Information and tips on how to keep you FIPPA FRIENDLY
Ontario universities were made subject to provincial Freedom of Information and Protection of Privacy Act (FIPPA) as of June 10th 2006.

OTHER PRIVACY ACTS YOU MAY HAVE HEARD OF:

- **PHIPA (PROVINCIAL)**
  - Personal Health Information Protection Act

- **PIPEDA (FEDERAL)**
  - Personal Information Protection and Electronic Documents Act

- **ATIP (FEDERAL)**
  - Access to Information Act
  - Privacy Act
In a university context FIPPA has three main purposes:

1) To provide all members of the public with the right to access all non-personal information in university controlled records. This right is limited only by specific exclusions from jurisdiction and exemptions from disclosure.

2) To provide individuals whose information is held by the university with the right to access their own information that is held by the university, to make corrections to their personal information when necessary and attach a statement of disagreement when a correction is requested but not made.

3) To protect the privacy of personal information held by the university by setting uniform standards for the collection, use, disclosure and destruction of that information.
PERSONAL INFORMATION is factual or subjective data. It includes, but is not limited to, details such as one’s name, home address and telephone, email address, student number, gender, age, martial status, health information, religion, education history (courses taken, grades and evaluative comments), employment history, opinions and financial data. It is data (either singly or in combination) that makes a person uniquely identifiable.

FIPPA legislation in Ontario protects personal information from unauthorized collection, use and disclosure.

Personal information does NOT include an individual’s business contact information. Their professional title, phone, email, address and fax number at their place of employment can all be made publicly available.
For a full definition of **Personal Information** please see Section 2 of FIPPA. You can access the legislation through Carleton’s FIPPA site at:

http://www.carleton.ca/privacy

**Note:** Until an individual graduates, **all information pertaining to their academic history is considered to be personal information** and is treated as confidential by the university. All inquiries about current students (or former students who did not graduate) no matter who from (including media or parents) is to be met with the same response – we cannot confirm or deny enrollment.
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.

A complete definition for this term can be found under Section 2(1) of FIPPA.
FIPPA requirements for the collection and use of personal information.

- Collect only the information needed to perform our lawfully mandated functions.

- Use the information we collect only for the purpose for which it was collected or for a consistent purpose.

- Undertake not to disclose personal information other than to the individual to whom it relates (except in the limited circumstances specified by FIPPA).

- Inform people when we collect their personal information and make clear what we intend to do with the information.
Can we ask a student for personal information?

Yes – but only as necessary for course or program delivery. Also, we must inform the student of the purpose for which the information is being collected. For example, emails may be collected to facilitate group work or seminar attendance. However, this information may not be used for another purpose without the consent of the student and should be kept only as long as necessary for the course.

Can we take attendance?

Yes – but try to be privacy aware. In a smaller class, answering to a name roll call is not an invasion of privacy. In larger classes, the use of complete student numbers on sign up sheets is discouraged as is passing around a class list of names and associated student numbers to initial.
Collection notices are necessary when asking a student for their personal information.

The collection notice states under what authority personal information is collected (the specific section of FIPPA) and makes a commitment not to use the information for a purpose other than that for which it was collected without consent. It must also include the name of a university contact person who can provide information about the application of FIPPA to the personal information being collected and who can provide information about gaining access to the information. A standard collection notice can be found at:

http://www2.carleton.ca/privacy/ccms/wp-content/ccms-files/collection_general.pdf

Contact Carleton’s Privacy Office for advice if you are unsure when collection notices are necessary.
There are two principles at work when deciding to share student information within the university. One is that FIPPA allows the sharing of information within the institution in order to do our jobs. This is covered by the statement in the FIPPA legislation to the effect that we will only use the information we collect for the purpose for which it was collected or a consistent purpose. The second is that, even within the institution, information is only to be shared on a need to know basis.
Section 42(1) of FIPPA speaks to the usual circumstances under which personal information may be disclosed.

- With direct consent from the individual to whom the information relates.
- For a purpose consistent with the purpose for which it was originally collected.
- Where necessary to facilitate the completion of one’s duties as associated with an employment position at the university.
Can we have access to personal information in a student record?

Yes – However, access to the information in a student record is given on a “need-to-know” basis. The level and nature of access should be directly related to the duties of the individual requesting access. An instructor will need to know whether someone is registered in their class but this information should be obtained from the administrator responsible for records of class enrollment and registration and not from the student record.

