| Sheridan \| Get Creative | THE SHERIDAN COLLEGE INSTITUTE OF TECHNOLOGY AND ADVANCED LEARNING | |
|---|---|---|
| **TITLE: PROCEDURE FOR REPORTING PRIVACY BREACHES AT SHERIDAN** | | |
| **Date of Approval: July 2, 2015**<br><br>**Effective Date: July 2, 2015** | **Mandatory Review Date: 3 years** | **Approved By: The Office of General Counsel** |

This document contains information intended to guide Sheridan community members in addressing a confirmed or suspected privacy breach. The *Freedom of Information and Protection of Privacy Act*[i] (FIPPA) applies to public educational institutions in Ontario, and provides rules to ensure the protection of individual privacy. FIPPA, in its sections 37-46, governs "the retention, use, disclosure and security of personal information".[ii]

## WHAT IS A PRIVACY BREACH?

According to Ontario's Information and Privacy Commissioner (IPC) a privacy breach occurs when:

*"[T]here is unauthorized access to or collection, use, disclosure or disposal of personal or health information."*[iii]

"Personal Information" is defined in section 2(1) of FIPPA as: "recorded information about an identifiable individual, including,

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, telephone number, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they relate to another individual,

(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual, and

(h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual; ("renseignements personnels").

A privacy breach may:

- affect an individual or a group of individuals;
- be discovered during the course Sheridan's business;
- be reported by someone within Sheridan, or by someone external to Sheridan, including the Information and Privacy Commission of Ontario.

***Examples of a privacy breach***

Examples of a privacy breach include:

- mistaken disclosure of personal information (e.g. an email containing personal information is mistakenly sent to the wrong person);
- stolen personal information (e.g. a lost computer);
- lost personal information (e.g. a misplaced file);
- use of personal information for a purpose inconsistent with the original purpose for which it was collected.

## WHAT TO DO IF A PRIVACY BREACH IS SUSPECTED OR CONFIRMED

Whether you suspect or are certain that a privacy breach has occurred, it is important that you take action immediately.

## REPORT IT!

- Report the privacy breach to your immediate supervisor. If your supervisor is not available, report the breach to the next available level of management. The head of the department or unit where the breach has occurred should also be notified. The individual with the most complete knowledge of the breach should fill out the form.
- Report the privacy breach to Sheridan's Office of the General Counsel, who will investigate the incident. The Office can be reached by contacting: Telephone No. 905-845-9430, ext. 2872, or emailing privacy@sheridancollege.ca.

## FOUR IMPORTANT STEPS

The necessary action to take in cases involving a breach of privacy will vary according to the circumstances surrounding the breach. The IPC has outlined the following four steps as a guideline for what to do when a breach of privacy occurs:

1. containing the breach and conducting a preliminary assessment;
2. evaluating the risks;
3. notification;
4. prevention.

Steps 1, 2 and 3 should be taken immediately after discovery of the breach and should be taken either simultaneously or in quick succession. Step 4 is a more long-term response to the privacy breach. These four steps are outlined in more detail below.

## STEP 1: CONTAINING THE BREACH AND CONDUCTING A PRELIMINARY ASSESSMENT

**Important Considerations**

### *1. Containing the breach*

Taking immediate steps to contain a privacy breach will minimize the damage caused. Steps to that you must take to effectively contain a breach:

- shutting down the system where the breach occurred;
- taking steps to recover lost information;
- restricting or revoking access to information, by doing things such as changing access codes or locks;
- contacting appropriate internal staff members and informing them of the breach (e.g. department head, supervisor);
- contacting Sheridan's Office of the General Counsel;
- contacting Sheridan Security in case of suspected criminal activity. They can be reached at:
    - Trafalgar campus: Extension 4044 from within campus or 905-815-4044 from outside campus;
    - Davis campus: Extension 4344 from within campus or 905-815-4344 from outside campus;
    - Hazel McCallion Campus: Extension 7944 from within campus or 905-815-7944 from outside campus;
    - Skill Training Campus: Extension 4181 from within campus or 905-815-4181 from outside campus;
- making note of any details of the incident that are known to you at the time. This will help any investigation that may take place.

It is important to remember not to take action that may compromise a later investigation, such as destroying material of possible evidentiary value.

