Saint Mary's University

Privacy Breach Management Protocol

GUIDE TO RESPONDING TO PRIVACY BREACH

Privacy Breach: Unauthorized disclosure of "personal information"

Index:

1. What is the purpose of the privacy breach management protocol?
2. What is a privacy breach?
3. Roles and responsibilities
4. Breach management process

    Step 1: Preliminary Privacy Breach Assessment Report & Containment
    Step 2: Full Assessment
    Step 3: Notification
    Step 4: Mitigation and Prevention
    Step 5: Lessons Learned

Appendix 1: Preliminary Privacy Breach Assessment Report

Appendix 2: Privacy Breach Checklist

1. What is the purpose of the privacy breach management protocol?

The protocol allows Saint Mary's University (the "University") to identify, manage, and resolve privacy breaches. It applies to all University information assets – such as personal information, personal health information, workforce personal information, and employee personal information. All members of the University community must follow this protocol, including all full-time and part-time employees, staff, and faculty, contract employees, contractors, people on secondment, temporary workers, and students.

2. What is a privacy breach?

A privacy breach is any event that results in personal information in the custody or control of Saint Mary's University being accessed, used, copied, modified, disclosed, or disposed of in an unauthorized fashion, either deliberately or inadvertently.

Some examples of breaches include:

- A USB key with unencrypted personal information being lost or stolen.
- An excel spreadsheet containing employee benefit information being emailed to the wrong person.
- Employees inappropriately browsing data files containing personal information for non-work-related purposes.
- Hacker engaging in malicious activity resulting in the compromise of the organization's personal information assets.

3. Roles and responsibilities

The following table summarizes the responsibilities of staff when a privacy breach is discovered.

Position	Responsibilities
• All staff	• Complete preliminary breach assessment report. (**Appendix 1**) and immediately report privacy breach to Privacy Officer. • Immediately undertake containment efforts. • Assist with breach investigations as required.
• Privacy Officer	• Receive preliminary breach assessment reports. • Assess the preliminary report to determine whether a privacy breach has occurred. • Recommend immediate containment efforts. • Identify and contact individuals to form an Incident Response Team. • Conduct appropriate internal notifications of the breach.

	• Conduct a full assessment of the breach – complete the privacy breach checklist (Appendix 2). • With the Incident Response Team, determine whether notification of affected individuals is required. • In consultation with communications staff, complete notification. • Notify and liaise with the Information and Privacy Commissioner. • With the Incident Response Team, identify risk mitigation and prevention strategies. • Assign responsibility for completing mitigation and prevention strategies. Follow up to ensure actions are completed. • Conduct trend analysis of privacy breaches. • Keep executive informed of all actions and decisions of the Incident Response Team.
• Chief Information Officer	• Participate on Incident Response Teams when the privacy breach involves systems. • Assist in investigations as to the cause of system-related breaches. • Identify containment and prevention strategies. • Assist in implementation of containment and prevention strategies involving IT or security resources.
• Legal counsel	• Participate as required on the Incident Response Team. • Assist Privacy Officer in assessing whether notification is required.
• Communications staff	• Assist in the drafting of breach notification letters.
• Labour relations/human resources staff.	• Assist in implementation of containment and prevention strategies that require cooperation of staff, particularly unionized staff.
• Office of primary responsibility – manager or supervisor	• Participate on Incident Response Team. • Assist in identifying containment, mitigation, and prevention strategies. • Implement containment, mitigation, and prevention strategies.
• Executive	• Receive and review all reports of privacy breaches. • Follow up with Privacy Officer to ensure that containment, notification, and prevention actions have been completed.

4. Breach Management Process

Step 1: Preliminary Report, Assessment & Containment
Step 2: Full Assessment
Step 3: Notification
Step 4: Mitigation and Prevention
Step 5: Lessons Learned

Step 1: Preliminary Report, Assessment & Containment

When a suspected privacy breach occurs, the employee who discovers the breach must conduct a preliminary assessment to identify the nature of the breach and to identify potential containment steps.

