PROTECTION OF PRIVACY 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:	Manager, 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 the actions required by and expectations of members of the college community regarding protection of privacy as defined by the Alberta *Freedom of Information and Protection of Privacy* (FOIP) *Act* and Regulation.

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.

Procedures:

Each division in the college is to manage operations in a manner that fulfills the following:

Collection of Personal Information

Collection of personal information will only occur where[2]:

- the collection is expressly authorized by an enactment of Alberta or Canada;
- the information is collected for the purposes of law enforcement; or
- that information relates directly to and is necessary for an operating program or activity of the college.

Documents used to collect personal information directly from an individual the information is about will all contain a FOIP notification statement that includes the following information:

- the purpose for which the information is collected;
- the specific legal authority for the collection; and
- the title, business address, and business telephone of the college employee who can answer the individual's questions about the collection[3].

All FOIP notification statements are to be approved by Compliance prior to use. For all new collections of personal information,

[1] FOIP Act, s.38
[2] FOIP Act, s.33
[3] FOIP Act, s.34(2)

Compliance can assist in drafting a succinct and legally defensible notification statement.

Correction of Personal Information
When collecting personal information, every reasonable effort is to be made to ensure that personal information collected is directly from the individual, and is accurate and complete[4].

An individual who believes that there is an error or omission in their personal information may request that the college correct the information[5]. This may be done by:

- Providing evidence of the error and outlining the correction required by submitting a completed Request to Correct Personal Information Form; or
- Requesting a correction to an opinion by way of an annotation or by linking the correction to that part of the record that is relevant.

The divisional head responsible for the record that collected the personal information will take action to correct any error and respond in writing within 30 days of the request for correction to the individual indicating that either[6]:

- the correction has been made, or
- an annotation or linkage has been made.

Use of Personal Information
Personal information will only be used:

- for the purpose for which it was collected, or for a use consistent with that purpose; or
- where the individual the information is about has identified the information and consented in writing to the specified use.

The college will only use personal information to the extent necessary, to enable the college to carry out its purpose in a reasonable manner[7].

Personal information of an individual that is used to make a decision that directly affects that individual will be retained for at least one year after using it[8].

Disclosure of Personal Information
Personal information will only be disclosed[9]:

- for responding to an access request for personal information regarding the person making the request as per the Access to Information Procedure;
- for the purpose of complying with an enactment of Alberta or Canada that authorizes or requires the disclosure;
- for the purpose for which the information was collected or a use consistent with that purpose;

[4] FOIP Act, s.35(a)
[5] FOIP Act, s.36(1)
[6] FOIP Act, s.36(7)
[7] FOIP Act, s.39(4)
[8] FOIP Act, s.35(b)
[9] FOIP Act, ss.40(1), (2), and (3)

- to an officer or employee of the college where the information is necessary for the performance of the duties of that person;
- where the individual the information is about has identified the information and consented in writing to the disclosure;
- for the purpose of complying with a court order having jurisdiction in Alberta; or
- for a purpose, not listed above for which that information may be disclosed under sections 40, 42, or 43 of the FOIP Act.

Employees who are collecting personal information or who have been provided access to personal information that has been collected will ensure that the personal information is kept confidential and may only disclose that personal information to other employees of the college who require the information in order to perform the duties of the position to which they were hired. The personal information that can be shared is limited only to that component of the personal information that is necessary for performing the job duties.

Consent

Informed and meaningful consent by an individual to use or disclose personal information that was collected for a purpose other than for which it was collected must specify:

- to whom the personal information may be disclosed;
- how the personal information may be used; and
- must be signed by the person who is giving consent.

The college requires consent in writing. However, in certain exceptional circumstances, consent may be received orally or electronically.

When consent to use or disclose personal information is sought by the college, NorQuest College will accept informed consent in an electronic form as long as it meets the following prerequisites:

- a record of consent will be retained as per the NorQuest College Records Retention and Disposition Schedule;
- it will be made accessible for future reference and use;
- it includes a NorQuest approved electronic signature to authentically identify the user; and
- meets section 7(5) of the FOIP Regulation.

Both the electronic signature and consent in electronic form must comply with NorQuest College's Digital Security and Business Technology Services policies and standards.

When consent to use or disclose personal information is sought by the college, NorQuest College will accept informed consent in an oral form as long as it meets the following prerequisites:

- a record of the consent will be created;
- it will be retained as per the NorQuest College Records Retention and Disposition Schedule;
- it will be made accessible for future reference and use;
- it will reliably authenticate the identity of the user; and
- meets section 7(6) of the FOIP Regulation.

Records Management
All records are to be managed in accordance with the NorQuest College Records Retention and Disposition Schedule, Records and Information Management Policy, and Records Management procedures.

Physical Records
Personal information collected and/or used by divisions must be stored in locations that provide reasonable safeguards against unauthorized access.

Electronic Records
Personal information access and use is subject to procedures established by the college that limit access to records to only those individuals that require access in order to perform their jobs.

Privacy Impact Assessments
A Privacy Impact Assessment (PIA) is a process of analysis that helps to identify and address potential privacy risks that may occur in the operation of a new or redesigned project. The college PIA process is done through a **Privacy Assessment Tool (PAT),** available through the Compliance Office.

PATs should be completed when required by the Compliance Office for the handing or collection of personal information when:

1. Developing, or procuring any new technologies or systems; such as through the Software Acquisition Process (SAP).
2. Implementing system upgrades and/or utilizing new functions within existing technologies.
3. The information used is of a highly sensitive nature and the impact of breach would cause a real risk of significant harm.
4. The classification of the information is protected or higher as per the college Digital Security Data Classification Standard.

If a PAT is not required, based on the Compliance Office approved exemption criteria, the business area will be notified that an exemption has been granted.

Privacy Breaches
A privacy breach occurs when there is a contravention of the FOIP Act through an unauthorized access to or collection, use, or 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 Breach of Personal Information 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.

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

Definitions:

Custody: means where the college has physical possession.

Control: means where the college has the authority to manage the record.

Consistent Purpose: means a purpose that has a direct and reasonable connection to the original purpose.

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.[10]

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

Software Acquisition Process (SAP): process to request permission to a website or application.

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

Related NorQuest College Information:	• Access to Information Procedure • Code of Conduct Policy • Digital Security Policy • Digital Security Standards and Procedures • *Freedom of Information and Protection of Privacy* (FOIP) *Act* Policy • NorQuest College Retention and Disposition Schedule • PAT Exemption Criteria (contact Compliance) • Physical Records Disposition Procedure • Physical Records Transfer and Retrieval Procedure • Privacy Breach Reporting Form • Privacy Breach Reporting Procedure • Records and Information Management Policy • Request to Correct Personal Information Form
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:	February 2013: new August 2013: update for document links and branding November 2014: update for change in procedure owner and administrator and document links June 2017: update to wording and Owner/Administrator November 2018: update to Consent section August 2019: Compliance Office template & reorganization update March 2022: reviewed as per the Policy and Procedure Framework Procedure; update to reflect current processes