Policy on Access to Information and Protection of Privacy

Office of Administration:	Office of the General Counsel
Approval Authority:	President and Executive Team
Approval Date:	July 2024
Next Review:	July 2028
Review History:	2012

1. Purpose

To ensure that Laurentian University of Sudbury (the "**University**") complies with its obligations under federal and provincial laws regarding access to information and protection of personal information, including the *Freedom of Information and Protection of Privacy Act* (**FIPPA**), the *Personal Health Information Protection Act* (**PHIPA**), and the *Personal Information Protection and Electronic Documents Act* (**PIPEDA**).

2. Scope

(a) The Policy applies to all administrators, faculty, staff, students, contractors, and volunteers of the University, and its affiliates, who have access to general and personal information.

(b) This Policy applies to all records in the University's custody or under its control, including records relating to the operation and administration of the University, and records containing information relating to administration, faculty, staff, and students.

(c) This Policy does not apply to:

(i) records placed in the University Archives by or on behalf of a person or organization other than the University;

(ii) records collected, prepared, maintained or used by or on behalf of the University in relation to any of the following:

A. proceedings or anticipated proceedings before a court, tribunal or other entity relating to labour relations or to the employment of a person by the University;

B. negotiations or anticipated negotiations relating to labour relations or to the employment of a person by the institution between the institution and a person, bargaining agent or party to a proceeding or an anticipated proceeding; or

C. meetings, consultations, discussions or communications about labour relations or employment-related matters in which the institution has an interest.;

(iii) records respecting or associated with research conducted or proposed by an employee of the University or by a person associated with the University; or

(iv) records of teaching materials collected, prepared or maintained by an employee of the University or by a person associated with the University for use at the University.

3. Policy Statement

3.1 The University will comply with FIPPA, which protects the privacy of individuals with respect to personal information held by the University, and provides individuals with a right of access to that information.

3.2 FIPPA also establishes a right of access to general information and under the University's custody or control in accordance with the principles that information should be available to the public, subject to limited and specific exemptions or exclusions.

The University will also comply with PIPEDA and PHIPA to the extent that those laws are applicable to University services, functions, or activities.

4. Definitions

"FIPPA" means the *Freedom of Information and Protection of Privacy Act*, RSO 1990, chapter F.31.

"Personal health information" has the meaning ascribed to it under PHIPA, and includes but is not limited to identifying information about an individual in oral or recorded form, if that information relates to the physical or mental health of the individual and relates to the provision of healthcare to the individual, or includes the individual's health card number.

"Personal information" has the meaning ascribed to it under FIPPA and means recorded information about an identifiable individual, including:

i. information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual;

ii. information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

iii. any identifying number, symbol or other particular assigned to the individual;

iv. the address, telephone number, fingerprints or blood type of the individual;

v. the personal opinions or views of the individual except if they relate to another individual;

vi. correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence;

vii. the views or opinions of another individual about the individual; and

viii. the individual's name if it appears with other private information relating to the individual or where disclosure of the name would reveal other private information about the individual.

"Personal information bank" means a collection of personal information that is organized and capable of being retrieved using an individual's name or an identifying number or particular assigned to the individual.

"PHIPA" means the *Personal Health Information Protection Act*, 2004, S.O. 2004, c. 3, Sched. A.

"PIPEDA" means the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

"Privacy breach" means the loss of, unauthorized access to, or unauthorized disclosure of, personal information under the University's custody or control. Situations that may result in a privacy breach include the theft or loss of a computing device including mobile devices containing personal information or accessing personal information that is not required for performance of one's work duties.

"Record" means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes:

i. correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine readable record, any other documentary material, regardless of physical form or characteristics, and any copy thereof; and

ii. any record that is capable of being produced from a machine readable record under the control of the University by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution.

"Information and Privacy Coordinator" means the person responsible for the coordination of activities related to FIPPA.

5. **Information and Privacy Coordinator**

(a) Under FIPPA, the designated head of the University, the President, has the authority and duty to make decisions on FIPPA requests.

