FIPPA - Q and A's for Instructors

Advice regarding the Freedom of Information and Protection of Privacy Act (FIPPA)

This advice guides best practices for student-faculty interactions in the context of reasonable privacy expectations. It should always be consistent with applicable U of T policies. This will help you to comply with FIPPA by following sound privacy practices.

Handling of Assignments

Purpose and Objective

This practice provides guidance on how best to collect, handle and return students work.

Checklist

☐ 1. Write grades and comments inside test books, papers and other work, where they cannot be easily seen by others. Fold and staple or tape test books, papers and other work closed, to ensure that grades and comments are not visible to others students when materials are returned to the student.

☐ 2. Collect student work with adequate supervision and security so students cannot see each other's answers/work or evaluations. Ideally, collect assignments in class under supervised conditions. If this is not possible, arrange for drop-off in your departmental office, TA office, or some place where assignments can be collected and held securely for your retrieval. Alternatively, provide a fixed, secure drop box or a mail slot in a central area. Retrieve submitted assignments frequently. Ensure that unsupervised methods of drop-off are reasonably resistant to circumvention efforts (i.e. mail-slot door cannot be easily broken into, papers cannot be retrieved through the drop slot or underneath the door, etc.)

☐ 3. Return work in class or with another supervised or secure method so that student work or evaluations never become available or visible to others. Never leave them in a public place for pick up. Return assignments only to the student responsible for the work and not to other individuals, unless written permission was given. Reveal grades or evaluations only to the individual responsible for the work.

Retain all unclaimed student work, including final exams, for **one year**, and then arrange for them to be securely destroyed. Divisions should have or develop policies on the confidential disposal of unclaimed work.

Background

Student assignments contain personal information of students, including the student number, name, and answers, personal views or opinions contained in the assignment.

The above practices should be adapted in courses where peer evaluation and/or group work are established or necessary parts of a program or curriculum. In such cases, students may require access to or knowledge of each other's work and evaluations. Students in such programs should be notified of ways in which their work, evaluations, and other personal information will be accessible to other students.

Posting of Student Grades

Purpose and Objective

This practice provides guidance for posting of students grades.

Checklist

☐ 1. Reveal grades and evaluations of tests and assignments only to the student to whom they pertain. Use **secure** electronic media, such as Blackboard, so individuals see only their own grade.

☐ 2. If secure electronic media like Blackboard are unavailable, and results **must** be posted, use truncated student numbers (e.g. last four digits only) to minimize the likelihood of students identifying each other's grades.

☐ 3. At the start of each session, advise students how you will post their grades (what fields will be posted, the location and duration of the posting). For example, you might post grades at one or two of your lectures for ½ hour before and after the lecture. Such limited posting limits exposure of grades and reduces the likelihood of students identifying each other's results.

☐ 4. In order to release academic and personal information of a student to a third party (e.g. a parent), the student must provide written consent. The student's consent is also required when their work is to be published or used as an example in class. If any doubt exists about the validity of a consent, verify it by asking the student.

Background

Student grades and identifiers, including student numbers, are personal information. Advise students that posting of grades is a courtesy to give them early notice but official grades are provided through ROSI.

Taking Student Attendance and Group Work Signup

Purpose and Objective

This practice provides guidance for taking attendance at class and exams and how best to have students sign up for group work.

Checklist

☐ 1. Collection of information about the presence or absence of a student is necessary. Collect only the information that you need to verify a student's presence.

Inform students at the start of the course how their personal information, including attendance, will be collected. Take attendance at lectures, seminars and labs as needed, but be sensitive to how this information is gathered, especially if you are using or generating a written list that students may view or photograph as it comes to them. The student's full name and complete student number should not be visible to others. If you wish to take attendance in writing, one option is to pass around sheets where students can record the last four digits of their student number. It is acceptable to take attendance verbally.

Adapt the above for group work practices or peer evaluation in your curriculum, e.g. ask students at the beginning of term to provide the personal information necessary to conduct the class. This may include name, phone number and/or e-mail addresses to share with fellow students so that group work schedules can be developed. Give clear notice of how this information is to be used, then keep it confidential and notify students if there is a change to how the information is to be used. Obtain the students' consent to use it in any new way that is not consistent with the purpose(s) for which you collected it.

