Risk Management and Access to Information
ATAC 4009
t: (807) 343-8518
mshaw1@lakeheadu.ca

INFORMATION AND ADVICE FOR FACULTY ON THE APPLICATION OF ONTARIO'S *FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (FIPPA)*

Table of Contents

Section — Page

(I) Background 2

(1) *FIPPA* is concerned with recorded information 2
(2) *FIPPA* distinguishes between personal and non-personal information 2
(3) *FIPPA*'s 3 main purposes 3

(II) Guidelines 4

(1) Requests for General Information Made to Faculty Members 4
(a) General Information That Should Be Disclosed 4
(b) Copyright Does NOT Shield from Disclosure 4
(c) General Information Exempted from Disclosure 5
(d) Other Possible Exemptions 5

(2) Requests for Personal Information 6

(3) Students' Access to Their Own Personal Information 7

(4) Request Procedure 7

(5) Faculty Members' Responsibilities to Protect Privacy 8
(a) Personal Information to Be Protected 8
(b) Collection & Use of, & Access to, Students' Personal Information 8
(c) Disclosure of Students' Personal Information 9
(d) Taking Attendance 9
(e) Group Work and/or Peer Evaluation 10
(f) Handling Assignments 10
i. When you collect assignments 10
ii. When you mark assignments 11
iii. When you return graded assignments 11
(g) Posting Grades 11
(h) Getting Consent 12

(6) Correspondence 12
(a) Email Communications 12
(b) Reference Letters 13

(7) Record Handling, Retention, and Disposal 13

(a) Security for Recorded Personal Information..... 13
(b) Transporting Records with Personal Information..... 14
(c) If Personal Information Records Are Illegally Accessed, Damaged or Corrupted, or Lost or Stolen..... 14
(d) Retention of Records with Personal Information 14
(e) Retention of Other Records 15
i. Non-Personal Records of Significance to the University's Operations 15
ii. Transitory Records 16
(f) Disposal of Records..... 16

(8) Faculty Members' Personal Information and Privacy..... 16
(a) Personal Information re Professional Duties 16
(b) Personal Information NOT Associated with Professional Duties 16
(c) Employment Records 17

****

(I) BACKGROUND

The full text of *FIPPA* and its associated regulations, 459 and 460, can be found online at http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm, and http://www.e-laws.gov.on.ca/html/regs/english/elaws_regs_900459_e.htm, and http://www.e-laws.gov.on.ca/html/regs/english/elaws_regs_900460_e.htm.

(1) *FIPPA* is essentially "watchdog" legislation which regulates the treatment of RECORDED information in the custody or control of the institutions under its jurisdiction – such as the Ontario universities to which *FIPPA* was extended on June 10, 2006.

- Note that if a record of information does not exist, a *FIPPA* institution does not have to create one. *FIPPA* gives neither access nor protection to unrecorded information – except in the case of the collection of personal information (see section 38(1)).

(2) The Act divides "recorded information" into two subcategories:

(a) records of non-personal, often called general, information, and

(b) records of personal information. The distinguishing feature of personal information is, as the Act makes clear in section 2 – its "definition" section - identifiability, that is, to the extent that information makes a person identifiable either

(i) directly (by, e.g., use of personal names, addresses, etc.) or

(ii) indirectly (by provision of contextual information that could make the individual identifiable, even without naming him or her, to some person or group),

that information is personal.

- It follows that, to the extent that personal information is anonymized, it ceases to be personal information under *FIPPA*.

(3) *FIPPA* has three main purposes in regulating institutions' treatment of information:

(a) The first purpose of the Act relates to the first subcategory: in effect *FIPPA* grants to the public (including non-citizens) a right of access to ALL non-personal information in the institution's records;

- This right is limited only by the specific (1) exclusions from jurisdiction and (2) exemptions from disclosure (which have been referred to as "carve-outs" from the right of total access) declared in the Act.

- This mandate of *FIPPA* is referred to in the "Freedom of Information" half of the Act's title.

(b) *FIPPA*'s second purpose relates to the second subcategory of information, personal information, and is exactly the *opposite* to its objective with non-personal information: here it seeks not to open but to restrict as much as possible the institution's treatment of information at all stages – from collection, through use, disclosure, and retention, all the way to final disposal.