Employees who discover potential breaches must:

- Immediately complete the Preliminary Breach Assessment Report (Appendix 1). The report assists employees in identifying a privacy breach and in identifying useful containment strategies. The preliminary report should be completed on the day the breach is discovered.
- Contact the Privacy Officer and provide a copy of the Preliminary Breach Assessment Report on the day the breach is discovered.
- Advise their supervisor of the potential privacy breach and of steps taken to contain the breach on the day the breach is discovered.

Supervisors and employees who discover potential breaches must:

- Take immediate action to contain the breach and to secure the affected records, systems, email or websites. Review the Preliminary Breach Assessment Report (Appendix 1) for suggested containment strategies.

Step 2: Full Assessment

Upon receipt of a notification of a potential privacy breach, the Privacy Officer must:

- Obtain a copy of the Preliminary Breach Assessment Report from the reporting employee (Appendix 1).
- Identify appropriate staff to form an Incident Response Team and organize an immediate meeting of the team.
- Identify breach containment strategies and assign responsibility for their implementation. Containment strategies should be identified and implemented on the day the breach is discovered.
- Conduct an investigation and complete the Privacy Breach Checklist including a risk assessment (Appendix 2). Conduct this step within one to five days of the breach.
- Based on the Privacy Breach Checklist and in consultation with the Incident Response Team, determine whether notification is appropriate and identify prevention strategies. Conduct this step within one to five days of the breach.
- Complete notification of affected individuals and notification of the Information and Privacy Commissioner. Conduct this step as soon as possible, generally within one to five days of the breach.

Step 3: Notification
The Incident Response Team, in consultation with the Privacy Officer, will determine whether and to whom notification will be given. Notification is an important mitigation strategy that can benefit both Saint Mary's University and the individuals affected by a breach. There are several individuals and organizations that may require notification:

(a) Internal officials: The Incident Response Team should identify appropriate officials within Saint Mary's University who require notification of the breach.

(b) Affected individuals: If a breach creates a risk of harm to any individuals, those affected should be notified. The Privacy Breach Checklist (Appendix 2) includes an assessment for whether notification should occur and how notification should be completed. The Privacy Breach Checklist also identifies the information that must be included in any breach notification letter.

(c) Office of the Information and Privacy Commissioner
If required, the Privacy Officer will notify the Office of the Information and Privacy Commissioner by phone, fax or email.

(d) Others
Appendix 2 includes a list of other organizations or individuals who may require notification depending on the facts of the breach. The Privacy Officer is responsible for implementing any notification decisions made by the Incident Response Team.

Caution: In responding to a privacy breach, be careful not to take steps that may exacerbate the existing breach or create a new one (i.e. disclosing additional personal information, notification letters addressed to the wrong person, notification letters that disclose information in the return address).

Step 4: Mitigation and Prevention
Once the immediate steps have been taken to mitigate the risks associated with the privacy breach and to provide appropriate notification, the Office of Primary Responsibility (the Office where the breach occurred), the Privacy Officer and the Incident Response Team must investigate the cause of the breach thoroughly, consider whether to develop a prevention plan and consider what that plan might include.

Mitigation and prevention strategies developed should reflect the significance of the breach and whether the breach was a systemic or isolated event. Mitigation and prevention plan may include the following:

Physical Controls
- Audit physical controls to identify outstanding weaknesses.
- Modify physical controls such as locks, alarms, security monitoring, or visitor access control to improve level of security.

Technical Controls

- Tighten restrictions on access to certain personal information based on roles, responsibilities and need to know.
- Encrypt personal information particularly on portable storage devices.
- Limit the ability to copy data to thumb drives.
- Limit access to non-work email.

Administrative Controls

- Review the enforcement of University policies, directives and process for the protection of personal information throughout its lifecycle.
- Revise or develop internal procedures and policies to address shortcomings identified.
- Develop contractual clauses to deal with breaches of privacy by third party service providers.

Personnel Security Controls

- Training and education
- Coaching/mentoring
- Disciplinary actions (reprimands, suspension, reassignment, termination)
- Revoke privileges and/or user access to system or records

Step 5: Lessons Learned

The Privacy Officer will track all privacy breaches across the organization and will use that information to identify trends both in the types of breaches occurring and within each step of the privacy breach management process. Collecting this information can facilitate identifying underlying patters with respect to personal information handling practices and may prevent future breaches.

