



Freedom of Information and Protection of Individual Privacy

Category: General;

Jurisdiction: Vice President, Administration and Finance;

Approval Authority: Executive Team;

Established on: February 2, 1999;

Amendments: March 11, 2008.

Preamble

In 1999 Lakehead University established an official policy on freedom of information and protection of individual privacy. The policy was modelled on Ontario's Freedom of Information and Protection of Privacy Act (FIPPA) - even though FIPPA did not at the time apply to the University. On June 10, 2006 FIPPA's jurisdiction was extended to the provincial universities, so Lakehead had to adjust its policy to ensure compliance with the Act. The main purpose of this revised policy is to lay down guidelines for the application of FIPPA to the special circumstances and requirements of Lakehead University, in accordance with the following principles, all of which reflect the imperatives of the Act:

- Subject to the disclosure exemptions and jurisdictional exclusions specified by FIPPA, information contained in University records will be available to members of the University community and to members of the public more generally.
- Necessary exemptions from the general principle favouring access will be as limited and specific as possible.
- The collection, retention, use, disclosure, and disposal of personal information contained in University records will be regulated in a manner that will protect the privacy of individuals to whom the information relates.

- Individuals will have the right, limited only by FIPPA restrictions, to access and correct personal information about themselves in the University's records.

Guidelines

General

1. Access to information and protection of privacy with respect to all records within the custody or control of the University are governed by FIPPA and these Guidelines. The Guidelines have been carefully revised to conform to FIPPA but, should a conflict occur between them, FIPPA shall prevail.
2. Under FIPPA, the President of Lakehead University is responsible for all aspects of the University's compliance with the Act, but section 62(1) authorizes the President to delegate his or her powers and duties to other officers of the institution, and they have been so delegated to the Vice-President (Administration and Finance) (hereinafter referred to as the "Vice-President") and the Director of Risk Management and Access to Information (hereinafter referred to as the "Director"). All questions or concerns about these Guidelines in particular, or freedom of information and protection of privacy at Lakehead University in general, should be directed at first instance to the Director.

Freedom of Information

Disclosure of Records

3. Provided that the relevant procedural requirements of FIPPA are complied with, any person who requests it shall be granted access to records in the custody or under the control of the University subject to the disclosure exemptions and jurisdictional exclusions set by FIPPA, including the following:
 - 1) Except in cases specified by FIPPA, the University shall refuse access to personal information in its records. Personal information is defined in section 2(1) of FIPPA as:

"recorded information about an identifiable individual, including,

"(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

"(b) 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,

"(c) any identifying number, symbol or other particular assigned to the individual,

"(d) the address, telephone number, fingerprints or blood type of the individual,

"(e) the personal opinions or views of the individual except where they relate to another individual,

"(f) 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,

"(g) the views or opinions of another individual about the individual, and

"(h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual;"

Student records fall into the category of personal information, and so their information cannot be disclosed except to the extent permitted by FIPPA.

All photographic and audio information, however recorded and stored, that can identify a person also falls within the FIPPA category of "personal information."

- 2) The University may refuse access to recorded information respecting or associated with research conducted or proposed by an employee of the University or by a person associated with the University, except for the subject-matter and amount of funding being received with respect to the research.
- 3) The University may refuse access to a record relating to meetings, consultations, discussions, or communications about labour relations or employment-related matters in which the University has an interest.
- 4) The University may refuse access to a record placed in its archives by or on behalf of a person or organization other than the University or one of its constituent units.

- 5) The University may refuse access to a record of teaching materials collected, prepared or maintained by a University employee or by a person associated with the University for use at the University or any of its constituent units.
 - 6) The University may refuse access to recorded information relating to specific tests or testing procedures or techniques that are to be used for an educational purpose, if disclosure could reasonably be expected to prejudice the use or results of the tests or testing procedures or techniques.
4. The University may classify any record it wishes as confidential and require that it be treated as such on the understanding that, in the event of a formal FIPPA request for information, the University must disclose all records, whether classified as confidential or not, which are responsive to the request and are not protected from disclosure by FIPPA exemptions or jurisdictional exclusions.