- The restriction is NOT absolute: certain "carve-outs" – i.e. jurisdictional exclusions and exemptions – apply.

- Here the "Protection of Privacy" half of the Act's title is reflected. In effect, the Act creates and seeks to enforce a right of privacy for all whose personal information is held in records under the custody or control of public institutions governed by FIPPA.

(c) Finally, *FIPPA*'s third purpose is to provide everyone with a right of access to their own personal information in a public institution's records,

(i) including the right to request correction of errors or omissions that an individual believes exist in his or her information;

(ii) and to require that a statement of disagreement be attached to any of his or her personal information for which a correction was requested but not made.

(iii) There are "carve-outs" from this right as well.

(II) GUIDELINES:

Most of *FIPPA*'s requirements for freedom of information and protection of privacy can be satisfied through the application of common sense, courtesy, and professionalism, hence, compliance with the Act does NOT require a radical departure from the practices generally followed at Lakehead prior to the Act's extension to the Ontario universities.

The guidelines provided below are best practices which are purely advisory and intended to help faculty comply with the law; they do not set or amend any Lakehead policy (that can be done only by Senate or the Board of Governors) and should be read in the light of established University policies, such as Freedom of Information and Protection of Individual Privacy at https://www.lakeheadu.ca/faculty-and-staff/policies/general/freedom-of-information-and_protection-of-individual-privacy; Disclosure of Personal Information – Posting of Student Marks at https://www.lakeheadu.ca/faculty-and-staff/policies/student-related/disclosure-of-personal-information-posting-of-student-marks; and Disclosure of Personal Information – Return of Graded Student Work at https://www.lakeheadu.ca/faculty-and-staff/policies/student-related/disclosure-of-personal-information-return-of-graded-studentwork..

These guidelines have been formulated in the light of advice and practices at other Ontario universities, especially the University of Toronto and Ryerson, Wilfrid Laurier, and York Universities.

All questions or concerns about these guidelines in particular or the application of *FIPPA* in general should be directed to the Director of Risk Management and Access to Information at (telephone) 343-8518, (fax) 346-7735, or (email) mshaw1@lakeheadu.ca. Detailed information about the Act and associated procedures and forms can be found at the web site of the Office of Risk Management and Access to Information at: http://riskandprivacy.lakeheadu.ca/

(1) Requests for General Information Made to Faculty Members:

(a) General Information That Should Be Disclosed: In general, if a request is made by anyone for non-personal recorded information that does not fall into one of *FIPPA*'s jurisdictional exclusions or exemptions, that information should be provided.

- In practice such disclosure would include documents that faculty would normally make available in any event, such as course syllabi or outlines, reading lists, etc.

- A fee can be included if it is normally charged for the item (e.g. through the Book Store).

(b) Copyright Does NOT Shield from Disclosure: Section 32.1 of the *Copyright Act* of Canada says that copyright *per se* does not preclude disclosure of information, whether general or personal.

- It does add the qualification, however, that the recipient of copyrighted information is not thereby authorized "to do anything that, by this Act, only the

owner of the copyright in the record, personal information or like information, as the case may be, has a right to do."

(c) General Information Exempted from Disclosure: *FIPPA* does NOT require faculty members to disclose:

(i) current or future exam questions,

(ii) teaching materials, or

(iii) research notes unless they wish to (and such disclosure is consistent with departmental practice). In fact, the only research information for which *FIPPA* requires disclosure in response to a request is the "subject-matter and amount of funding being received" for the research (section 65(9)).

(iv) In addition you do NOT have to disclose records that are not in the "custody or control" of the University (see section 10(1) of the Act). For practical purposes here are the main parameters of what records fall into the University's "custody or control:"

1. Records relating to University business, including but not limited to communications, administrative documents, course outlines and syllabuses, grade sheets and grading "rubrics", and student assignments, whether in hard copy or electronic format (e.g. emails), whether held on University premises or email accounts or on non-University premises or email accounts, generally come under the University's custody or control.

2. Records that do not relate to University business, even if they are kept on University premises or in University email accounts, are generally not in the University's custody or control.