### *2. Preliminary assessment*

A preliminary assessment involves ascertaining and recording the following basic information:

- when the incident occurred (date and time);
- where the incident occurred;
- when the incident was discovered (date and time);
- how the incident was discovered;
- facts pertaining to the breach and its discovery.

## STEP 2: EVALUATING RISK

An appropriate response to the privacy breach can only be formulated once an assessment of the risks associated with the breach has been done. This involves determining what the type of personal information involved in the privacy breach was, and its level of sensitivity.

**Important Considerations**

### *1) The personal information involved*

This may include:

- **The data elements involved in the breach**
  Determine what information was involved in the privacy breach.
- **The format of the records**
  Determine whether the records involved in the breach were in paper, electronic or other form. In case of electronic information, determine whether the information was encrypted, anonymized or otherwise restricted, and the security measures, both physical and technical, at the time of the breach.
- **The sensitivity of the information involved**
  The risk of harm increases with the sensitivity of the information involved in the breach. Sensitive information includes but is not limited to the following: health information, government issued identification such as social insurance numbers, and financial information such as bank account and credit card numbers. A combination of personal information associated with the privacy breach carries with it more risk.

### *2) Cause and extent of the breach:*

This includes:

- **The cause and extent of the breach**
  It is important to determine what caused the privacy breach and what the extent of the breach was. How much information was taken? Who could the possible recipients be?
- **Risk of further breach**
  The risk of further breach can be assessed by considering:
  - whether the information involved was encrypted or otherwise difficult to access;
  - whether the information may be used in identity theft or for other fraudulent purposes; and
  - the steps that have been taken to minimize harm.

### *3) Persons affected*

Determine the number of individuals affected by the breach. Also determine their identity and role within the institution, i.e. were they employees, students, or third parties?

### *4) Foreseeable harm*

Determine the:

- harm that could result to individuals from the privacy breach, such as risk to their physical or financial security, or damage to their reputation;
- harm that could result to Sheridan from the breach, for example, financial loss, damage to reputation, or loss of confidence/trust;
- possible harm to public health or safety as a result of the breach.

## STEP 3: NOTIFICATION

Notifying affected individuals can be useful in mitigating the harmful effects of a privacy breach.

**Important Considerations**

### *1. Notifying affected individuals*

Assess the harm that may be caused to affected individuals as a result of the breach. If there is a risk of harm, it is generally necessary to notify the affected individual. An exception to this would be if such a notification would interfere with law enforcement, or where it would endanger public health or safety.

### *2. The process by which to notify*

Once it is determined that an affected individual should be notified, it is important to do so as soon as is reasonably possible. Determine when and how the affected individual will be notified, and who will notify them. Usually, the department that has a direct relationship with the affected individual will notify them. Sheridan's Office of the General Counsel should be consulted in this regard. Generally, it is preferred that a direct method of communication be used, such as phone, email or in-person.

### *3. The content of the notification*

The notification should include the following information:

- information about the incident and when it occurred;
- the information involved in the breach;
- any steps that have been taken to address the breach and mitigate damage;
- future steps planned to prevent such occurrences;

- if required, guidance should be given on how individuals can protect themselves from such breaches in the future;
- who to contact within Sheridan if further information is sought.

Complete the Privacy Breach Report Form available at the following link. Send the completed Privacy Breach Report Form to the Office of the General Counsel at 1430 Trafalgar Road, Oakville, Ontario, L6H 2L1, or by email at privacy@sheridancollege.ca.

## STEP 4: INVESTIGATION AND PREVENTION

Sheridan's Office of the General Counsel will conduct an investigation into the breach and consider whether a prevention plan needs to be developed. The Office will also determine whether the Information and Privacy Commissioner of Ontario needs to be informed of the breach.

Prevention plans may include:

- a review of existing policies;
- training;
- audit of both physical and technical security;
- an audit to ensure the implementation of any prevention plans in place.

---

[i] R.S.O. 1990, c. F.31.

[ii] Office of the Information and Privacy Commissioner for Ontario: "Privacy Breach Protocol: Guidelines for Government Organizations", online, https://www.ipc.on.ca/images/Resources/Privacy-Breach-e.pdf.

[iii] Office of the Privacy Commissioner of Canada: "Key Steps in Responding to Privacy Breaches", online, < https://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.pdf>.