# 6.E-2008 Privacy Breach Procedure

## 1. Purpose

To guide the response to and containment of a privacy breach, to minimize the potential harm from a privacy breach and to prevent additional breaches.

## 2. Overview

A privacy breach occurs when there is unauthorized collection, use, disclosure or destruction of personal information. From time-to-time instances of breach of information maintained under the custody or control of St. Mary's University (University) may occur. The following procedure outlines the critical actions that need to be taken following the discovery of a potential privacy breach.

## 3. Procedure

### 3.1 Report

Even if a breach is only suspected and has not yet been verified, it must be reported to the appropriate individual upon notification. Notification can come from either an internal source (i.e. an employee) or an external source (i.e. a third-party contractor).

If reporting internally, a privacy breach or suspected breach needs to be reported to:

a. Supervisor and/or information steward (the individual responsible for the security and integrity of the information) for the area affected by the breach.
b. Human Resources – Privacy Division.

| Approval Authority | Responsible Office | Effective Date | Date Last Revisited | Review Frequency |
|---|---|---|---|---|
| **Board of Governors** | **Human Resources** | | | **Every 5 years** |

It is important to provide as much information as possible when reporting. Some points that should be included are:

- what happened,
- in which department,
- when the incident occurred,
- how the breach was discovered, and
- whether any corrective action has already been taken.
- Any additional information on the incident should be included (i.e. if law enforcement were involved).

### 3.2 Assess

Once a report of the situation is made to the appropriate individuals, an assessment of the situation will be carried out to determine whether a privacy breach has indeed occurred. Two important questions are asked during an assessment:

a. Is personal information involved?
   Not all data in the custody or control of the University is personal information. Therefore, the first part of the assessment is to identify the type of information affected by the incident in order to determine whether a breach has occurred.

b. Has an unauthorized disclosure occurred?
   Unauthorized disclosure is the defining characteristic of a privacy breach. Whether it is intentional, inadvertent or as a result of criminal activity, an unauthorized disclosure constitutes a privacy breach.

If the answer to both questions is "yes", a privacy breach has occurred. The following factors are relevant in determining the severity of the breach:

- Sensitivity of the personal information. Some personal information is more sensitive than others. Publicly available information such as that found in a public telephone directory may be less sensitive whereas government-issued identification such as SIN, driver's license and health care number, and financial account numbers are more sensitive. A combination of personal information is also more sensitive than a single piece of personal information.

- Context of the personal information. For example, a list of student names may not be sensitive. However, the same information about students who will be away from home for a travel study program may be more sensitive.

- Potential uses of the personal information. The combination of certain types of sensitive personal information suggest a higher risk due to the potential for identity theft. For example, an individual's name and address together with government-issued identification numbers or date of birth

- Whether the personal information is adequately encrypted or is otherwise not easily accessible.

- Whether there is a reasonable chance of harm to affected individuals from the disclosure including non-financial losses. For example, if the schedule of a student who is being stalked is released and could result in physical danger. Or, if the information lost includes disciplinary records which can cause harm to individuals' reputations.

- The number of people affected by the breach.

- Whether the information was fully recovered without further disclosure.

An assessment of the severity of the breach will help determine response to the breach. For example, if a laptop containing adequately encrypted information is stolen, subsequently recovered and investigations show that the information was not tampered with, notification to individuals may not be necessary.

**3.3 Contain**

Once it has been determined that a privacy breach has occurred, containment must follow. This involves taking corrective action such as retrieving the personal information that has been released if the breach involved a hard copy, or isolating/suspending the activity, process or system if it was an electronic breach, etc. For example, if online access has been compromised and individuals are able to view other students' records then the entire system would need to be shut down until the problem is resolved. The main goal is to alleviate any consequences for both the individual(s) whose personal information was involved and the University.

### 3.4 Document

The *Information Loss or Breach Report* form should be used to document the details of the privacy breach and the containment activities as well as notification and follow up plans to assist with the implementation of correct remedial measures, in responding to an investigation by the Office of the Information and Privacy Commissioner of Alberta (OIPC) and in evaluating responses so areas for possible improvement may be identified.