(d) Other Possible Exemptions: *FIPPA* lists a great number of additional categories of information for which disclosure can be refused. Most of these exemptions are detailed in sections 12 to 22 of the Act. Following are some that may have relevance for faculty (again, if you have any doubt about whether or not to disclose a document, contact the Director of Risk Management and Access to Information):

(i) Information whose disclosure could be reasonably expected to endanger or seriously threaten anyone's life, safety, or health (so, for example, universities, including Lakehead, have denied requests for access to records concerning animals used in research or experimentation, or the facilities/equipment used in such activities, because this disclosure could expose employees to real danger at the hands of animal rights extremists) (s. 14(1)(e) and s. 20);

(ii) Information that could "endanger the security of a building or the security of a vehicle carrying items, or of a system or procedure established for the protection of items, for which protection is reasonably required" (s.14(1)(i));

(iii) "A report prepared in the course of law enforcement, inspections or investigations by an agency which has the function of enforcing and regulating compliance with a law" (s. 14(2)(a));

(iv) Information received in confidence from a government or international organization of states (s. 15);

(v) A record that (a) "reveals a trade secret or scientific, technical, commercial, financial or labour relations information," (b) supplied (c) by a third party in confidence, that could (d) harm the interests of an institution or individual (s. 17(1)) (note: all four conditions have to be met for this exemption to apply);

(vi) A record revealing information obtained on a tax return or gathered for the purpose of determining tax liability or tax collection (s. 17(2));

(vii) A record containing trade secrets or financial, commercial, scientific or technical information with potential monetary value (s. 18(1)(a));

(viii) Information whose disclosure could reasonably be expected to prejudice the economic interests of an institution (s. 18(1)(c));

(ix) "Plans relating to the management of personnel or the administration of an institution that have not yet been put into operation or made public" (s. 18(1)(f));

(x) "Information including the proposed plans, policies or projects of an institution where the disclosure could reasonably be expected to result in premature disclosure of a pending policy decision or undue financial benefit or loss to a person" (s. 18(1)(g));

(xi) A record subject to solicitor-client privilege (s. 19(a));

(xii) Information whose disclosure could threaten fish or wildlife species at risk (s. 21.1(1)).

(2) Requests for Personal Information: A request for personal information, such as grades on tests and papers, by the person to whom the information relates should be honoured – but normally such information should NOT be given to anyone to whom it does NOT relate – unless

(a) they actually need it to carry out the University's business (e.g. the Registrar's Office, Deans, Directors, Chairs), or

(b) you have the written consent of the person to whom the information relates to disclose it (e.g. to parents).

- Ideally grades should be posted only via Marks Management in "MyInfo," so students who request this information can simply be referred there.

- Note: students who want official copies of their transcripts must go through the official University procedures for ordering and paying for them. Students who inquire about official transcripts should be directed to the Registrar's Office.

(3) Students' Access to Their Own Personal Information:

(a) If an instructor keeps files on his/her students and a student requests access to information about him/her contained in those files, under *FIPPA* the instructor is obliged to provide that access – except to information (see *FIPPA* section 49)

(i) that is personal information about someone else;

(ii) that has been supplied in confidence AND is evaluative or opinion material compiled solely for the purpose of

1. assessing the teaching materials or research of the student;

2. determining suitability or eligibility for admission to an academic program; or

3. determining suitability for an honour or award for achievement or service.

(iii) that is medical information whose disclosure could reasonably be expected to prejudice the mental or physical health of the individual to whom it relates; or

(iv) that is a research or statistical record.

Always in such matters, however, check departmental and Faculty policy and consult with your Chair or Dean prior to disclosure. If there's any doubt about whether or not particular information should be disclosed, always feel free to consult with the Director of Risk Management and Access to Information

(b) If it is concluded that a student should be granted access to his/her personal information in a file in your office, you have the choice of allowing him/her to view the information on site or of providing him/her with a copy.

(4) Request Procedure: If a faculty member turns down a request for information, the requester should be informed that he or she has a right to make a formal Freedom of Information request under *FIPPA* in accordance with the procedures specified in the web site of the University's Office of Risk Management and Access to Information at http://riskandprivacy.lakeheadu.ca/.