(b) The President has delegated this authority and these duties to the General Counsel, who may assign the function of the University's Information and Privacy Coordinator (**UIPC**) to a member of the Office of the General Counsel. The UIPC is responsible for coordinating the University's activities related to FIPPA. The UIPC will be the contact person for all inquiries under FIPPA as described in Duties of the Information and Privacy Coodinator. **NTD: Link to Procedure]**.

(c) The UIPC will document information on all FIPPA requests and complaints received, ensure that all requests are processed within established time limits, and generate annual statistics for the Information and Privacy Commissioner of Ontario, among other assigned duties.

(d) The UIPC's contact information is as follows:

Information and Privacy Coordinator
935 Ramsey Lake Road
Sudbury, ON
P3E 2C6

Email: Generalcounseloffice@laurentian.ca

6. **Access to Information**

(a) The University routinely provides information to the public through its administrative and academic units, its Department of Communications & Public Affairs, and its website. A request for information contained in University records can also be made formally. However, it is not necessary to file an official

request for information that is routinely released to the public. Informal inquiries are welcomed and will be dealt with by the appropriate department heads. Faculty and staff are encouraged to release general information, respond to routine inquiries, and provide copies of records as appropriate while respecting the need to protect privacy.

(b) Formal access requests can be made under FIPPA, which provides every person with the right to access a record, in whole or in part, under the custody or control of the University, subject to certain statutory exclusions and exemptions. Examples of such exclusions and exemptions include, for example:

- Where the record contains the personal information of another individual, and that individual's consent for disclosure has not been provided;
- When the record is subject to solicitor-client privilege;
- Where disclosure of the record could reasonably be expected to interfere with a law enforcement matter; and
- Where the record was collected, prepared, maintained or used by or on behalf of the University and is about labour relations or employment-related matters in which the University has an interest.

(c) Every person also has the right to access their own personal information that is in the custody or control of the University. As with general access requests, the extent of the right of access to personal information is subject to exclusions and exemptions provided in FIPPA.

Similar rights of access to records of one's own personal health information and personal information exist under PHIPA and PIPEDA, respectively.

(d) Formal requests for access to information under FIPPA must be made in writing, accompanied by a $5 application fee, and provide enough detail to allow the University to identify the records. All requests must also include the following contact information: name, address, and daytime telephone number. There is no application fee for access requests under PHIPA or PIPEDA.

(e) For more information and details on the request procedure, please see the University's Procedure for Handling Access to Information and Correction Requests **[NTD: Link to Procedure]**.

(f) For any questions about this Policy, please contact the UIPC at Generalcounseloffice@laurentian.ca.

7. **Correction of Personal Information**

(a) Where an individual believes that there is an error or omission in the personal information they have obtained access to, they may request the correction of that personal information.

(b) If the University declines to correct the information as requested, the individual has the right to require that a statement of disagreement be attached to the information reflecting any correction that was requested but not made. In such cases, the individual also has the right to require that any person or body to whom the personal information has been disclosed within the year before the time a correction is requested or a statement of disagreement is required, be notified of the correction or statement of disagreement.

(c) For more information and details on the correction request procedure, please see the University's Procedure for Handling Access to Information and Correction Requests. **[NTD: Link to Procedure]**

8. **Collection, Use and Disclosure of Personal Information**

(a) Personal information will be collected, used, maintained, disclosed, and disposed of in accordance with the applicable legislation, policies, agreements, and best practices.

(b) Collection of personal information

(i) The University only collects the personal information that is necessary for the administration of the University's programs, services, and functions.

(ii) Personal information will not be collected unless it is expressly authorized by statute, used for purposes of law enforcement, or necessary for the proper administration of a lawfully authorized activity.

(iii) Personal information will be collected according to the following principles:

- the personal information collected must be necessary to fulfill a legitimate University activity or purpose;
- the personal information collected must be the minimum amount necessary for the activity or purpose; and
- the personal information must be collected directly from the individual or if indirectly, with the clear knowledge and authority of the individual, or as permitted by FIPPA and other applicable legislation.

(iv) When personal information is collected, notice will be provided to the individual containing, at a minimum, the legal authority for the collection, the purpose for the collection and how the information is intended to be used, and the contact information for a University employee who can answer questions about the collection.

