedules and absences; compensation, pension and benefits; finances and financial awards; grievances; misconduct investigations and discipline; career counseling, professional development and training; outside activities; employment separation, termination and retirement; etc.);
- financial history (e.g., banking, tuition, loan, grants and tax information; donors and donations; etc.);
- criminal history (e.g., complaints; incident reports; criminal record checks; etc.);
- images (e.g., student and employee photo identification systems);
- anyone else’s opinions about an individual;
- an individual's personal views or opinions; and,
- name, address and phone number of parent, guardian, spouse or next of kin.

“Privacy breach” means when there is illegal access to or collection, storage, retention, disposal, use or disclosure of personal information. The Act describes the only circumstances when and how the University is authorized to collect, store, retain, dispose of, use and disclose personal information about individuals (students, faculty, staff, alumni, donors, etc.). A situation that is not authorized under the Act is illegal and thereby a privacy breach. Examples include but are not limited to:

1. The collection and use of personal information when there is no demonstrable need for it to administer a university sanctioned program or activity;
2. Unauthorized access to and use of student, employee, alumni or donor personal information stored in a university database or paper filing system by a person who has no need to know for the purpose of performing her or his assigned employment duties;
3. An email message or its attachment containing student, employee, alumni or donor personal information addressed and sent to the wrong person(s) who have no need to know;

4. Disclosing student, employee, alumni or donor personal information to an external third party when it is not explicitly authorized under the Act;

5. Files containing applicants’ personal information are not password protected or encrypted and are accessible through an unsecured website, network or shared drive enabling unauthorized access;

6. The loss or theft of a computer, tablet or other digital storage media (e.g., flash drive, CD, DVD) on which personal information is stored, regardless of whether the devices and files are password protected or encrypted;

7. A hacked university information technology system allowing the hacker unauthorized access to personal data about students, employees, alumni or donors;

8. The use of a software application or service provider who stores student, employee, alumni or donor personal information outside Canada without the person’s prior express written consent or other legal authority stipulated under the Act;

9. The copying, removal and retention of personal information in records belonging to the University when a staff or faculty member’s employment with the University terminates; and

10. The disposal of paper records or digital storage devices containing individuals’ personal information by means of recycling programs. Recycling is not a means of secure and confidential destruction. Confidential destruction uses a secure procedure and a method that makes personal data recovery impossible (e.g., crosscut or hammer-mill shredding, pulverizing or burning of paper records and deleting digital data in a way that it is immediately overwritten, erased and cannot be reconstructed).

“Service provider” means a person retained under contract to perform services for SFU.

“Volunteer” means a person who performs a service for the University without being paid.

Procedure

The person discovering the privacy breach (e.g., faculty, staff, IT Services) will immediately take the actions described below. Steps 1-3 will be carried out simultaneously or in quick succession. When responding to a Privacy Breach, the first three steps are priorities.

Departments in which a privacy breach occurs will complete steps 1-3. The Information and Privacy Officer or Coordinator will complete steps 4 and 5.

Step 1 – Identify and Contain

1. Contact the Information and Privacy Officer or Coordinator who will advise you what further steps to take and send you a copy of the Privacy Breach Report for you to complete.

2. Identify the scope of the potential privacy breach and take initial steps to contain it.

3. Recover the personal information. Ensure that no paper or electronic copies of the personal information were made or retained by the person who was not authorized to receive the information and obtain the person’s contact information for subsequent notification. In cases where copies were made or received, please see step 3 below for what action to take.

4. Determine if the privacy breach would allow unauthorized access to any other personal information and take what steps are necessary to protect that data (e.g., change computer passwords, temporarily shut down access to an electronic information system).
5. Contact Safety and Risk Services immediately if you believe the privacy breach could lead to identity theft, financial fraud, physical harm, damage to an individual's personal or professional reputation, breach statutory or contractual obligations, fail to meet professional or certification standards or cause a person some other type of harm or injury.