Can we share personal information about my students with other university employees?

Yes – But only with the employees whose duties and responsibilities authorize them to have access to that information and who need the information in order to carry out their duties.
Can we post student grades in a public place?

Ideally marks should only be posted in the secure environments of WebCT or Carleton Central. If it is necessary to post marks in a public place, steps should be taken to make the individuals anonymous. For example, use only the last four digits of the student number and scramble the order. Do not leave graded assignments in a public place for pick-up. Grades and comments should be written on an inside page.

Can we post student personal information on web pages or include it on CVs?

Yes- as long as we obtain their permission first. An email is sufficient to include information on a CV but to publish biographical information on web pages or to use student information for promotional purposes, a more formal consent should be obtained. See the Provost’s Faculty Resources for the “Consent to Publish Student Information Form” (http://www2.carleton.ca/provost/ccms/wp-content/ccms-files/Consent_Student_INFORMATION.pdf).
Can we give references for students and employees?

Yes – However, sharing personal information outside of the university should only take place with the consent of the individual. This consent may be obtained by the person or institution requesting the reference or it may be obtained directly from the student. Be sure to have written proof of consent (an email from the student will suffice) and keep it for at least one year. Without consent you are not at liberty to disclose any information about the individual – that includes confirming whether or not the student attends Carleton (or attended in the past and did not graduate) or worked in your department.
Access to confidential letters of reference

The assessments and recommendations included in a letter of reference do not have to be disclosed to the subject named in response to a request for access to information (as per sections 49 and 65 of FIPPA). This includes assessments of:

- Teaching Materials
- Research
- Employment
- Suitability, eligibility or qualifications for admission to an academic program
- Suitability for an honor or award to recognize outstanding achievement or distinguished service.

The disclosure of references and evaluations pertaining to Carleton faculty and instructors is governed by the application of the applicable Collective Agreement.
What if it is an emergency? Can I disclose personal information without permission?

Yes - FIPPA does not require that permission be obtained before disclosing personal information in the event of an emergency, (whether to someone inside or outside the university). FIPPA allows for the disclosure of personal information in exceptional circumstances such as those relating to protection of health and safety or for compassionate reasons. The Student Mental Health Framework (https://www2.carleton.ca/studentsupport/ccms/wp-content/ccms-files/Carleton-University-Student-Mental-Health-Framework.pdf), specifically those sections on Communication and Documentation and Notification Protocols) gives more information on determining when and to whom to disclose information in the event of an emergency. Consult with the Director of Student Affairs or the Privacy Office if time allows; if not, use your best judgment.
How long do we keep personal information?

FIPPA mandates that all records (including email) that carry personal information and that relate to university business must be kept for a minimum period of one year – unless the individual to whom the information relates consents to earlier disposal.

In some cases the operational requirements of the university or government regulation will require that records be retained for longer periods.

Exams, essays and other student work should be kept as long as is necessary for the student to exhaust all avenues of appeal or at least one year – whichever is longer. Most departments keep student work at least 18 months.
Once it is no longer necessary to keep copies of student work it should be disposed of in the departmental shred bin or shredded before disposal.

DO NOT PUT COPIES OF STUDENT WORK (or any other record still containing student personal information) IN THE GARBAGE!
FIPPA requires that the university protect personal information from unauthorized access, use and disclosure.

- Avoid keeping personal information on removable storage devices (usb keys, laptops, blackberries) that are not encrypted. Paper documents (such as student papers) and data devices should be locked in the trunk not left on the seat and should never be left in a car overnight.
- When communicating with students by email attempt to confirm their identity before disclosing personal information. One way to do this is through the use of a ‘Connect’ account.
- Ensure personal information that may be on your desk or on computer screens is not visible to visitors to your office. Log out of your computer if leaving it unattended. Keep sensitive personal information in a locked cabinet when you are not present.
What is a privacy breach?

A privacy breach is an incident involving the unauthorized disclosure of personal information in the custody or control of Carleton. This would include personal information being lost or stolen, accessed by unauthorized persons or disclosed outside the parameters allowed by FIPPA.

You must contact the Privacy Office immediately if you believe a privacy breach has occurred.