Financial Data

5. In addition to any disclosure of financial information otherwise required by FIPPA, the University shall continue to prepare annual financial statements whose contents can be disclosed without infringing the various interests protected by the aforementioned access exemptions and jurisdictional exclusions.

Protection of Privacy in the Collection, Use, Disclosure, Retention, and Disposal of Personal Information

Collection of Personal Information

6. Under the authority of the Act Respecting Lakehead University, the University shall collect and record only such personal information as is either reasonably necessary to the proper administration of the University and its academic and other programs or is required by virtue of data collection or reporting requirements lawfully imposed upon the University by federal or provincial governmental authority. The University shall ensure that the forms by which it collects personal information carry the collection notice stipulated by section 39(2) of FIPPA.

Use of Personal Information

7. The University shall not use personal information in its custody or under its control except as permitted by FIPPA.

8. The University may use personal information in its custody or control for statistical analyses intended to support, improve, and promote the University's operations and services.

Disclosure of Personal Information

9. The University shall not disclose personal information in its custody or control without the consent of the person to whom the information relates, except as permitted by FIPPA. Following are examples of permissible disclosure:
 - 1) to the extent necessary for an officer, employee, volunteer, consultant or agent of the University to perform his or her duties and where such disclosure is proper in the discharge of the University's functions;
 - 2) where disclosure of faculty's, staff's or students' postal and/or email addresses is made to staff of University owned and operated commercial outlets (excluding the University's Office of Alumni Relations) who need this information for promotion of the outlets' goods and services, or to staff of the Office of University Advancement who need this information to raise funds for the University, on condition that:
 - a. at each contact with an individual to whom the information relates notice is given that the individual has the right to request that he or she not be contacted again;
 - b. each such request is honoured; and
 - c. the staff who have used this personal address information for the said promotion and fundraising do not disclose it to any other person or entity without the consent of the person(s) to whom the said information relates.
 - 3) in compassionate circumstances, to facilitate contact with the spouse, a close relative or a friend of an individual who is injured, ill or deceased;
 - 4) for the purpose of complying with a requirement to provide information lawfully imposed upon the University by a federal or provincial governmental authority;
 - 5) to a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result, on condition that the said agency produce written confirmation, with supporting contact information of an official authority within the

- said agency, that such an investigation is underway, or that such a proceeding is likely to occur;
- 6) where disclosure to University officials is necessary for the investigation of allegations that individuals have
 - a. made false statements, or
 - b. engaged in other misleading conduct concerning their attendance or performance or status within, or completion of, an academic program of the University, or
 - c. breached the University's regulations or codes of conduct, or
 - d. otherwise engaged in ethical or professional misconduct or illegal activity or;
 - 7) in the event that the University has, on the basis of sound evidence, formally found, or determined, that an individual has
 - a. made a material misrepresentation to the University, or
 - b. engaged in other misleading conduct concerning his or her attendance or performance or status within, or completion of, an academic program of the University, or
 - c. breached the University's regulations or codes of conduct, or
 - d. has otherwise engaged in ethical or professional misconduct, or
 - e. has been convicted of illegal activity by a court or tribunal in which case personal information about that individual may be disclosed
 - a. within the University to personnel who need the information to carry out their duties, and/or
 - b. as appropriate, to other postsecondary institutions, and/or
 - c. to professional bodies and/or law enforcement institutions as required by professional ethics, regulations, or law.
 - 8) to maintain the University's public directories, whose elements may include:
 - a. names of faculty, staff, and other individuals performing official functions within the University, their academic and professional titles, qualifications, and memberships, their work addresses, telephone numbers, fax

- numbers, and e-mail addresses, and the duration of their employment at or association with Lakehead University;
- b. ONLY IN RELATION TO GRADUATION AND CONVOCATION: names of students, the programs and specializations in which they are graduating, the Faculties, Schools, or other divisions from which they are graduating, the degrees, diplomas, minors, and certificates conferred upon them by Lakehead University, their degrees, diplomas, and certificates from other institutions, the scholarships and awards that they have received at Lakehead University, and the award of First Class Standing in their Lakehead University degrees, diplomas, and minors;
- 9) for the disclosure of photographic or audio information recorded from a public event, where the main purpose of the disclosure is to publicize the event or promote the University;
- 10) to the extent necessary for the collection of debts owed to the University.