6. Contact IT Services immediately if you believe the security of an electronic system has been compromised.

7. Contact Campus Security immediately if you believe personal information was stolen (e.g., an office was broken into and computers stolen).

**Step 2 – Report**

8. Notify immediately all appropriate staff in your program area about the privacy breach, including your supervisor, manager, chair or director.

9. Report the privacy breach to the University Secretary if you are unable to contact either of the Information and Privacy Officers or Coordinator.

10. Complete Section 1 of the Privacy Breach Report and return it to the Information and Privacy Officer or Coordinator as soon as possible.

11. The Coordinator of Information and Privacy will decide when it is necessary that the University report a privacy breach to the Office of the Information and Privacy Commissioner for British Columbia (OIPC). The Coordinator will make this decision upon considering the circumstances that caused the privacy breach; the type, quantity and sensitivity of the personal information involved; the number of individuals affected; the number of unauthorized recipients; the media on which the personal information was stored and transmitted; the location where it was stored; and any other relevant factors.

**Step 3 – Notify**

12. Notify in writing the individuals whose privacy was breached. The Information and Privacy Officer or Coordinator will provide you with a template of the privacy breach notification letter. The notification will describe the extent of the breach, the personal information breached and the steps taken to address the breach, both immediate and long-term.

13. Notify in writing the individuals who received the personal information without authority, either to recover it or to ensure its confidential destruction. The Information and Privacy Officer or Coordinator will provide you with a template of the personal information recovery notification letter. The notification will request that the information either be returned to the University or the individual confirm in writing its confidential destruction. In cases of electronic records, the notification will require confirmation that the personal information was deleted from the person’s desktop computer, server and any other storage device or media in such a way that it cannot be recovered.

14. Ask the Information and Privacy Officer or Coordinator to review the notification letters prior to sending them.

**Student Personal Information only:**

15. Send the Associate Registrar, Information, Records and Registration a spreadsheet (either one you create or an existing class list) of all student names and student ID numbers whose personal information was breached. Student Services will place a privacy breach service indicator on each student record in the Student Information Management System for these students. The service indicator will require students to make requests for official university documents in person at the Registrar’s Office until the service indicator is lifted. This security measure is intended to protect students from identify theft or fraud when requesting a Confirmation of Enrolment Letter, a parchment or a transcript.
Step 4 – Investigate

16. The Information and Privacy Officer or Coordinator will conduct an internal investigation into the privacy breach to:
   (i) Review the circumstances surrounding the breach, determining and documenting all relevant facts;
   (ii) Ensure the immediate requirements of containment and notification are addressed; and
   (iii) Review the adequacy of existing physical, procedural and technical security measures used to protect personal information and recommend any improvements.

Step 5 – Management Review

17. The Information and Privacy Officer will:
   (i) Report the privacy breach, including remedial steps taken, findings, conclusions, advice and recommendations to the Director or Manager of the program area, the Information and Privacy Coordinator and other administrators if necessary;
   (ii) Report the investigation results to the Chief Safety Officer when a privacy breach could lead to identity theft, financial fraud or compromise the security of university property;
   (iii) Report the investigation results to the Chief Information Officer when a privacy breach was also a data security breach of an electronic information system; and
   (iv) Advise the OIPC of the University’s findings and work with the OIPC to make any necessary changes, when the University deems it necessary to notify the OIPC of the privacy breach.

18. The Information and Privacy Officer or Coordinator will:
   (i) Educate and train staff regarding protection of privacy requirements at the request of the department in which the privacy breach occurred; and
   (ii) Prepare periodically a summary of reported privacy breaches, identifying and recommending solutions to systemic privacy breaches.

Authority

This Procedure is administered by the Coordinator of Information and Privacy under Information Policy I 10.02 Head of the Institution and Delegation of Authority Under the Freedom of Information and Protection of Privacy Act.

Refer to the Archives and Records Management website for contact information:
- Coordinator of Information and Privacy
- Information and Privacy Officers