### 3.5 Notify

Following a full assessment and containment of the situation, the Privacy Officer will determine whether notification of the individual(s) whose personal information was affected by the privacy breach is required. The following factors will be considered when deciding whether to notify:

- What are the legal and contractual obligations?
- What is the risk of harm to the individual?
- Is there a reasonable risk of identity theft or fraud?
- Is there a risk of physical harm?
- Is there a risk of humiliation or damage to the individual's reputation?
- What is the ability of the individual to avoid or mitigate possible harm?

Once a decision to notify has been made, the Privacy Officer will oversee the notification process to the affected individuals, except in situations when notice is not appropriate or possible (e.g. identities of individuals affected by the breach are unknown, contact information is unavailable or if notice would interfere with a law enforcement investigation).

The preferred method of notification is direct – by phone, letter, email or in person – to affected individuals. Indirect notification – website information, posted notices, media – will generally only occur where direct notification could cause further harm, is prohibitive in cost or the contact information for affected individuals is not known.

The notification should provide the affected individual(s) with sufficient information about:

- What happened and when.
- A generic description of the types of personal information involved in the breach, including whether any unique identifiers or sensitive personal information were involved in the breach.
- The nature of potential or actual risks of harm.
- What action has been taken by St. Mary's University College to address the situation.
- What appropriate action the individual(s) should take to protect themselves against identity theft or other harm (i.e. tracking credit cards, monitoring bank accounts, etc.).
- Contact information for the St. Mary's University College Privacy Officer.
- Contact information for the OIPC.

Individual(s) should be notified as soon as is reasonably possible while taking into account the following factors and details:

- Ensuring that the facts of the situation have been confirmed and well documented to avoid passing on faulty information and making the situation worse.
- Ensuring notice is being provided to the right person.
- Determining if a personal representative or other authorized parties need to be notified if the individual(s) in question cannot receive the notification for any reason (capacity, age, language, etc.).

- Creating a script for telephone notifications so the same information is always given to ensure accuracy and consistency and to clearly identify contact information.

- Making letter notifications clear and concise, using the university's letter head and envelopes.

- Ensuring not to include unnecessary personal information in the notice to avoid possible further unauthorized disclosure.

### 3.6 Communicate

In addition to the affected individuals, other internal or external parties may need to be briefed on the privacy breach such as:

- University President, External Relations staff, Security Coordinator, etc.

- Office of the Information and privacy Commissioner of Alberta (OIPC)

- Police (if theft or other crime is suspected)

- Insurers or others (if required by contractual obligations)

- Credit card companies, financial institutions or credit reporting agencies (if their assistance is necessary for contacting individuals or assisting with mitigating harm)

### 3.7 Investigate

In most circumstances the University will be responsible for investigating its own privacy breaches. An internal investigation must:

- Identify and analyze the events that led to the privacy breach

- Evaluate what was done to contain it

- Recommend remedial action to help prevent future breaches

The Privacy Office will handle the documentation at this point. Any assistance employees can give during the investigation to help fulfill the above requirements should be provided.

There are instances in which the OIPC will be conducting its own investigation. In the event that the OIPC chooses to investigate and publicly report the privacy breach, employees should cooperate fully with their efforts and provide all relevant information.

### 3.8 Implement Change

The most vital outcome of any privacy breach is an understanding of what went wrong and how to prevent and avoid breaches in the future. Once any breach has been fully contained, documented and investigated, the Privacy Committee will undergo:

- A review of relevant information management systems to enhance compliance.
- Amendments or reinforcements to existing policies and practices for managing and safeguarding personal information.
- The development and implementation of new security or privacy measures.
- Staff training on legislative requirements, security and privacy policies, practices and procedures to reduce the potential of future breaches.
- Assessment of the effectiveness and timeliness of the notice to affected individual(s) to determine if practices need to be modified.
- Testing and evaluation of remedial actions to determine if they have been implemented correctly, and if policies and practices need to be modified.