

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY (FOIP) ACT POLICY

This document is the parent policy for any college or divisional procedures. Questions regarding this policy are to be directed to the identified Policy Administrator.

Functional Category:	Operations
Approval Date:	March 23, 2022
Effective Date:	March 23, 2022
Policy Owner:	Vice President, Administration and Chief Financial Officer
Policy Administrator:	Manager, Compliance

Objective:

This policy governs the development, implementation, and review of NorQuest College's (college) legislative obligations under the *Freedom of Information and Protection of Privacy (FOIP) Act* for all information in its custody and control. NorQuest College is legislatively required to adhere to the FOIP Act and all members of the college community must comply with the college's responsibilities under the Act.

Authority to establish this policy 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.

Policy:

Purpose

This policy is to support the five purposes of the FOIP Act in saying that NorQuest will:

- (a) allow any person a right of access to records in the custody or under the control of the college subject to limited and specific exceptions as set out in the FOIP Act,
- (b) control the manner in which the college may collect, use, and disclose personal information,
- (c) allow individuals, subject to limited and specific exceptions as set out the FOIP Act, a right of access to personal information about themselves held by the college,
- (d) allow individuals a right to request corrections to personal information about themselves that is held by the college, and
- (e) refer to the independent review process of decisions made by the college under the FOIP Act and the resolution of complaints.

Compliance with the FOIP Act

All NorQuest College employees have the responsibility to protect against the unauthorized access, collection, use, disclosure, or destruction of personal information.

Employees can demonstrate compliance with the FOIP Act by providing information through routine disclosure where possible, always protecting the personal information in the custody and control of the college, and assisting the Compliance Office in the college duty to accurately and completely respond to any FOIP Request to Access Information.

All college employees must understand and comply with the FOIP Act and shall not:

- Access or use personal information that is outside your area of responsibility;

- Destroy official records that have not met their retention periods within the Records Retention and Disposition Schedule;
- Disclose personal information to a third party without proper authorization;
- Avoid participating in the processing of a FOIP Request to access information when required to do so as directed by the Compliance Office.

Delegation Authority

The power to delegate authority to make decisions under the FOIP Act falls to the head of the public body. The President and CEO of NorQuest College as the head of the public body, and as decided upon in the NorQuest Delegation Authority Matrix, has the delegation authority.

Non-Compliance

Non-compliance with this policy, as supported by the Act, may result in disciplinary action and/or penalties as per section 92 of the FOIP Act.

Violations: 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.

Employees are responsible for adherence to the FOIP Act and for following the requirements within the *Freedom of Information and Protection of Privacy (FOIP) Act* Policy and its related procedures. Violations may result in individual disciplinary penalties up to and including termination.

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 a board member's relationship with NorQuest. In these circumstances, the Compliance Office 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 Procedure is warranted.

Training

Upon commencement of employment with the college, staff must successfully complete the Compliance FOIP Fundamentals online course. The course must then be repeated on a two-year refresher cycle or as required by Compliance as a mitigation measure in response to a breach of personal information under the FOIP Act. FOIP Training progress will be administered and tracked by the college.

Definitions:

Applicant: is the person who submits a formal Access to Information Request. The right of access extends to all persons this includes students, employees, and members of the public.

College community: any student, faculty, administrative or staff member of the college, member of the public serving in a recognized capacity for the college, guardian of an underage student acting on behalf of the student in the college community, and employee of an agency contracted by the college.

Compliance Office: office responsible for providing overall support for the coordination and maintenance of the college's policies and

procedures. Compliance provides direct support throughout the design, implementation, maintenance and retirement of all college policies and procedures.

Delegation: the formal process whereby the head of a public body authorizes an employee or officer within the public body to perform certain duties or to exercise certain powers or functions of the head under the Act. A delegation under the Act must be in writing. The formal process whereby the head of a public body authorizes an employee or officer within the public body to perform certain duties or to exercise certain powers or functions of the head under the Act. A delegation under the Act must be in writing.

Employee: under the FOIP Act and for the purposes of this policy, 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.¹

Record: recorded information created, received, and maintained by an organization or individual in pursuance of its legal obligations or in the transaction of business. Means a record of information in any form and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or

¹ From www.oipc.ab.ca.

stored in any manner, but does not include software or any mechanism that produced records.

Routine Disclosure: means allowing access to records that do not contain personal information outside of a formal Access to Information Request.

Related NorQuest College Information:

- [Access to Information Procedure](#)
- [Code of Conduct & Respectful Workplace & Learning Environment Complaints & Investigation Procedure](#)
- [Code of Conduct Policy](#)
- [Digital Security Policy](#)
- [FOIP Request to Access Information form](#)
- [NorQuest College Delegation Matrix](#)
- [Physical Records Disposition Procedure](#)
- [Privacy Breach Reporting Procedure](#)
- [Protection of Privacy Procedure](#)
- [Records and Information Management Policy](#)
- [Records Retention and Disposition Schedule](#)

Related External Information:

- [Freedom of Information and Protection of Privacy Act](#)
- [Freedom of Information and Protection of Privacy Regulation](#)
- [Post-Secondary Learning Act](#)

Next Review Date:

January 2026

Revision History:

March 2018: policy drafted and approved
 August 2019: Compliance Office template & reorganization update
 March 2022: reviewed and updated as per the Policy and Procedure Framework Procedure