

Privacy Guidelines and Confidentiality Statement
for the Office of the Dean of Students & Residence, Innis College
(updated February 2016)

Privacy Guidelines

The University's Notice of Collection for students reads as follows:

The University of Toronto respects your privacy. Personal information that you provide to the University is collected pursuant to section 2(14) of the University of Toronto Act, 1971. It is collected for the purpose of administering admissions, registration, academic programs, university-related student activities, activities of student societies, financial assistance and awards, graduation and university advancement, and for the purpose of statistical reporting to government agencies. At all times it will be protected in accordance with the *Freedom of Information and Protection of Privacy Act*. If you have questions, please refer to www.utoronto.ca/privacy or contact the University Freedom of Information and Protection of Privacy Coordinator at 416-946-7303, McMurrich Building, room 201, 12 Queen's Park Crescent West, Toronto, ON, M5S 1A8.

To this end we,

- always write in a professional manner, including in emails;
- keep official records needed for operations or to demonstrate due diligence;
- destroy transitory records on an on-going basis;
- only use or disclose personal information for the purpose it was collected or a reasonably consistent purpose; or with the individual's consent; or within the University on a need-to-know* basis; or in emergencies and to reduce threats to health or safety; and
- protect personal information.

*Need-to-know means that you may disclose personal information to a University employee, officer, agent or contractor who needs the information to perform official, proper University duties.

Information in the Office of the Dean of Students & Residence is strictly confidential and must always be protected with strong security. The following required practices will help us to effectively protect privacy.

Electronic information

1. Student personal information is confidential and should never be transported outside the office, whether on a laptop or a portable storage device such as a USB key, even in encrypted form. Student information should never be kept on a home computer. Any exceptions must be approved in advance by the Dean of Students.
2. Personal information (such as name, student number, contact, academic or financial information, etc.) should not be stored on local devices (e.g. your computer hard drive or a USB key). This information should be in ROSI or on the secure network environment of the Dean of Student's Office. Any exception, which requires local storage, must be approved in advance by the Dean of Students and the information must be encrypted.
3. Always use a strong password to access UTOReMail remotely.
4. Official University email (UTOR address to UTOReMail address), is considered to be secure, but other external email (such as your Gmail or Yahoo account) is not. If email containing personal or other confidential information must be sent to a non-UTOR address, the personal/confidential information must be sent as an encrypted attachment (PDF, Word document, Excel spreadsheet, etc.) and the password must be sent to the recipient of the email using another secure means, such as the telephone.

5. Regardless of the content, when sending electronic messages to groups of students, always use either a listserv or the mail merge function in Microsoft Office.
6. If any personal information is lost, stolen or inappropriately accessed/disclosed, immediately notify the Dean of Students and FIPP Office. Often the consequences can be minimized with quick intervention.
7. Ask IT staff to securely destroy confidential electronic information that is no longer needed.

Paper documents

1. Paper records containing student personal information are confidential and should not be transported outside the office unless necessary. This should only be done with prior written approval of the Dean of Students and with effective security.
2. The front desk of the Residence, nor the Office of Student Life should be left unattended or unsecured, unless a full-time appointed University staff member has a view of the desk and is in a position to prevent unauthorized access to confidential information at the desk.
3. If leaving the office for any period of time during the day, lock your computer and (if practical) also lock your office door.
4. Place personal and/or confidential information in locked cabinets overnight, thereby ensuring that documents are protected behind two levels of locks – one on the building and/or office, and another on the cabinet.
5. Always use a cross-cut shredder to destroy confidential paper records.
6. If any personal information is lost, stolen or inappropriately accessed/disclosed, immediately notify the Dean of Students and the University's FIPP Office. Often the consequences can be minimized with quick intervention.

Parents and third parties (including professors who are parents)

1. We often receive requests from parents or other third parties for access to student information. Ontario privacy legislation prevents us from sharing any personal information with a third party unless the individual (e.g. the student) has consented. This includes the fact of registration. In order to share any student information with a parent, we must have written authorization from the student, or have the student present at the time of sharing. Written authorization from a student for release of information to a third party should be limited to one discrete transaction or goal at one time.

Emergency situations

1. We have an obligation to provide personal information in compelling circumstances that affect the health or safety of an individual, where providing that information would help. Emergencies, health and safety trump privacy.

Acquaintance with applicants and students

1. It sometimes happens that we know or are related to an applicant or student. In such situations, inform the Dean of Students immediately and take particular care to avoid any unnecessary discussion of the applicant or student.

If there are any questions or special requirements with regard to these issues, please feel free to discuss them with the Registrar of Innis College. Further information is provided in "Access and Privacy Practices: General and Administrative" at:

<http://www.provost.utoronto.ca/Assets/Provost+Digital+Assets/Provost/Provost+Digital+Assets/Provost/fippa.pdf>

Confidentiality Statement

Records of Innis College undergraduate applicants, students and alumni are the responsibility of Innis College.

Such records, regardless of form or medium, may contain sensitive information, including:

- personal information required in the administration of official student academic records;
- registration and enrolment information;
- scholarships, awards and bursary information;
- results for courses and academic periods;
- evaluations of students' academic performance;
- results of petitions and appeals;
- professional/medical information;
- letters of reference;
- personal and biographical information.

All staff of the Office of the Dean of Students & Residence (student staff members or administrative staff, volunteer or paid), have access to relevant portions of students' records in the performance of their duties. This information is confidential, and it is a key responsibility of the Office of the Dean of Students & Residence to ensure that these records are kept confidential and secure.

Staff members of the Office of the Dean of Students & Residence are permitted to access only the personal information required to fulfil job responsibilities. Information must not be released to or discussed with anyone other than the individual whose information is involved, or other staff in the Office or elsewhere at the University who need the information to do their jobs.

As a member of the Office of the Dean of Students & Residence, I understand that I shall have access to personal and other confidential information, including student records – academic and other – in the performance of my duties. I also understand that this information cannot be discussed outside the context in which it is raised, nor for other purposes than those for which it is available to me, outside the University of Toronto, and can only be shared within the University on a need-to-know, or emergency, health or safety basis.

By signing this form, I confirm my understanding of the responsibilities accorded those who have access to student and other confidential information and records. Furthermore, I confirm that I understand and agree to abide by the requirements and guidelines of the University of Toronto regarding confidentiality of student records and the requirements of the Freedom of Information and Protection of Privacy Act.

Name

Signature

Date

Date Received by the Registrar