Do not disclose student personal information to anyone except for the performance of their University responsibilities. If you receive an inquiry from someone other than the student, refer it to the student's registrar.

☐ 2. Where written proof of attendance at final exams is necessary, students should provide it so that their personal information (i.e. their presence or absence) is not easily known or captured by others. Do not circulate an attendance list that allows students to learn each other's personal information such as full name, full student number or their presence/absence.

A good practice is to use individual attendance forms or cards which are given to each student, and which ask for the date, their full name, full student number, course number and session, instructor's name, and their signature. (See sample here) Such a form is completed at the beginning of the exam, and placed beside (or face down on top of) their student photo ID card on the examination desk. Invigilators should walk around the room to verify student photo ID cards on a student-by-student basis, noting the attendance on a sheet of names and numbers. Students should sign their individual attendance form in the presence of the invigilator as the forms are collected. Keep attendance forms for each exam in a secure place for at least one year and then destroy, along with the exams.

☐ 3. For students signing up for group work, use practices that do not require students to reveal unnecessary personal information to other students. Ideally students should have access to secure, confidential electronic group sign-up.

These practices are unnecessary where it is appropriate or necessary for students to know each other and interact to do group work or to develop academic or professional communities. The group work purposes and context will help determine appropriate practices for the class.

Where confidentiality is appropriate, consider using available secure electronic sign-up methods, post sign-up sheets with tear-off tabs, or provide coded cards for each session in class so students can fill in and return the tab or coded card to you confidentially. Otherwise, you may elect to use a supervised sign-up sheet in class. In this case, it is best if each successive entry on the sheet is covered so that previous students' information is not visible to students who receive the sheet later. Avoid the use of unsupervised student sign-up sheets.

Background

The presence or absence of a student is the personal information of that student. The University's Notice of Collection informs students that their personal information is collected, among other things, "for the purpose of administering admissions, registration, academic programs…" Verification of attendance and the identity of students in class and at exams is a necessary activity in the delivery of the University's academic programs. Conduct verification in the least privacy-invasive manner consistent with course and program requirements.

E-mail correspondence with and about students

Purpose and Objective

This practice provides guidance for conducting e-mail correspondence with students, faculty and administrators.

Checklist

☐ 1. Do not use unencrypted e-mail to communicate personal information. The security of unencrypted e-mail has been compared to a postcard.

Handle e-mail containing sensitive personal information, (e.g. student educational or medical history, financial information, special arrangements about course work, evaluations, etc.), with particular care. Consider keeping sensitive e-mail in a separate folder(s) if practical.

Retain e-mails from and to students containing personal information which you ***use*** (e.g. in evaluation or to advise them) for at least one year after the last use, like all other personal information that you use in University business. Information used for making official decisions, or that has an effect on a student's rights, can be requested or revisited during the minimum one year retention period. Examples include correspondence about accommodations, re/evaluations, appeals, and sanctions. In these cases, archive relevant e-mail in folders.

Avoid "reply all" responses where practical. If you need to communicate with a group of students, use "bcc" to avoid disclosing recipient identities to the whole group, and to prevent the over-distribution of subsequent exchanges. Consider creating individualized e-mail messages to a single group, like a class. If necessary, consider asking for IT advice on methods. *Blackboard* has options for creating individualized messages to each class member.

☐ 2. Advise students at the start of the course what e-mail practices you will follow. Remind your classes that you are expected to correspond with students only through their official University e-mail account, and they are responsible for information communicated to them this way. Official University e-mail accounts are more secure than other e-mail services and are consistent with the University's *Policy on Official Correspondence with Students*

If a student corresponds by e-mail from another ISP account (e.g. hotmail, Gmail etc.), consider whether to reply to that e-mail address or to advise the student to communicate with official University e-mail. Relevant factors for this decision include: whether the information is personal or sensitive and should be communicated through the official University e-mail; and, whether it is important information you may wish to rely on as having been formally conveyed to the student at utoronto.ca, as provided for in the Policy on Official Communication with Students.

☐ 3. The same advice for e-mail with students applies to e-mail correspondence with other faculty members and administrators.

Manage your e-mail folders with at least as much care as you would paper correspondence.

Write e-mails in a professional manner. Do not create an e-mail message that you would regret if it later appeared in a newspaper.

Forward e-mail with caution; do not over-distribute messages. E-mail messages can easily be copied and forwarded instantaneously to people for whom it was not intended.