(a) An "Information Access Request Form" has to be filled out and a fee of $5.00 must be paid for each such request.

(b) Upon receipt of the Form and the $5.00 fee,

(i) the Director of Risk Management and Access to Information determines where the requested information is held in the University and works with the Department or person in charge of this information to pull the records requested and to determine if any *FIPPA* exclusions or exemptions apply.

(ii) As allowed by *FIPPA*, fees are charged to the requester for the time taken to search for and prepare records for release.

(iii) If the information is to be disclosed, any personal or other excluded or exempted information is expunged from the copy given to the requestor.

(5) Faculty Members' Responsibilities to Protect Privacy

(a) Personal Information to Be Protected: *FIPPA* protects privacy by regulating the collection, use, disclosure, and destruction of personal information.

Remember that, as far as *FIPPA* is concerned, **"personal information" means recorded information that can, directly or indirectly, identify an individual**. Students' personal information thus includes

(i) records containing their names, identification numbers, gender, email addresses, telephone numbers, addresses, program and course enrolments, grades, health information, and their opinions and modes of expression.

(ii) Photographs and videos, as well as voice recordings, are also considered records bearing their personal information.

(b) Collection and Use of, and Access to, Students' Personal Information: As a course instructor you should not collect, access, or use any more personal information from your students than you actually need to conduct your course.

(i) Inform your students at the start of every course (e.g. in your course outline or syllabus) how their personal information will be collected and used.

(ii) In general, you do not have the right to consult a student's academic record outside your course or to access other personal information about the student which is not necessary for your course.

- Faculty who serve on appeals panels or who are charged with academic advising may confidentially access these records only to the extent necessary to discharge their duties.

- Senior Administrators, Deans, Directors, Chairs and their specified administrative staff may access records only for necessary

administrative purposes and are not authorized to share these records with faculty.

- If you think that you have a justifiable reason for consulting such records, apply to the Registrar.

(iii) The collection and use of still or moving images or identifiable sounds of your students must be necessary to your course/instruction/activity or there must be voluntary, informed consent from each individual involved before the images and/or sounds are collected and used.

(c) Disclosure of Students' Personal Information: An individual's personal information in your possession in consequence of your duties or activities as a faculty member should NOT be revealed to others unless one or more of the special grounds for disclosure listed in *FIPPA*, section 42 apply, chief among which are:

(i) the individual consents to the disclosure;

(ii) the disclosure is consistent with the purpose for which the personal information was obtained;

(iii) the disclosure is made to an officer, employee, consultant, or agent of the University who needs the record in the performance of his or her duties.

The University collects and uses personal information in order to be able to run its various, especially academic, operations effectively. Limited disclosure for this purpose is justified by the "consistency" principle in (ii) above. Hence the "collection notice" in the University's admission confirmation form advises new students that their personal information may be used and disclosed "as shall be necessary for the administration of the University and its programs." This principle applies within the classroom but, where personal information must be disclosed, always try to keep the disclosure to a minimum.

(d) Taking Attendance: Taking attendance can be regarded as indispensable to course administration - but be "privacy sensitive" as you go about it.

(i) Ideally a student's full name and complete student ID number should not be visible to others so, unless it really is necessary for practical purposes (as in larger classes), don't send attendance sheets bearing this information around the class for students to initial. If taking attendance is necessary, consider sending out blank, lined paper instead of detailed rosters and getting students to write down, say, only the last four digits of their identification numbers (although this will obviously entail more work for you or your GAs when you later try to match the attendance sheets to your class rosters).

(ii) In smaller classes, it is not a violation of students' privacy to require them verbally to confirm their presence at the prompting of roll call.

(iii) During examinations invigilators should walk around the room to verify student photo ID cards on a student-by-student basis and personally note the attendance on a roster that the students cannot see. Students should sign their individual exams.

(e) Group Work and/or Peer Evaluation: If group work and/or peer evaluation are integral elements in a course, disclosure of students' pertinent personal information to other students is permissible to the extent that it is required for the effective completion of these activities – but, again, be sensitive to privacy concerns; for example:

(i) At the beginning of the course, inform your students in your course syllabus about what personal information you will collect (e.g. names, telephone numbers, and/or email addresses) and how you will allow it to be used (e.g. to enable group members to communicate with each other and to develop work schedules). You may then request the students to provide you with the identified personal information.

