

Reporting Suspected or Confirmed Privacy Breaches

Consult Procedure for Reporting Privacy Breaches before completing this form.

Contact the Office of General Counsel at: privacy@sheridancollege.ca or 905-845-9430 x 2872

Ensure that the necessary details of the incident and any corrective actions are documented in **Steps 1 to 3** below, to aid in investigation and corrective action (Step 4) by the Office of General Counsel.

General Information

Name and title of unit manager in charge of assessment and investigation:

Date of incident:

Location of incident:

When and how the incident was discovered:

What happened (brief description):

Step 1: Contain

Have the records concerned been retrieved or access to them stopped? Yes No

Can you confirm that no copies have been made or retained by the individual(s) concerned who were not authorized to receive the information? Yes No

Provide contact information for individual receiving unauthorized information (for any required follow-up action – if more than one individual, attach details in separate sheet)

Name: Phone: Email:

Address:

If a system was breached, date the system was shut down:

Computer access codes or authorizations revoked or changed on:

Identify and describe any weaknesses in physical or Electronic security:

Corrective Actions Recommended:

Step 2: Assess the Risks

Personal Information

Sheridan

What personal information was involved?
List the data elements:

Format of records:

Was information encrypted, anonymized or otherwise not easily accessible? Yes No

Describe the physical or technical security measures in place at the time of the breach:

Sensitivity of the personal information: High Medium Low

In general, the more sensitive the personal information, the greater the harm to individuals from a privacy breach.
High* e.g. health, financial, student or employment information, especially in combination
Medium* e.g. opinion material
Low* e.g. name and address only *Note these are general examples only; content also determines sensitivity

Cause and extent of the breach

Cause of breach:

Risk of ongoing or further exposure of the information: High Medium Low

Is this breach: an isolated incident the result of a systemic problem

Describe the incident:

Number of individuals whose personal information is affected by the breach:

Affected individuals or groups: students employees external others –describe:

Foreseeable harm

Is there foreseeable harm from the breach: Yes No I don't know

If yes, what harm could result from the breach? Check one or more below.

Harm to Individuals:

Risk to physical security financial loss identity theft damage to reputation/relationship

Other – describe:

Harm to Sheridan

Loss of trust in institution Damage to Sheridan reputation Financial losses or exposure

Legal proceedings Other – describe:

Harm to Public

Risk to public health Risk to public safety Other - describe:

Sheridan

Step 3: Notify Affected Individuals

Depending on the circumstances, notifications could include some of all of the following – See the **Procedure for Reporting Privacy Breaches** for details:

Have all affected individuals been notified as to:

| | | |
|--|-----|----|
| Description of breach | Yes | No |
| The specifics of the information inappropriately accessed, collected, used or disclosed | Yes | No |
| Steps taken so far to address the breach | Yes | No |
| Future steps planned to prevent further privacy breaches | Yes | No |
| Additional information, if required, about how individuals can protect themselves | Yes | No |
| Contact information for individual (include position title) within Sheridan to answer questions or provide further information | Yes | No |

Date(s) of notification:

Form of notification: letter in person telephone email other – describe:

If all affected individuals have not been notified, please explain:

Report completed by (name, unit, position title):

Date:

Send completed Privacy Breach Report Form by email to privacy@sheridancollege.ca (pdf). If sending by email, save this form with a new name and attach it to email; or by mail to the Office of General Counsel at 1430 Trafalgar Road, Oakville, ON, L6H 2L1.

NOTE: Limit distribution of the completed Privacy Breach Report Form to only those individuals who need to be informed about the incident as part of their duties and responsibilities.

Step 4: Investigate and Correct

For Office of General Counsel use only.