POLICY

University of Niagara Falls Canada

Policy Title:	**Privacy Protection and Access to Information Policy**
Policy Number:	**2602**

1. Purpose

The purpose of this Policy is to ensure that the University protects the privacy of its students, employees, contractors, alumni, donors, research participants, retirees, and other University personnel (subsequently referred to as 'members') whose personal information is in the University's custody or control and that it upholds applicable legislation governing the collection, use, and disclosure of personal information. The Policy outlines the principles and practices we will follow in protecting members' personal information. Our privacy commitment includes ensuring the accuracy, confidentiality, and security of our members' personal information and allowing our members to request access to, and correction of, their personal information.

2. Scope

2.1. UNF follows the guidelines set out in the Freedom of Information and Protection of Privacy Act, R.S.O. 1990 ('FIPPA') and the Personal Information Protection and Electronic Documents Act ('PIPEDA').

2.2. This policy applies to all information and records in the custody and/or under the control of the University.

2.3. This policy includes all records and information created by or received in connection with university-related business, whether in printed or electronic form.

2.4. This policy shall also be read in conjunction with other instruments that may, in certain circumstances, govern access to information and protection of privacy matters including collective agreements.

2.5. All employees of UNF are responsible for the protection of the privacy of members whose personal information is in the custody and/or under the control of the University.

3. Principles

University of Niagara Falls is guided by the following principles:

3.1. Accountability:

The University is responsible for personal information in its custody and/or under its control and has designated a Privacy Officer who is accountable for the organization's compliance with this policy.

3.2. Identifying Purposes and Consent:

- The University will identify to the individual(s) the authority and purposes for the collection and use of personal information at the time of collection, and the contact information of an employee who can answer questions about the collection.
- The University will obtain the individual's consent to the collection of sensitive personal information and personal information collected for the purpose of disclosure outside the University.
- The University will collect personal information directly from the subject of the information whenever it is feasible and appropriate to do so. When direct collection is not feasible or appropriate, the University will make every reasonable effort to ensure the accuracy of personal information collected from third parties.

3.3. Limiting Collection:

- The University will limit its collection of personal information to that which is required for its programs and services in accordance with the applicable privacy legislation. Wherever feasible and appropriate, the University will collect personal information about members directly from the individual involved.
- A Privacy Notice will be provided to individual(s) at the time of record or information collection.

3.4. Limiting Use, Disclosure, and Retention:

- The University will use personal information only for the purpose for which it was collected or compiled in accordance with the applicable privacy legislation for a consistent purpose and with the written consent of the individual, or for the purpose for which the information was disclosed to the University.
- Employees of the University will collect and use only the minimum amount of personal information needed. The University will not disclose personal information to any individual(s) other than the subject unless it is required to do so in accordance with applicable regulation.
- Any disclosure shall be limited to the minimum amount necessary.

3.5. Accuracy:

- The University will make every reasonable effort to ensure that the personal information it collects, uses, and discloses is accurate and complete.
- Each member is responsible for ensuring their information is correct and current.

3.6. Security:

- The University will ensure that the personal information in its custody is secured in a manner appropriate to the sensitivity and purpose of the information.
- The University will ensure that records containing personal information are protected from unauthorized collection, access, use, disclosure, and disposal by putting in place reasonable administrative, physical, and technical security measures.
- All employees will ensure that any personal information which they handle as part of their job with UNF is secure from unauthorized access, and that collection, use and disclosure of personal information is minimized.
- The University and all employees will ensure that records are managed in accordance with an established records retention and disposal schedule.

3.7. Openness:

- This Policy and all related procedures will be made available on the University's website.
- Printed copies will be made available from the Privacy Officer, who will also respond to any privacy-related questions.
- The University will notify affected any individual(s) of potentially detrimental breaches of its privacy controls.

3.8. Individual Access:

- An individual may request their personal information by making a written request to the University department responsible for the information, or to the Privacy Officer.
- UNF may require an individual to prove their identity before providing access to information.
- A fee may be levied by the University if the request requires the use of extra personnel and/or University resources.
- When personal information is used to make a decision affecting a member, the information will be kept for at least one year so that the individual will have sufficient opportunity to access the information, if desired.
- Upon request from an applicant, the University will correct an error or omission in an applicant's personal information or annotate the file if no correction is made.

3.9. Challenging Compliance:

- Complaints or questions with respect to the University's compliance with this policy must be directed to the Privacy Officer.
- The Privacy Officer shall investigate all complaints received or shall delegate the investigation to another investigator.

4. Access Rights

4.1. Individuals have the right to ask for their own personal information and to request a correction of records containing their own personal information.

4.2. Individuals seeking access to a record must submit a written request to the Privacy Officer that provides sufficient detail to identify the record.

4.3. The Privacy Officer will respond to all Access Requests within 30 business days.

- In certain circumstances, UNF may take a 30-business day extension. These circumstances include:
- When the individual(s) have not given UNF sufficient information to identify a requested record;
- When there is a large number of records and meeting the request within the time limit would unreasonably interfere with the operations of the University; or
- When more time is needed by NFY to consult with a third-party.