(ii) Keep this information confidential and secure – disclosing it only to the extent necessary to realize the uses you have indicated in your syllabus.

(iii) Notify students if there will be any change in how the collected information will be used, and get the students' permission to use it in any new way that is not consistent with the purpose for which you collected it in the first place.

(f) Handling Assignments: The assignments that your students submit to you may contain a variety of personal information, including in each case the student's name, identification number, and personal views or opinions (so, for example, as the law is currently interpreted essays are considered students' personal information); hence, a good deal of confidentiality must be accorded to these assignments at all stages of your dealing with them:

(i) When you collect assignments:

1. If students submit their work in class, ensure that they cannot see each other's assignments.

2. If you cannot receive students' work in class, arrange for drop-off in your departmental office, GA office, or some place where assignments can be collected and held securely for your retrieval. Alternatively, your Department could provide a fixed, secure drop box or a mail slot in a central area. Submitted assignments should be retrieved as soon as possible.

3. Ensure that unsupervised methods of drop-off are reasonably resistant to circumvention efforts (e.g. so that mail-slot doors cannot be easily broken into, papers cannot be retrieved through the drop slot or from under the door, etc.).

(ii) When you mark assignments:

1. Write grades and comments inside test books, papers and other materials where they cannot easily be seen by others.

2. If grades or comments are easily visible on the external pages of a test book, paper or other materials, fold, staple or tape them closed so that the grades or comments cannot be seen. Alternatively, you might consider having each student submit a large, resealable envelope with their name on it along with each assignment or test so that their work can be confidentially returned to them in the envelope.

(iii) When you return graded assignments:

1. Assignments and class tests should be returned in each case only to the student who completed and submitted the assignment or test – unless the student consents in writing otherwise. They should not be left unattended in public places, such as the front of a classroom or outside an office, where anyone can pick them up and look through them (see the Senate policy entitled, Disclosure of Personal Information – Return of Graded Student Work at https://www.lakeheadu.ca/faculty-and-staff/policies/student-related/disclosure-of-personal-information-return-of-graded-studentwork).

2. Remember that, before you may release academic and personal information about a student to a third party (e.g. a parent or friend) other than a University officer who needs the information to perform his or her duties, the student must provide written consent.

3. The consent of the student is also required before his or her work can be published or used as an example in class – unless the work can be truly anonymized so that no class member can identify the author.

(g) Posting Grades: Ideally, students' grades should be posted only in the University's secure Marks Management system, where students can see only their own grades (see the Senate's policy, Disclosure of Personal Information – Posting of Student Marks at https://www.lakeheadu.ca/faculty-and-staff/policies/student-related/disclosure-of-personal-information-posting-of-student-marks).

- If you need any assistance in using Marks Management contact the Office of the Registrar.

- Moreover, be sure to inform your students in your course syllabus that all grade postings, whether in Marks Management or elsewhere, are provisional and unofficial - until they appear on the student's official University transcript.

If you do post grades outside Marks Management,

(i) Don't post by email unless it is encrypted or your students actually consent to posting by this means, since the confidentiality of unencrypted email cannot be guaranteed.

(ii) Make sure that public postings (e.g. on your office door) are anonymized so that students can identify only their own grades (hence students' names should not be placed beside their grades and the grades should not be listed according to the alphabetical order of student names).

(iii) For smaller classes (roughly 15 or fewer students) public postings should be avoided altogether, since, regardless of the absence of names, class members may still be able to figure out each other's grades.

(h) Getting Consent: It is recommended that you briefly explain in your course outline or syllabus which students receive at the beginning of your course what personal information you intend to collect from them and how you intend to use and disclose it. Provided that such collection, use, and disclosure are actually necessary to the teaching and learning experience in the course, students who continue their registration in your course will have, in effect, consented to the advertized collection, use, and disclosure.

(6) Correspondence

(a) Email Communications: Email offers a fast and convenient way to communicate with your students, colleagues, and others, but should, as has been noted above, be used with caution:

(i) Ideally you should send all messages only to students' Lakehead email accounts, because that is the only way you can be sure that you're sending information to the right addresses.