A breach does not necessarily constitute non-compliance with FIPPA, but failure to correct any faulty practices or procedures within your department or office could lead the university to be assessed penalties under the Act. Contact the Privacy Office if you have further questions.
FIPPA allows the disclosure of personal information for research purposes if,

- the disclosure is consistent with the conditions or reasonable expectations of disclosure under which the personal information was provided, collected or obtained,

- the research purpose for which the disclosure is to be made cannot be reasonably accomplished unless the information is provided in individually identifiable form, and

- the person who is to receive the record has agreed to comply with the conditions relating to security and confidentiality prescribed by the regulations; or

- if the disclosure does not constitute an unjustified invasion of personal privacy. R.S.O. 1990, c. F.31, s. 21 (1).
The following are the terms and conditions relating to security and confidentiality that a person is required to agree to before a head may disclose personal information to that person for a research purpose:

1. The person shall use the information only for a research purpose set out in the agreement or for which the person has written authorization from the institution.

2. The person shall name in the agreement any other persons who will be given access to personal information in a form in which the individual to whom it relates can be identified.

3. Before disclosing personal information to other persons under paragraph 2, the person shall enter into an agreement with those persons to ensure that they will not disclose it to any other person.

4. The person shall keep the information in a physically secure location to which access is given only to the person and to the persons given access under paragraph 2.

5. The person shall destroy all individual identifiers in the information by the date specified in the agreement.

6. The person shall not contact any individual to whom personal information relates, directly or indirectly, without the prior written authority of the institution.

7. The person shall ensure that no personal information will be used or disclosed in a form in which the individual to whom it relates can be identified without the written authority of the institution.

8. The person shall notify the institution in writing immediately if the person becomes aware that any of the conditions set out in this section have been breached. R.R.O. 1990, Reg. 460, s. 10 (1).

An agreement relating to the security and confidentiality of personal information to be disclosed for a research purpose shall be in Form1. R.R.O. 1990, Reg. 460, s. 10 (2).
With limited exceptions, FIPPA does not apply to records about or associated with research or records of teaching materials.

Research records include records that are collected, prepared and maintained for a research purpose. The research may be proposed, in progress or completed. Research may be conducted or proposed by a university employee, student, research assistant, private research partner or other individual, group or organization associated with the university.

Teaching materials are records that are collected, prepared and maintained for a teaching purpose.

Records of research and teaching may be found in all media and may be stored on campus or elsewhere.

Despite the fact that FIPPA does not apply to records of research, the subject-matter and amount of funding being received with respect to the research shall be disclosed in response to an access to information request.
Can the public obtain access to teaching materials and/or research-related records?

No – Most research-related records and teaching materials are excluded access under FIPPA. This includes material such as research and study notes, reports, manuscripts, and publications - unless they were specifically commissioned or prepared under contract for the University or in the context of administrative work.
Normally, a formal request for access to information is not an issue that will impact heavily on your work.

In general, if you are asked for information that you would normally provide such as a course syllabus or outline, a reading list or copy of an assigned reading you should provide that information. You should also provide personal information – such as grades on tests and papers - if it relates to the student making the request.

If a request for access involving records from your area is received by the Privacy Office, your department will be contacted with a description of the records requested. Although you may believe that the records requested are not accessible under FIPPA, this is a decision that will be made by the Privacy Office.
If someone submits a formal request under FIPPA, can my e-mail communication be released?

Yes - Faculty and staff e-mail, personal mobile device files, and even home computer communication on university matters may be disclosed under FIPPA and therefore care and professionalism should always be exercised when communicating by e-mail.

Does FIPPA apply to the records of faculty that are created as part of professional or volunteer work performed outside of regular employment with the university?

No - FIPPA does not apply to records that are personal to you. However, to prevent confusion these records should be kept separate from the records related to your duties for the university. Avoid the use of university e-mail to transmit personal information. If university email is used, create a separate ‘Personal’ folder for these items.
Carleton’s Privacy Office is your best resource should you have any questions about the practices and procedures at Carleton regarding the FIPPA.
Should you have any questions concerning FIPPA and its role in your department please feel free to contact us:

**Cheryl Foy**  
University Secretary, General Counsel and Privacy Officer  
607A Robertson Hall  
Carleton University, 1125 Colonel By Drive  
Ottawa, ON, Canada, K1S 5B6  
Tel: 613.520.2600, Ext.2054  
Fax: 613.520.3731  
E-Mail: cheryl_foy@carleton.ca

**Linda White**  
Corporate Archivist and Assistant Privacy Officer  
607 Robertson Hall  
TEL 613.520.2600 ext 2935  
FAX 613.520.3731  
E-mail: linda_white@carleton.ca