Appendix 1: Preliminary Privacy Breach Assessment Report		
Report Prepared by: **Email:** **Phone:**		**Date:**
A. Breach Identification and Containment		
Instructions: Review the preliminary assessment list below. If you answer yes to any of the questions below, complete the remainder of this assessment report and immediately (same day) forward a copy of this report to the Privacy Officer.		
Preliminary Assessment	**Yes/ No**	**Suggested Containment Strategies**
1. Was there an abuse of access privileges (e.g. unauthorized access or use of records that contain personal information)?		a) Immediately restrict, suspend, or revoke access privileges until completion of the investigation. b) Determine whether personal information was further disclosed to others (verbally or via copies). c) Attempt to retrieve the documents in question, and document the steps taken. d) Complete this *Preliminary Report* and contact the Privacy Officer.
2. Was personal information inappropriately disclosed (e.g. improper application of severances (material removed or blacked out), incomplete de-identification)?		a) Attempt to retrieve documents. b) Determine whether personal information was further disclosed to others (verbally or via copies). c) Document the steps taken. d) Complete this *Preliminary Report* and contact the Privacy Officer.
3. Was personal information lost (e.g., through the mail, during a move or on a misplaced electronic device)?		a) Attempt to retrace steps and find the lost document(s). b) Determine whether personal information was further disclosed to others (verbally or via copies). c) Document the steps taken. d) Conduct an inventory of the personal information that was or may have been compromised. e) Complete this *Preliminary Report* and contact the Privacy Officer.

Preliminary Assessment	Yes/ No	Suggested Containment Strategies
4. Was personal information stolen (e.g. theft of computer equipment or devices)?		a) Attempt to retrieve the stolen equipment or device. b) Document the steps taken. c) Complete this *Preliminary Report* and contact the Privacy Officer.
5. Was personal information in an unencrypted email sent to the wrong address?		a) Cease transmission of email or correspondence to the incorrect address. b) Determine whether the email address is incorrect in the system (e.g. programmed incorrectly into the system). c) Attempt to recall the message. d) Determine where the email went. e) Request that the recipient delete all affected email or correspondence, with confirmation via email that this has been done. f) Determine whether personal information was further disclosed to others (verbally or via copies). g) Document the steps taken. h) Complete this *Preliminary Report* and contact the Privacy Officer.
6. Was personal information faxed, mailed, or delivered to a wrong address?		a) Determine where the document went. b) Determine whether the address is incorrect in the system (e.g. programmed incorrectly into system). c) Request that the recipient return the document(s) if mailed, or request that the fax be destroyed, with confirmation that this has been done. d) Determine whether personal information was further disclosed to others (verbally or via copies). e) Document the steps taken. f) Complete this Preliminary Report and contact the Privacy Officer.
7. Did a third party compromise (hack into) a system that contains personal information?		a) Contact security and IT to isolate the affected system, disable the affected system, or disable the user account to permit a complete assessment of the breach and resolve vulnerabilities. b) Document the steps taken.

Preliminary Assessment	Yes/ No	Suggested Containment Strategies
		c) Complete this *Preliminary Report* and contact the Privacy Officer.
8. Did the sale or disposal of equipment or devices that contain personal information occur without a complete and irreversible purging of the item before its sale or disposal?		a) Contact IT. b) Document the steps taken. c) Complete this *Preliminary Report* and contact the Privacy Officer.
9. Was there an inappropriate display of personal information clearly visible to employees or clients? (e.g. posting of medical appointments or types of leave, home telephone numbers, slides of PowerPoint presentations that contain personal information, etc.)?		a) Remove, move or segregate exposed information or files. b) Preserve evidence. c) Determine whether personal information was further disclosed to others (verbally or via copies). d) Document the steps taken. e) Complete this *Preliminary Report* and contact the Privacy Officer.
10. Was there an inappropriate collection of personal information?		a) Determine whether personal information was further disclosed to others (verbally or via copies). b) Complete this *Preliminary Report* and contact the Privacy Officer.
11. Was there an unexpected or unintended use of collected data? Is there a risk for re-identification of an affected individual or another identifiable individual?		a) Determine whether personal information was further disclosed to others (verbally or via copies) b) Complete this *Preliminary Report* and contact the Privacy Officer.
12. Was there an improper or unauthorized creation of personal information?		a) Complete this *Preliminary Report* and contact the Privacy Officer.