- If students insist on receiving email in accounts provided by other service providers, e.g. Hotmail or Yahoo, have them in each case request the privilege in writing, including the email address and their signature – and keep the consent on file.

(ii) Remember that, by the very nature of the technology, email communication, unless it's been encrypted, is fundamentally insecure: once it's been sent, it can be hacked into, copied, cached, and forwarded in altered form without your knowledge.

- To use the standard analogy, one should consider email communication as no more confidential than sending a postcard by mail.

- Be careful, then, about what you put in your emails; in particular try to avoid including sensitive confidential information, such as grades,

identification numbers, financial information, health information, or evaluative comments.

- When you're composing, keep in mind the general caution that anything you put in an email could end up on the front page of a newspaper!

(iii) Web CT can offer more secure communication with your students than can email – so you should use this service if you must communicate highly sensitive information to your students. Contact the Technology Services Centre or the Office of Continuing Education and Distributed Learning for more information.

(iv) The same precautions that you should take in email correspondence with your students apply to emails between yourself and other faculty, staff, administrators, colleagues at other institutions, and the public.

(b) Reference Letters: if you are asked to write a confidential letter of reference consisting of assessments and recommendations concerning any of the following subjects, provided that the letter does not go beyond an institution governed by *FIPPA* in Ontario, the assessments and recommendations will NOT have to be disclosed to the person assessed (see, in general, sections 49 and 65 of *FIPPA*):

(i) Teaching materials;

(ii) Research;

(iii) Employment;

(iv) Suitability, eligibility or qualifications for admission to an academic program;

(v) Suitability for an honour or award to recognize outstanding achievement or distinguished service.

- Be sure to post "CONFIDENTIAL" at the head of any such letter.

(7) Record Handling, Retention, and Disposal

(a) Security for Recorded Personal Information: Make sure that you keep all records in your possession bearing personal or other confidential information relating to University business reasonably secure:

(i) Ensure that records with sensitive information are not visible to visitors to your office or to anyone in the classroom or laboratory, whether the records are piled on your desk or apparent on your computer screen.

(ii) Keep your sensitive hard copy documents in a filing cabinet that can be locked when you are absent.

(iii) If you have sensitive records in your computer, make sure that you have adequate virus, spyware, and spam protection, that you back up your records, and that you keep your computer passwords private. You should also consider password protecting highly sensitive documents.

(iv) Make sure that you log out of your computer if you will be leaving it unattended for any significant period of time, and that you lock the door to your office when you leave it.

(b) Transporting Records with Personal Information: Try to avoid taking records bearing personal information out of their secure campus locations, but if you have to (e.g. for marking assignments or tests or calculating grades at home), make sure that you keep them secure both in their transportation and in their destination:

(i) There are horror stories about laptop computers full of personal information stolen from cars or hotel rooms (an egregious example: a physician's laptop which was carrying the personal health information of some 2900 patients from the Hospital for Sick Children in Toronto (see http://www.ipc.on.ca/English/Decisions-and-Resolutions/Decisions-and-Resolutions-Summary/?id=7616). The best practice when transporting sensitive records in such portable data storage devices is to encrypt them – passwords don't offer sufficient protection. Contact TSC for further information.

(ii) Both your hard copy documents and portable data storage devices should be locked in your car trunk, not left in the cabin which can be easily broken into.

(iii) No records of personal information should be left in a vehicle overnight.

(c) If Personal Information Records Are Illegally Accessed, Damaged or Corrupted, or Lost or Stolen: Report the problem immediately with full details to the Director of Risk Management and Access to Information. The University is obliged to report privacy breaches to Ontario's Information and Privacy Commissioner.

(d) Retention of Records with Personal Information:

(i) All records, including email communications, that

1. carry personal information,
2. relate to University business, and
3. have been used,

must be kept securely for at least one year – unless, in each case, the person to whom the personal information relates consents to the record's earlier disposal.

- Note that in some cases departmental, School, Faculty, or University practice or policy, or government regulation or law, may require retention for longer periods.