E-mails can be requested, although not always disclosed, under FIPPA. Once a FIPPA request has been made, you cannot delete any e-mail messages responsive to the request.

Background

Your e-mail messages are University records and may be accessible under FIPPA. Work email records of employees are the property of the University.

Unencrypted email is not considered secure or an appropriate vehicle for the transmission of sensitive personal information.

Students' Records

Purpose and Objective

This practice provides guidance for accessing and retaining student records.

Checklist

☐ 1. Access to personal information such as student academic records must only be given on a need-to-know basis to University faculty or staff who need the information for their professional duties and as necessary and proper in the discharge of the University's functions. Instructors will usually not have the right to access student academic records form other programs or courses.

Faculty who serve on appeals panels or who have academic advising roles, may confidentially access student records as necessary for those purposes. Chairs/Directors and their specified administrative staff may access records for administrative purposes only and are generally not authorized to share these records with faculty.

If you have any doubt about your right to access academic records, consult the *Policy on Access to Student Academic Records*, or ask the Registrar or your FOI liaison BEFORE attempting such access.

☐ 2. Under the *Policy on Access to Student Academic Records*, students have a right to access their official student record and related academic information. If a student wishes to access records held by an academic department, it is advisable to contact or discuss the request with the Registrar or FOI Liaison.

Students should view their file in the department office under the supervision of office staff or the Chair. Copies of records may be provided, so long as they do not contain exempt information. If a student wishes to change the personal information contained in the file, they can do so through established official processes and offices, such as their Registrar.

☐ 3. Retain all records containing personal information for at least one year after the last use by the University, including student records.

☐ 4. Do not disclose personal information, such as grades and evaluative remarks, to anyone except the student to whom it pertains. If students have been notified of particular data practices, like peer/group evaluation, it is then appropriate to require them to share their information/work/evaluations for purposes of such peer/group evaluation.

☐ 5. Return all student work before the end of the academic term. Retain any final exams or other unclaimed work for at least one year after communicating the grade to students before destroying the work.

☐ 6. Do not collect and use personally identifiable images, e.g. photos or videos unless necessary to the course/instruction/activity or unless voluntary, informed consent from the individual is obtained before the image is collected. Where image collection is not necessary for official University purposes, it should not occur without explicit, no-prejudice opt in.

Background

Student work including papers and tests, grades, standing, and evaluative comments relating to work is personal information under FIPPA. Personal information includes images of students. The same principles apply to these as to other types of personal information.

The one-year FIPPA retention requirement for personal information is a minimum requirement. Longer retention requirements may be required for different record types. For example, retain all documents and correspondence that may be relevant to a petition or Academic Appeal process or a proceeding under the *Code of Behaviour on Academic Matters* until any proceedings are completed and until the date for a possible petition or academic appeal has passed.

Personal information is defined in FIPPA as **"**recorded information about an identifiable individual**".** Examples include: student name, home address, home phone number, student e-mail address (personal or university), identifying numbers (e.g. student number, employee number or SIN), education or health history, sexual orientation, race, national or ethnic origin, religion, marital or family status.

Your own professional contact information is not personal information (faculty member's business phone number, University e-mail, business mailing address). Information about your professional/work activities is not personal information.

The University is governed by its Grading Practices Policy and by the *Policy on Access to Student Academic Records.* You should become familiar with these, since they articulate practices expected of faculty members.

For privacy reasons, the photo used to produce the T-card is destroyed immediately.

Handling of Reference Letters

Purpose and Objective

This practice provides guidance on handling of reference letters respecting students or colleagues.

Checklist

☐ 1. Write letters of recommendation for students or colleagues, if you would have done so before the University was covered by FIPPA.

Background

Under FIPPA, the University is not obligated to reveal confidentially supplied evaluative or opinion material that was supplied solely to assess teaching materials or research, and/or to determine suitability, eligibility or qualifications for admission to academic programs or for an honour or award.

When an individual who is the subject of such a letter/evaluation requests access to it under FIPPA, the University has the discretion under FIPPA to refuse the request.

If you are writing a letter of reference for another organization or employer, where you are not confidentially supplying evaluative or opinion material for one of these purposes, it will not be possible under FIPPA to refuse disclosure of the letter to the individual to whom it pertains.