Preliminary Assessment	Yes/ No	Suggested Containment Strategies
13. Was there an improper or unauthorized retention of personal information?		a) Complete this *Preliminary Report* and contact the Privacy Officer.
14. Remarks/Other:		

B. Breach Details		
1. Date(s) of breach:	2. Time of breach:	3. Location of breach:
4. When and how was the breach discovered?		
5. Provide a brief description of the breach (what happened, how it happened, etc.):		
6. Identify the person whose information was compromised (name and personal record identifiers, if applicable). If information regarding more than one person was compromised, please attach a list.		7. Is/are the affected individual(s) aware of the breach? __ Yes __ No
8. Format of information involved: ____ Electronic records ____ Paper records ____ Other (describe): _____	9. What information was involved (check all that apply): ____ Medical _____ Employee ____ Other (describe): _____	
10. List the immediate containment actions and/or interventions, if any:		

11. Is there information or evidence to support the allegation of the breach? If yes, please specify:		
12. Has your supervisor been notified of the breach? __ Yes __ No		
C. Please name the person(s) directly involved in this breach (witnesses, investigator, individual who may have caused the breach, victims, etc.). Attach a list if necessary.		
1. Name	Title/Position	Contact information:
2. How was this person involved?		
3. Name	Title/Position	Contact information:
4. How was this person involved?		

Send this form immediately to University Privacy Officer: privacy@smu.ca, phone 902-491-6565.

Appendix 2: Privacy Breach Checklist

Use this checklist to evaluate your response to a privacy breach and to decide whether to report the breach to the Office of the Information and Privacy Commissioner.[1] For a further explanation of how to manage a privacy breach see *Key Steps to Responding to Privacy Breaches* available at: https://oipc.novascotia.ca.

Date of report: _____

Date breach initially discovered: _____

Contact information:

Public Body/Health Custodian/Municipality:

_____

Contact Person (Report Author):

_____

Title: _____

Phone: _____ Fax: _____

E-Mail: _____

Mailing Address: _____

Incident Description

Describe the nature of the breach and its cause. How was the breach discovered and when? Where did it occur?

_____

_____

_____

_____

Steps 1 & 2: Containment & Risk Evaluation

Answer each of the following questions and then, based on those answers, complete the risk evaluation summary on page 15.

[1] The OIPC can be reached by phone at 902-424-4684 or 1-866-243-1564, by fax at (902) 424-8303 and by email at oipcns@novascotia.ca.

(1) Containment

Check all the factors that apply:

- ❑ The personal information has been recovered and all copies are now in our custody and control.
- ❑ We have confirmation that no copies have been made.
- ❑ We have confirmation that the personal information has been destroyed.
- ❑ We believe (but do not have confirmation) that the personal information has been destroyed.
- ❑ The personal information is encrypted.
- ❑ The personal information is not encrypted.
- ❑ Evidence gathered so far suggests that the incident was likely a result of a systemic problem.
- ❑ Evidence gathered so far suggests that the incident was likely an isolated incident.
- ❑ The personal information has not been recovered but the following containment steps have been taken (check all that apply):
    - ❑ The immediate neighbourhood around the theft has been thoroughly searched.
    - ❑ Used item websites are being monitored but the item has not appeared so far.
    - ❑ Pawn shops are being monitored.
    - ❑ A remote wipe signal has been sent to the device but no confirmation that the signal was successful has been received.
    - ❑ A remote wipe signal has been sent to the device and we have confirmation that the signal was successful.
    - ❑ Our audit confirms that no one has accessed the content of the portable storage device.
    - ❑ We do not have an audit that confirms that no one has accessed the content of the portable storage device.
    - ❑ All passwords and system user names have been changed.

Describe any other containment strategies used:

_____

_____

_____

_____

(2) Nature of Personal Information Involved

List all of the data elements involved (e.g. name, date of birth, SIN, address, medical diagnoses, connection with identified service provider such as welfare or counselling etc.)