(ii) Since student assignments and tests come under the rubric of records of personal information, they too, in theory, must be securely retained for one year if they have not been picked up by the students who submitted them (see in particular the Senate policy on Retention of Examinations at http://policies.lakeheadu.ca/policy.php?pid=124).

- In some cases, however, such retention may be extremely inconvenient, if not impossible, due to lack of space. In these cases something like the following warning should be included in the course syllabus handed out at the beginning of term:

  "N.B. Students are advised that, due to lack of storage space, unclaimed graded assignments (except final examinations) will be destroyed at the end of the last month of the semester unless, in a particular case, the instructor considers that special considerations should apply or the student makes a special arrangement for return of his or her work. By remaining registered in this course, students will be deemed to have consented to this disposition of their unclaimed work."

- Keep in mind, though, that graded assignments and tests may be needed as evidence in appeals concerning grades or academic misconduct and so may, in any event, have to be preserved beyond the end of a semester. Check with your Department, School, or Faculty for policy and practice in this regard.

(iii) Each message in your telephone voice mail is considered a "record" under *FIPPA* – but Lakehead's new telephone answering service will automatically delete voice messages 28 days after you've listened to them. The best practice here is to transcribe into a notebook or file a summary of each message.

- If the summary carries personal information relating to University business that is used, it too must be preserved for at least one year.

(e) Retention of Other Records:

(i) Non-Personal Records of Significance to the University's Operations: *FIPPA* imposes NO period of retention on records that do NOT carry personal information – but some records in this category, which can be generally classified as official University records and which serve important business functions, such as supporting program delivery or policy development, or dealing with legal, financial, and other needs, do nevertheless have sensitive

information that may have to be preserved for some time. Check with your Department, School, or Faculty.

(ii) Transitory Records: Records that have only limited, temporary significance or applicability are generally classified as "transitory records." They are NOT protected by *FIPPA* or other laws, regulations, or University policies and should be disposed of as soon as their usefulness has ended. Examples of transitory records include (but are not limited to):

1. Redundant duplicates of other documents;
2. Rough notes superseded by a final document;
3. Appointments and meeting schedules;
4. Communications bulletins;
5. Unsolicited advertising materials;
6. Email, phone, and other messages that do not relate to University business (e.g. spam!).

(f) Disposal of Records:

(i) When you dispose of records (including transitory records) that you have used which bear personal information relating to University business, ensure that you take reasonable steps to protect the security and confidentiality of the records throughout the destruction process. Ideally hard copy documents should be confidentially shredded, and make sure that electronic documents have not been left in your computer's trash file, but deleted forever.

(ii) When you destroy a record of personal information, note the general category of the record, its date of composition, its date of destruction, and the method of destruction (e.g. "student email re course requirements, composed between January 1 and December 31, 2006, disposed of January 31, 2008 by deletion"). Keep this disposal information in a retrievable file – whether hard copy or electronic.

(8) Faculty Members' Personal Information and Privacy

(a) Personal Information re Professional Duties: Under *FIPPA* personal information related to an individual's role and activities in a professional capacity is NOT protected from general disclosure (see, e.g., *FIPPA* section 2(3)). Hence faculty members' names, academic and professional credentials, professional titles, and institutional addresses, telephone numbers, fax numbers, and email addresses, can all be included in the University's public directories.

(b) Personal Information NOT Associated with Professional Duties: Personal, non-University addresses, telephone numbers, and email addresses, as well as portrait photographs, voice recordings, and all other purely personal information not connected with faculty members' professional University duties CANNOT be published without the faculty members' permission – except to the extent (and ONLY to the extent) that such information is needed for security purposes or to

provide access to University facilities (e.g. the Library, swimming pool, etc.). Disclosure of this kind of personal information for these purposes can be made, normally, only within the institution to employees, contractors, or volunteers who actually need the information to perform their duties.

(c) Employment Records: *FIPPA* excludes most employment-related records from its jurisdiction (see section 65(6) of the Act) and so authorizes neither protection of nor access to these records. Consequently the Collective Agreement between the University and the Lakehead University Faculty Association (LUFA) governs access to and protection of most information in faculty members' employment records (see in particular articles 12 and 14 of the Collective Agreement).

****