Posting Student Personal Information on Websites

Posting student personal information (e.g., student photos) on a public website or even a password accessible site available to other students, must be done with caution. Because of the public nature of such websites, inappropriate postings of some types of information may cause significant harm to students.

Advise students in advance that their personal information will be posted electronically. In most cases you will need to obtain their consent or give them an opportunity to opt out. For more information contact your Faculty Liaison Officer or Western's Information and Privacy Office.

Communicating Health or Safety Concerns

FIPPA does not preclude communication within the University where there are serious concerns about a student's health or safety. If you are concerned that a student may harm him or herself or others, immediately contact Campus Community Police Service. A student's consent is not needed. Any disclosures to parents or other third parties will ordinarily be handled through Campus Police or Housing.

E-mail Use

Ensure that e-mail recipients are correctly identified and that they are not sent personal information not intended for them. If the information is particularly sensitive, password protect or encrypt the message. Contact ITS, your Liaison Officer or Western's Information and Privacy Office for more information.

Security and Retention of Personal Information

You must safeguard the security of student personal information in your custody, whether the information is contained in a paper record or in an electronic file. Exercise extra care if the personal information is taken off-campus. Use passwords to lock the system or information on the mobile device or laptop. If you must transport sensitive information, use encryption software to encrypt the information effectively and securely.

FIPPA requires that all records (including e-mail correspondence) containing personal information that is "used" by the University be retained for at least 12 months, unless the individual to whom the information relates agrees to a shorter period. You should be particularly scrupulous about retaining for the 12-month period all correspondence to or from students that contains personal information used for evaluations, grading, appeals, counselling, or other academic purposes. Longer retention periods for certain types of information may be required under various University policies or under the University's Records Retention and Disposal Schedules. Contact Western Archives for further information.

What is a Privacy Breach?

A privacy breach is an unauthorized collection, use, or disclosure of an individual's personal information. Misplaced or improperly stored files, stolen laptops, and inadvertent disclosures (e.g., in an e-mail) are common sources of privacy breaches.

What to Do if a Privacy Breach Occurs

Notify your Department Chair and Dean immediately if you become aware of a possible privacy breach involving student personal information. They will ensure that the relevant units, including Western's Information and Privacy Office, are notified so that immediate steps are taken to contain the breach.

WHO TO CONTACT FOR MORE INFORMATION

Your Liaison Officer and Alternate

See up-to-date list available at
<http://www.uwo.ca/privacy/liaison.html>.

Western's Information and Privacy Office

Chris Graves, Information and Privacy Coordinator
Terry Morrissey, Associate University Secretary and Director, Information and Privacy Office
Tel: 519-661-2111, ext. 84541 or 84543
E-mail: privacy.office@uwo.ca
Website: http://www.uwo.ca/privacy

PROTECTING STUDENTS' PERSONAL INFORMATION:

A Guide for Faculty and Staff

Western

Western's Information and Privacy Office
May 2009

This brochure provides a brief overview of some key requirements under provincial legislation and University policies with respect to the collection, use, and handling of student personal information, as well as some recommended "best practices".

Freedom of Information and Protection of Privacy Act (FIPPA)

The Freedom of Information and Protection of Privacy Act is the Ontario public sector legislation that governs the University's handling of personal information. The legislation authorizes the University to collect and use only such personal information as is needed for the purposes of its various programs and activities. It also includes requirements relating to how personal information is collected and standards for handling it once it is in our possession.

Definition of Student Personal Information

FIPPA defines personal information as "recorded information about an identifiable individual". Student personal information includes home address, home phone number, personal e-mail address (non-UWO account), ID photos, opinions and assessments of or about the student, education history, medical information, student or other identification numbers, marks, grades, and needs-based financial information.

"Public" Personal Information

The Senate-approved Official Student Record Information Privacy Policy states that the following student information is considered to be publicly available and will be provided to third parties upon request: name, degree and date of graduation, Faculty or School and major field of study, merit-based awards and scholarships. However, a student may request that this information cease to be made publicly available by contacting the Office of the Registrar. All requests for such information should be referred to that office.

Queries from Parents and Other Third Parties

You may not reveal information (e.g., admission information, grades) about students to parents or other individuals without the consent of the student, regardless of the student's age.

Access to and Use of Student Personal Information

Under FIPPA, the University and its employees may collect, use and share student personal information to the extent necessary to administer University programs and activities. However, the University must notify students of the purposes for which their personal information will be collected or used. To comply with this requirement, the University has drafted a broadly worded "Collection Notice" that covers most of the regular uses of student personal information across the University (see <http://www.registrar.uwo.ca/Security.cfm#privacy> and <http://grad.uwo.ca/section_one.htm>). If you plan to collect particularly sensitive information, contact your Faculty Liaison Officer to find out if a separate notice is needed. If so, Western's Information and Privacy Office will work with the Liaison Officer to draft a notice that complies with FIPPA.

Access to Student Academic Records

Senate policies stipulate that students' academic records are confidential and that access is restricted to faculty and staff who have a legitimate need for the information in order to carry out their responsibilities as they relate to the administration of student affairs. For example, an instructor sitting on a scholarship committee would have the right to view certain academic records. Access to portions of an academic record may also be permitted with the consent of the student.

Access to Student Medical Information

Students often provide medical information when requesting academic accommodation for an illness. You must handle such information with particular care and share it only on a need to know basis.

Instructors are prohibited under Senate policy from collecting medical documentation from undergraduate students seeking accommodation for illness. Students must submit medical documentation directly to the appropriate Dean's Office which is required to hold the records in confidence.

Sharing Student Personal Information in the Classroom or with Off-Campus Institutions

If a course or program requires students to share their personal information with the instructor or their classmates (e.g., resumes), or if their personal information will be provided to off-campus institutions (e.g., placement sites), inform students of this requirement prior to, or at the outset of, the course or program (e.g., in course or program material or a course outline). Ensure that students are not asked to share more information than is required for the purposes of the course or program.

Communicating Grades to Students

Senate has set out rules on how final grades are to be communicated to students. The electronic posting of grade lists with personal identifiers is prohibited. If final grades are to be communicated electronically, they must be communicated on an individual basis and, currently, WebCT* is recommended for optimal security. Paper lists of grades linked to student numbers may be posted in a Department for larger classes only (15 or more students) provided that the student numbers are truncated and listed in random order and provided that the Department is satisfied that the grades cannot be linked to individual students.

These rules should be followed when communicating other, non-final marks to students. Communicating marks by e-mail, even to individual students, is not recommended.

Returning Marked Assignments and Exams to Students

Return marked assignments, tests and examinations to students in a manner that does not reveal the responses or grades to others. Senate policy requires that student assignments, tests and exams be handled in a secure and confidential manner and prohibits leaving student work in unattended public areas for pickup.

---

* Faculty and staff can consult with ITS about different software that may become available over time.