- ❑ Name
- ❑ Address
- ❑ Date of birth
- ❑ Government ID number (specify) _____
- ❑ SIN
- ❑ Financial information
- ❑ Medical information
- ❑ Personal characteristics such as race, religion, sexual orientation
- ❑ Other (describe)

_____

_____

(3) Relationship

What is the relationship between the recipient of the information and the individuals affected by the breach?

- ❑ Stranger
- ❑ Friend
- ❑ Neighbour
- ❑ Ex-partner
- ❑ Co-worker
- ❑ Unknown
- ❑ Other (describe)

_____

_____

_____

_____

(4) Cause of the Breach

Based on your initial investigation of the breach, what is your best initial evaluation of the cause of the breach?

- ❑ Accident or oversight
- ❑ Technical error
- ❑ Intentional theft or wrongdoing
- ❑ Unauthorized browsing
- ❑ Unknown
- ❑ Other (describe)

_____
_____
_____

(5) Scope of the Breach

How many people were affected by the breach?

- ❑ Very few (less than 10)
- ❑ Identified and limited group (>10 and <50)
- ❑ Large number of individuals affected (>50)
- ❑ Numbers are not known

(6) Foreseeable Harm

Identify the types of harm that may result from the breach. Some relate strictly to the affected individual; but harm may also be caused to the public body and other individuals if notifications do not occur:

- ❑ **Identify theft** (most likely when the breach includes loss of SIN, credit card numbers, driver's licence numbers, debit card information etc.)
- ❑ **Physical harm** (when the information places any individual at risk of physical harm from stalking or harassment)
- ❑ **Hurt, humiliation, damage to reputation** (associated with the loss of information such as mental health records, medical records, disciplinary records)
- ❑ **Loss of business or employment opportunities** (usually because of damage to reputation to an individual)
- ❑ **Breach of contractual obligations** (contractual provisions may require notification of third parties in the case of a data loss or privacy breach)
- ❑ **Future breaches due to technical failures** (notification to the manufacturer may be necessary if a recall is warranted and/or to prevent a future breach by other users)
- ❑ **Failure to meet professional standards or certification standards** (notification may be required to a professional regulatory body or certification authority)
- ❑ **Other** (specify)

_____

(7) Other Factors

The nature of the public body's relationship with the affected individuals may be such that the public body wishes to notify no matter what the other factors are because of the importance of preserving trust in the relationship. Consider the type of individuals that were affected by the breach.

- ❑ Client/customer/patient
- ❑ Employee
- ❑ Student or volunteer
- ❑ Other (describe)

_____

Risk Evaluation Summary:

For each of the factors reviewed above, determine the risk rating.

Risk Factor	**Risk Rating**		
	Low	Medium	High
1) Containment			
2) Nature of the personal information			
3) Relationship			
4) Cause of the breach			
5) Scope of the breach			
6) Foreseeable harm from the breach			
7) Other factors			
Overall Risk Rating			

Use the risk rating to help decide whether notification is necessary and to design your prevention strategies. Foreseeable harm from the breach is usually the key factor used in deciding whether to notify affected individuals. Step 3 below analyzes this in more detail. In general, though, a medium or high-risk rating will always result in notification to the affected individuals. A low-risk rating may also result in notification depending on the unique circumstances of each case.

Step 3: Notification

(1) Should affected Individuals be Notified?

Once you have completed your overall risk rating, determine whether notification of affected individuals is required. If any of the following factors apply, notification should occur. If the *PHIA* test is satisfied, notification must occur.

Consideration	Description	Factor applies
Legislation	Health custodians in Nova Scotia must comply with sections 69 & 70 of *PHIA* which require notification.	
Risk of identity theft	Most likely when the breach includes loss of SIN, credit card number, driver's licence number, debit card information, etc.	
Risk of physical harm	When the information places any individual at risk of physical harm from stalking or harassment.	
Risk of hurt, humiliation, damage to reputation	Often associated with the loss of information such as mental health records, medical records or disciplinary records.	
Loss of business or employment opportunities	Where the breach could affect the business reputation of an individual.	
Explanation required	The public body may wish to notify if the affected individuals include vulnerable individuals, or where individuals require information to fully understand the events, even when the risks have been assessed as low.	
Reputation of public body	Where the public body is concerned that the breach will undermine trust of citizens, the public body may decide to notify to ease concerns and to provide clear information regarding the risks and mitigation strategies undertaken, even when risks assessed are low.	