4.4. Personal information collected by UNF may be used and disclosed for the purposes of administrative, information technology, law enforcement, statistical, research or provincial/federal government activities.

4.5. UNF shall collect, use and disclose personal information for the following purposes:

- Academic and non-academic programs and evaluations;
- Recruitment, admission and graduation;
- Financial aid assistance, awards and bursary;
- Philanthropic initiatives and activities;
- Employment related matters;
- Security and information technology;
- Institutional planning, research, and statistics; and
- Third-party organization(s) for UNF-related activities.

4.6. UNF shall only disclose personal information in its custody or control in circumstances where:

- An access request is submitted and is in accordance with the provisions of this policy and the applicable regulation(s);
- An individual to whom the information relates has consented to disclosure in writing;
- It is for the purpose for which it was collected or for a consistent purpose;
- It is necessary to aid in the investigation of an allegation that an individual has made false statements or engaged in other misleading conduct;
- It is for the health and/or safety of an individual;
- Facilitation of contact with the spouse, close relative or emergency contact of an employee or student who is injured, ill or deceased; and,
- Disclosure is required by the federal government to facilitate the auditing of a shared cost program.

4.7. Records will be exempt from disclosure in circumstances where granting access could:

- Harm law enforcement or an ongoing law enforcement investigation;
- Harm another individual, another individual's business interests or the public;
- Damage UNF's economic interests if the records – containing financial, commercial, scientific or technical information – belonging to UNF have actual or potential monetary value;
- Damage UNF's competitive position if the records contain institutional plans or information that have not been made public;
- Damage UNF's legal position if the records are subject to solicitor-client privilege or prepared by counsel for the potential use in giving legal advice or in litigation;
- Undermine the effectiveness and/or fairness of an auditing procedure;
- Undermine the effectiveness and/or fairness of an examination, testing procedure or other means used in the evaluation of student learning including a record of question that is to be used on an examination or test.

5. Fees

5.1. UNF will not assess any fees/charges for manually searching for records containing the requestor's own personal information.

5.2. Any other requests under the freedom of information act for access to record(s) must include a $5 application fee, as well as any applicable fees related to the request, including:

- Record searches for any searches beyond three (3) hours spent locating and retrieving records at a rate of no more than $7.50 per 15 minutes of search time;
- Preparing the record for disclosure;
- The cost of developing a computer program to produce a record, at a rate of no more than $15 for every 15 minutes of work;
- Other computer and related costs incurred in locating, retrieving, processing and copying records;
- Shipping costs;
- Photocopies and/or computer printouts at a rate of no more than $0.20/page;
- Records provided on CD-ROMs at a cost of no more than $10/CD-ROM; and
- Other costs incurred by the University in responding to a request.

5.3. The University will inform the requester about the details of the fee to complete the request when the requester will be charged $25 or more.

5.4. If the fee estimate is greater than $100, the requester may be required to pay a deposit equal to 50% of the estimate before any further steps are taken to respond to the request.

5.5. Individuals seeking access to information may be permitted to seek waiver of payment of all or part of the fees assessed in certain circumstances if, in the Privacy Officer's opinion, it is fair and equitable to do so.

6. Disclosure

6.1. Employees may only share students' personal information with other employees whose duties and responsibilities authorize them to have access to that information.

6.2. A student's parents, guardians or spouse may be provided access to personal information of the student if prior consent from the student, aged 16 or over, is obtained.

7. Disposal of Personal Information

7.1. UNF shall retain personal information for a period of at least one (1) year from its last use unless the affected individual consents to a shorter period. Personal information cannot be destroyed prior to this time and may be subject to longer retention periods.

7.2. It is an offence to alter, conceal or destroy a record with the intent of denying a right of access. Intentional destruction of UNF's records may result in a fine and/or legal proceedings.

8. General Data Protection Regulation (GDPR)

8.1. Employees and students will adhere to GDPR principles pertaining to the handling of personal data of EU residents studying and/or working at UNF and will ensure that EU residents are notified when information is collected from them directly or from a third party, e.g., a recruiter, and how that data is being controlled.

8.2. EU residents will have rights to access, amend or have their data removed from UNF's records, when it is no longer being held for the purpose it was collected or required on other legal grounds. The UNF Privacy Officer will be the point of contact for such requests.

9. Definitions

These definitions apply to terms as they are used in this policy.

Word/Term	Definition
Personal Information	Personal Information means recorded information about an identifiable individual, including the individual's address, sex, age, education, medical or employment history and other information about the individual under the University's custody or control as provided in FIPPA.
Privacy	The protection of the collection, usage, storage, destruction, and dissemination of personal information on alumni, donors, students, staff, faculty, and University stakeholders.
Privacy Breach	Privacy Breach means an unauthorized collection, use or disclosure of someone's personal information, in contravention of the Freedom of Information and Protection of Privacy Act or the Personal Health

Word/Term	Definition
	Information Protection Act. The breach may affect an individual or a group.
Records	Records are any recorded information regardless of whether it is printed on paper, on film (or some other analog information carrier) or available in digital form that can be recovered, reproduced and accessed. This includes emails, electronic information, books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing in which information is recorded or stored by graphic, electronic, mechanical or other means.