Retention and Disposal of Personal Information

10. All University departments and employees shall take reasonable precautions to protect the security of all records, including electronic communications, in their custody or control which contain personal information relating to University business. Such records may be removed or copied from their secure University repositories only on grounds of real necessity and, when they are removed or copied, must be specially secured against loss, theft, copying, contamination, perusal by unauthorized persons, or destruction except when they have been officially consigned to scheduled disposal, in which case secure methods of disposal, protecting the records from loss, theft, copying, or perusal by unauthorized persons, must be followed. Any loss of records bearing personal information should be reported immediately to the Director.
11. With respect to records bearing personal information which are held in the University's Archives, or which have not been used, or which relate to employment, labour relations, research, or teaching materials, the University shall follow practices required by law or by records management standards for the retention and disposal of such records. With respect to all other records, including electronic communications, in the University's

custody or under its control which bear personal information that has been used by University staff, contractors, or volunteers and that relates to University business, all University departments and employees shall

1. retain those records for at least one year after their creation unless, in each case, the individual to whom the personal information relates consents to its earlier disposal;
2. make arrangements for the secure transfer of such records to the University's Archives or for the records' destruction after at least one year from their creation; and
3. establish a disposal record of this transfer or destruction.

Access and Correction Rights

12. Every individual shall be granted access, within the limits imposed or permitted by FIPPA, to records containing personal information which the University has in its custody or control concerning that individual, and with respect to which the individual is able to provide sufficiently specific information to render the records reasonably retrievable by the University.
13. The University shall make reasonable arrangements to ensure that explanations for student evaluations are made available to the affected students, together with copies of such materials as are relevant to such explanations and which can be disclosed without undermining the integrity of the evaluation system or method in question or invading the privacy of another person.
14. Every individual who is granted access to University records bearing their personal information and who, in consequence, believes that the said personal information is defective by reason of an error or omission, is entitled to:
 1. request that the error or omission be corrected;
 2. require that a statement of disagreement be attached to the information reflecting any correction that was requested but not made; and
 3. 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.

Exemptions from the Access Right

15. As permitted or required by FIPPA, the University may refuse to disclose some kinds of records containing personal information to the individual to whom the information relates, and in particular records

- 1) whose disclosure would constitute an unjustified invasion of the privacy of another individual;
- 2) consisting of evaluative or opinion material compiled solely for the purpose of determining suitability, eligibility, or qualification for employment or for the awarding of a contract with the University and other benefits where the disclosure would reveal the identity of a source who furnished information to the institution in circumstances where it may reasonably have been assumed that the identity of the source would be held in confidence;
- 3) supplied explicitly or implicitly in confidence, bearing evaluative or opinion material compiled solely for the purpose of
 - a. determining suitability, eligibility or qualifications for admission to an academic program of the University;
 - b. assessing the teaching materials or research of a University employee or of a person associated with the University;
 - c. peer review processes related to determinations concerning eligibility or suitability for the granting of promotion, tenure, or renewal, research grants or other benefits to members of the University community or for similar purposes; or
 - d. determining suitability for an honour or award to recognize outstanding achievement or distinguished service.

