Breach of Personal Information Reporting Procedure

This procedure is governed by its parent policy. Questions regarding this procedure are to be directed to the identified Procedure Administrator.

Functional category	Operations
Parent policy	*Freedom of Information and Protection of Privacy* (FOIP) *Act* Policy
Approval date	March 24, 2022
Effective date	March 24, 2022
Procedure owner	Vice President, Administration and Chief Financial Officer
Procedure administrator	Director, Information, Risk and Compliance

Overview

NorQuest College (college) has an obligation to collect, use, and disclose personal information for purposes that facilitate achieving its mandate and complying with law. The college also has an obligation to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or destruction.[1]

This procedure outlines expectations and required actions by members of the college community regarding breaches of personal information, the

[1] FOIP Act, s.38

protection of privacy, and the college's duties as defined by the Alberta *Freedom of Information and Protection of Privacy* (FOIP) *Act.*

Authority to establish this procedure is derived from the NorQuest College Board of Governor's Policy No. 5, which delegates authority to the President and CEO to establish policies and procedures for the college's management and operation.

Procedure

A privacy breach occurs when there is a contravention of the FOIP Act through an unauthorized access to or collection, use, disclosure or disposal of personal information. Four steps will be taken to respond to a privacy breach: containment, evaluation, notification, and prevention.

All college employees are required to follow the Privacy Breach Reporting Procedure in the event of a breach involving personal information. Employees must contact Compliance immediately if they suspect that a privacy breach has occurred.

Identifying a Breach

There are six main types of breaches:

- **Human Error - Accidental Disclosure** (i.e. misdirected email)
- **Human Error - Accidental Loss** (i.e. loss of physical devices or paper containing personal information)
- **Theft** (i.e. stolen physical devices or paper containing personal information)
- **Malicious** (i.e. unauthorized access by malicious actor(s)
- **Data Leak** (i.e. breach of College Policy, and/or Procedure, and/or BTS Standard)
- **Technical** (i.e. untraceable technical error)

When a breach of personal information is suspected the employee involved and/or the employee reporting the breach (for example, the employee who discovered the breach) will work with the Compliance Office as outlined in

this procedure. If Compliance determines a breach of personal information did not occur, they will notify the business area in writing of the findings.

1. Containment

In the event of a breach or suspected breach involving personal information occurs:

A. Immediate containment of the record(s) must swiftly be undertaken. This includes recalling internal email messages and notifying all recipients:
   - that they received it in error,
   - to advise not to open and/or distribute the record, and
   - to destroy the information including from their downloaded files and recycle bin.

B. The employee responsible for the custody and control of the information at the time of the breach must preserve a copy of the evidence of the breach and notify Compliance within one working day after becoming aware of the incident. If the incident is not reported within one working day, a reason for the delay must be communicated to the Compliance Office.

C. Compliance will then initiate the Privacy Breach Reporting Process, as outlined in the reporting form, within two working days upon receipt of notification of the incident to the compliance@norquest.ca inbox.

2. Evaluation

The breach will be evaluated through the information supplied by the business area and/or via the Privacy Breach Reporting Form to determine if the event requires notification to internal and/or external stakeholders. The evaluation process is independent and will be led by the Compliance Office, to determine if a breach of personal information occurred under the FOIP Act. This can include gathering digital evidence directly from the Business Technology Services (BTS) division. Evaluation will include determining the number of affected individuals, if notification to external regulatory bodies will be required, the intentional or unintentional nature of the breach, and overall risk.

3. Notification

The business area, or the Compliance Office if the breach is large in scope and overall risk, must notify the affected individual(s) of the breach as soon

as possible from the date the breach was discovered. Notification should include:

- a description of what happened;
- what information was involved;
- what is being done to prevent a similar breach in the future;
- what the affected individual(s) can do (i.e., changing their passwords), if possible; to mitigate the likelihood of the risk; and
- who to contact for more information (i.e., Compliance Office).

4. Prevention

A. Once the Privacy Breach Reporting Form is returned to the employee reporting the incident, it must be signed by all required parties and returned to Compliance@norquest.ca as soon as possible from the time the original form was sent to the business area by Compliance.
B. The business area responsible for the breach must also undertake and implement any required physical, technical, and/or administrative safeguards as recommended by the Compliance Office in the Privacy Breach Reporting Form.
C. Compliance will follow-up with the business area three months after the close of the breach for a status update on required changes to improve safeguards.

Protection of Privacy Obligations

All employees are expected to be aware of and uphold their obligations under the FOIP Act as reflected in college policy, procedure, and Digital Security standards.

In keeping with the Code of Conduct Policy, a malicious breach, data leak, and/or repeated breach offences under the FOIP Act could result in disciplinary action up to and including termination of an employee's employment, or of the relationship of a board member with NorQuest. In these circumstances, Compliance will provide the signed Privacy Breach Reporting Form to People and Culture to review and determine if an investigation under the college Code of Conduct Policy or Respectful Workplace and Learning Environment Policy is warranted.

Legislative Compliance

Senior management that have been identified as a Legislative Owner, as per the Legislative Compliance Reporting Procedure, are responsible for being aware of and reporting breaches under FOIP within their business area when completing their annual Legislative Certificates for the FOIP Act and Regulation.

Definitions

Employee: under the FOIP Act and for the purposes of this procedure, an employee includes a person who performs a service for the college as an appointee, volunteer, or student or under a contract or agency relationship with the college.

Personal Information: means recorded information about an identifiable individual, including:

- the individual's name, home address, and/or home telephone number;
- the individual's business address and/or business telephone number*;
- the individual's race, national or ethnic origin, colour, or religious or political beliefs, or associations;
- the individual's age, sex, marital status, or family status;
- an identifying number, symbol, or other particular assigned to the individual;
- the individual's fingerprints, other biometric information, blood type, genetic information, or inheritable characteristics;
- information about the individual's health and health care history, including information about a physical or mental disability;
- information about the individual's educational, financial, employment, or criminal history, including criminal records where a pardon has been given;
- anyone else's opinions about the individual; and
- the individual's personal views or opinions, except if they are about someone else.

*Note: Business contact information is a type of personal information that is routinely disclosed in a business or professional context. The disclosure of

business contact information, in and of itself, is not usually an unreasonable invasion of privacy as per section 40(1)(bb.1) of the FOIP Act.

Privacy Breach (breach): means a loss of, unauthorized access to, or unauthorized disclosure of personal information.[2]

Related information

NorQuest College

- Access to Information Procedure
- Code of Conduct & Respectful Workplace & & Learning Environment Complaints & Investigation Procedure
- Code of Conduct Policy
- Digital Security Policy
- Digital Security Standards and Procedures
- *Freedom of Information and Protection of Privacy* (FOIP) *Act* Policy
- Legislative Compliance Reporting Procedure
- Privacy Breach Reporting Form

External

- *Freedom of Information and Protection of Privacy Act*
- *Freedom of Information and Protection of Privacy Regulation*
- Office of the Information and Privacy Commissioner of Alberta

Next review date

Month 2026

[2] From www.oipc.ab.ca.

Revision history

Date	Version Number	Action
March 2022	V1	New
January 2024	V2	Information, Risk & Compliance template & reorganization update