10. Responsibility

All employees are expected to undertake Privacy awareness training authorized by the University.

Each "user department" responsible for University information shall maximize the likelihood information is being used properly and appropriately by:

- Identifying the information;
- Determining whether it is of a restricted nature and/or highly risk sensitive;
- Developing, implementing, and maintaining reasonable and clear procedures that:
  - establish access rules;
  - identify change control requirements and responsibilities;
  - identify confidentiality requirements;
  - promote "good housekeeping" practices such as locking away confidential files when not in use, destroying confidential information when discarded, and not sharing passwords to computer accounts with anyone other than their supervisor and/or the department information security officer;
  - establish appropriate password, data integrity, storage, backup, and recovery practices where local department computer applications exist;
  - Having employees sign an acknowledgement that they are aware of this policy and the related departmental procedures, and that they are expected to act appropriately in maintaining the confidentiality and integrity of the information to which they have access.

Some departments are also "owners" of computer applications. Examples of these applications include Financial Systems, Human Resources/Payroll Systems, Student Information Systems, Alumni Systems, and various academic systems.

- The ownership of these systems includes the additional responsibilities of:
  - establishing application access rules for the broader University community;
  - developing, implementing, and maintaining reasonable and clear procedures for granting application access to the broader University community;
  - designating an application security officer within the "owner" department responsible for setting up and maintaining authorized user security access profiles on these systems;
  - maintaining the skill sets necessary to support these practices.

Some departments also have the responsibilities for the traffic (network) processing (computer programs) and storage of data on behalf of the University community.

- These departments have the added responsibilities of:
  - establishing the technical infrastructure access rules for the University community (access to networks and computers);
  - establishing change control rules for processing and storage technology (computer programs and data bases);
  - establishing storage, backup, and recovery rules for computer programs and databases;
  - developing, implementing, and maintaining reasonable and clear procedures for granting access to the technical infrastructure, storage, backup, data integrity, and recovery practices;
  - designating a data security officer within the "technical" department responsible for setting up and maintaining authorized user security access profiles for the technical infrastructure;
  - maintaining the skill sets necessary to support these practices.

11. Duties of the Privacy Officer

All personal information inquiries or complaints fall under the jurisdiction of the Privacy Officer.

Members of UNF and UNF staff may request access to their personal information and may request corrections to personal information so that it is complete and accurate.

The Privacy Officer will ensure that personal information is secured.

The Privacy Officer will ensure the protection of personal information safeguarded by UNF including:

- Limiting access to personal information to those employees who require access to the information in the performance of their job function;
- Installing and maintaining reasonable security safeguards to prevent unauthorized access of its computer system and hard copy files;
- Not collecting or disclosing personal information for purposes other than what is listed in this policy;
- Ensuring that personal information kept is accurate and current; and
- Destroying personal information (when required) in a manner that maintains the confidentiality of that personal information.

Action Required	Position Responsible	Action Required
1. Contain the breach.	Program area where breach occurred.	Immediate
2. Report the breach within the organization or public body	• Program area staff (report to management) • Management • Privacy Officer	Same day as breach discovered
3. Designate lead investigator and select breach response team as appropriate	Privacy Officer	Same day as breach discovered
4. Preserve the evidence	Lead Investigator or Privacy Officer	Same day as breach discovered
5. Contact police if necessary	Privacy Officer	Within 2 days of breach discovery
6. Conduct preliminary analysis of risks and cause of breach	Lead Investigator	Within 2 days of breach discovery
7. Determine if the breach should be reported to Privacy Officer	Privacy Officer in consultation with executive	Generally, within 2 days of breach
8. Take further containment steps if required based on preliminary assessment	Lead Investigator or Privacy Officer	Within 2 days of breach
9. Evaluate risks associated with breach	Lead Investigator or Privacy Officer	Within 1 week of breach
10. Determine if notification of affected individuals is required	Privacy Officer	Within 1 week of breach
11. Conduct notification of affected individuals	Privacy Officer or program area manager	Within 1 week of breach
12. Contact others as appropriate	Privacy Officer or program area manager	As needed
13. Determine if further in-depth investigation is required	Privacy Officer or program area manager	Within 2 to 3 weeks of the breach
14. Conduct further investigation into cause & extent of the breach if necessary	Privacy Officer, security officer or outside independent auditor or investigator	Within 2 to 3 weeks of the breach
15. Review investigative findings and develop prevention strategies	Privacy Officer or program area manager	Within 2 months of breach
16. Implement prevention strategies	Privacy Officer or program area manager	Depends on the strategy
17. Monitor prevention strategies	Privacy Officer or program area manager	Annual privacy/security audits