(2) When and How to Notify

When: Notification should occur as soon as possible following a breach. However, if you have contacted law-enforcement authorities, you should determine from those authorities whether notification should be delayed in order not to impede a criminal investigation.

How: The preferred method is direct – by phone, letter, email or in person. Indirect notification via website information, posted notices or media should generally only occur where direct notification could cause further harm, is prohibitive in cost, or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach.

Considerations Favouring <u>Direct</u> Notification	Check If Applicable
The identities of individuals are known	
Current contact information for the affected individuals is available	
Individuals affected by the breach require detailed information in order to properly protect themselves from the harm arising from the breach	

Individuals affected by the breach may have difficulty understanding an indirect notification (due to mental capacity, age, language, etc.)	
Considerations Favouring <u>Indirect</u> Notification	
A very large number of individuals are affected by the breach, such that direct notification could be impractical	
Direct notification could compound the harm to the individuals resulting from the breach	

(3) What to Include in Breach Notification Letters

The information included in the notice should help the individual to reduce or prevent the harm that could be caused by the breach. Include all the information set out below:

Essential Elements in Breach Notification Letters	Included
Date of breach	
Description of breach	
Description of personal information affected	
Steps taken so far to control or reduce harm (containment)	
Future steps planned to prevent further privacy breaches	
Steps individuals can take - consider offering credit monitoring where appropriate	
Information and Privacy Commissioner's contact information – Individuals have a right to complain to the Information and Privacy Commissioner	
Public body, municipality or health custodian contact information – for further assistance	

(4) Others to Contact

Authority or Organization	Reason for Contact	Applicable
Law-enforcement	If theft or crime is suspected	
Information and Privacy Commissioner for Nova Scotia	• For assistance with developing a procedure for responding to the breach, including notification to ensure steps taken comply with obligations under privacy legislation • The personal information is sensitive • There is a risk of identity theft or other significant harm • A large number of people are affected • The information has not been fully recovered	

	• The breach is a result of a systemic problem or a similar breach has occurred before	
Professional or regulatory bodies	If professional or regulatory standards require notification of the regulatory or professional body	
Insurers	Where required in accordance with an insurance policy	
Technology suppliers	If the breach was due to a technical failure and a recall or technical fix is required	

Confirm notifications completed c

Key contact	**Notified**
Privacy officer within your public body, municipality or health custodian	
Police (as required)	
Affected individuals	
Information and Privacy Commissioner for Nova Scotia	
Professional or regulatory body – identify:	
Technology suppliers	
Others (list):	

Step 4: Prevention

Once the immediate steps are taken to mitigate the risks associated with the breach, you need to take the time to thoroughly investigate the cause of the breach. This could require a security audit of both physical and technical security. As a result of this evaluation, you should develop or improve as necessary adequate long-term safeguards against future breaches.

Consider making improvements in each of the following areas listed below. Also, take the opportunity to revisit your privacy management framework,[2] and assess if any further adjustments are necessary as part of your prevention strategy.

[2] For information on what constitutes a privacy management framework visit the tools tab on the Office of the Information and Privacy Commissioner website at: https://oipc.novascotia.ca.

Physical Controls
What physical controls were in place at the time of the breach? Describe any modifications to physical controls such as locks, alarms, security monitoring, or visitor access control.

Technical Controls
Was there an IT security strategy in place at the time of the breach? Describe any modification to technical controls intended to prevent future similar breaches.

Administrative Controls
Administrative controls refer to the procedural safeguards implemented for safe handling of personal information, which includes the enforcement of an institution's policies, directives and processes for the protection of personal information throughout its lifecycle. Describe the administrative controls in place at the time of the breach. Describe improvements made to administrative controls in response to the breach. If you do not already have a privacy breach protocol in place, ensure that one is developed as part of your plan.

Personnel Security Controls
Personnel security controls refer to a public body's (or health custodian's) management of its employees – suitability, proper training, supervision, and disciplinary procedures. What personnel security controls were in place at the time of the breach - for example, security clearances, confidentiality agreements and privacy training requirements? What steps have been taken to improve personnel security controls in this particular case and in general to prevent future similar breaches?