Implementation, Monitoring and Dispute Resolution

16. The Director, who reports to the Vice-President, shall be responsible for the implementation of these Guidelines as well as all applicable federal and provincial information access and privacy legislation within the University.
17. The Director shall oversee and ensure the adoption within the University of record-keeping and disclosure practices consistent with these Guidelines and access and privacy legislation.
18. All requests for access to information or for the correction of personal data, and all complaints about breaches of privacy, shall be made in accordance with the guidelines laid out in the web site of Lakehead University's Office of Risk Management and Access to Information at <http://riskandprivacy.lakeheadu.ca/projects/fippa/>, and shall be processed as indicated there.
19. All appeals from decisions of the Director on the requests referred to in Guideline 17 must be made to the Information and Privacy Commissioner of Ontario, as indicated in the guidelines in the web site of the University's Office of Risk Management and Access to Information.
20. If the Information and Privacy Commissioner disclaims jurisdiction to hear an appeal, it may be made to the Vice-President instead, who shall have full authority to determine the manner in which an appeal shall be investigated and the procedures to be followed in any hearing, interview or proceeding that the Vice-President may consider appropriate in order to effect a proper disposition of the appeal. If, at the conclusion of an investigation, the Vice-President finds that the appellant is not being treated in accordance with these Guidelines, the Vice-President shall make an appropriate recommendation to the Director, together with a request that the Director report to the Vice-President and the appellant on the nature of such action as has been taken in response to the recommendations within a specified period of time. The Vice-President shall file written reports concerning any such investigations and recommendations, as well as reports from affected administrative officers, to the University's President. A copy of each report shall be forwarded to the appellant. The recommendations of the Vice-President shall not be binding on any affected administrative officer or the President of the University. In any case where the recommendations of the Vice-

President are not accepted, the President shall report this decision and the reasons therefore to the governing body of the University to whom the President is normally accountable.

21. The Vice-President may delegate any of the powers and responsibilities assigned to him or her in Guideline 19 to any other administrative officer of the University, except the Director.
22. The Director, who shall consult with the University's Freedom of Information and Protection of Privacy (FOIPP) Committee as appropriate, shall have the following additional responsibilities and powers:
 - 1) to review existing policies and procedures in the University for compliance with FOIPP legislation and these Guidelines, and
 - a. where the Director determines that their compliance is satisfactory, confirm their acceptability and monitor their implementation; and
 - b. where the Director determines that their compliance is not satisfactory, recommend improvements to the appropriate University bodies, and monitor the implementation of the improvements;
 - 2) where policies and procedures for complying with FOIPP legislation and these Guidelines do not exist, to determine whether they are necessary and, if they are, to make recommendations to the appropriate University bodies and monitor their implementation;
 - 3) where the Director determines that implementation of FOIPP policies and/or procedures is not satisfactory, to so inform the departments/units and personnel responsible for the implementation or their supervisors and, if the gravity of the deficiency warrants, to report the matter to the Vice-President;
 - 4) to ensure that all FOIPP policies and procedures, including these Guidelines, include clear provisions for implementation;
 - 5) to formulate and review policies to promote the inclusion of compliance with FOIPP legislation in all planning and analysis undertaken by University authorities and to monitor the success of those policies;
 - 6) to undertake and review training and communication procedures for the application of FOIPP legislation in the University;

- 7) to recommend, from time to time, appropriate amendments to these Guidelines.
23. The Director shall prepare and present to the governing bodies of the University an annual report concerning the implementation of access to information and privacy legislation, as well as these Guidelines, within the University.

Fees

24. All fees with respect to requests for access to information shall be determined in accordance with the guidelines in the web site of the Office of Risk Management and Access to Information.

Review Period: 7 years;

Date for Next Review: 2023-2024;

Related Policies and Procedures: To be determined;

Policy Superseded by this Policy: None.

The University Secretariat manages the development of policies through an impartial, fair governance process, and in accordance with the Policy Governance Framework. Please contact the University Secretariat for additional information on University policies and procedures and/or if you require this information in another format:

Open: Monday through Friday from 8:30am to 4:30pm;

Location: University Centre, Thunder Bay Campus, Room UC2002;

Phone: 807-346-7929 or Email: univsec@lakeheadu.ca.