(v) For more information about how the University collects personal information under FIPPA, please see the University's FIPPA Notice of Collection of Personal Information. **[NTD: link to Notice of Collection]**

(vi) For collections of personal health information in the context of seeking or receiving health care, please refer to the individual health information custodian's Notice of Collection under PHIPA, and the University's Procedure for Handling Personal Health Information. **[NTD: link to procedure]**

(c) Use of personal information

(i) Personal information will be only used for the purpose for which it was obtained, compiled or disclosed, or for a consistent purpose or with the individual's consent.

(ii) Personal information in alumni records may be used for the purpose of the University's own fundraising activities in compliance with the requirements of FIPPA and other applicable legislation.

(iii) The University may use third party service providers to assist in its operations, and may transfer personal information to these service providers for processing. In some cases, these service providers may be located outside of Canada. The University will use contractual means to protect personal information that is transferred to service providers.

(iv) For uses of personal health information in the context of seeking or receiving health care, please refer to the individual health information custodian's Notice of Collection under PHIPA, and the University's Procedure for Handling Personal Health Information. **[NTD: link to procedure]**

(v) For uses of personal information in the course of non-core commercial activities at the University (i.e. those regulated under PIPEDA), please see the individual service provider's privacy policy.

(d) Disclosure of personal information

(i) Personal information will be disclosed only to the person to whom it relates, except where the individual consents, or where the disclosure is for the purpose that the information was obtained, or where disclosure is made to University employees, or to consultants or agents engaged by the

University, where the disclosure of the information is necessary and proper for the performance of their duties.

(ii) Personal information may be disclosed as permitted by FIPPA. For example, personal information may be disclosed:

A. under compelling circumstances affecting the health and/or safety of an individual or individuals;

B. on compassionate grounds to facilitate contact with a family member of an individual who is injured, ill, or deceased;

C. to an institution or a law enforcement agency in Canada to assist with investigations;

D. in compliance with any other exceptions cited in FIPPA and other applicable legislation; and

E. for the purpose of the University's own fundraising activities in compliance with the requirements of FIPPA and other applicable legislation.

(iii) For disclosures of personal health information in the context of seeking or receiving health care, please refer to the individual health information custodian's Notice of Collection under PHIPA, and the University's Procedure for Handling Personal Health Information. **[NTD: link to procedure]**

(e) The University is accountable for the personal information in its custody and under its control.

9. **Security Safeguards**

(a) Personal information in all formats (electronic, paper, verbal, or other) will be protected throughout its lifecycle (collection, use, disclosure, retention and disposal) through the use of physical, administrative, and technical safeguards as determined by University policy and in accordance with legislative requirements and best practices.

(b) The University uses role-based access to personal information, which ensures that University employees, agents, and service providers have access to the minimum amount of personal information required to perform their functions and duties.

(c) Contractual or other measures will be used to protect personal information that has been transferred to, or is collected by, agents and service providers.

10. **Personal Information Banks**

As required by FIPPA, the University maintains an Index of Personal Information Banks which outlines all faculties, administrative offices or services that create and maintain personal information banks for purposes of carrying out University services or functions.

11. **Records Management**

(a) An individual's personal information will be retained for at least one year after use unless the individual to whom the information relates consents to its earlier disposal. Thereafter the personal information will be disposed of in accordance with the University's Records Management Policy and related Retention Schedules.

(b) Care will be taken in the disposal or destruction of personal information to prevent unauthorized access to the information.

(c) When records are destroyed or deleted, all reasonable steps will be taken to ensure the information cannot be retrieved.

12. **Personal Health Information**

(a) Personal health information collected, used, and disclosed by University health information custodians shall be managed in accordance with the requirements of PHIPA.

(b) For more information about how the University handles personal health information, please see the University's Procedure for Handling Personal Health Information.

13. **Related Policies, Procedures, and Forms NTD: link to policies**

LU Electronic Services Acceptable Use

Privacy Breach Report Form

Notice of Collection of Personal Information

Notice of Collection of Personal Health Information

Privacy Breach Protocol

Procedure for Handling Access to Information and Correction Requests

Procedure for Handling Privacy Complaints

Policy on Records and Information Management

Duties of the Information and Privacy Coordinator

Policy on Access to Electronic General Personal Information

Policy on Managing Confidential Digital Information