U of T Bound by Freedom of Information, Protection of Privacy Act

PHOTO COURTESY OF RAFAEL ESKENAZI

Rafael Eskenazi, director of U of T's FIPPA office, says the university's existing privacy practices are sound.

Stories by W. D. Lighthall

Although the University of Toronto — like all public universities in Ontario — became subject to the Freedom of Information and Protection of Privacy Act (FIPPA) June 10, 2006, it shouldn't cause a major upheaval in the way faculty and staff do business.

Legislation similar to FIPPA has been in effect for some time in British Columbia, Alberta and Quebec and universities within those jurisdictions have found it has not unduly affected their day-to-day operations.

"U of T has been protecting personal information in its operations for a long time and the university's existing privacy practices are quite sound," said Rafael Eskenazi, director of U of T's FIPPA office. "I would say the need at this point is for awareness about FIPPA among our university community. To a certain extent, what FIPPA does is formalize the privacy protection and accountability policies we already have in place."

To protect individual privacy, FIPPA requires that personal information held by universities, such as student records, must be protected. As well, the act gives the public the right to access university records through a freedom of information (FOI) request. This includes the right to request access to a university's administrative and operational records as well as requests by individuals wanting access to records containing their personal information.

Eskenazi said the freedom of information component of FIPPA is intended to support public accountability in government funded institutions. "It allows the public a window into how we conduct ourselves," he said.

Not all university records are subject to freedom of information requests. Exceptions include records related to labour and employment matters and, on the academic side, most research records and teaching materials.

Otherwise, "we should understand that absolutely any record that is in the custody or control of the university can be requested as part of an FOI request. And that should inform the level of professionalism applied to the process of creating and maintaining records," Eskenazi said. "Release is not automatic; we review records in detail and consult with the record holder to carefully consider the consequences of release. We apply FIPPA and other applicable law and policy to protect privacy, third-party rights and university operations from inappropriate disclosures."

FIPPA protects individual privacy while preserving Ontario universities' abilities to collect and use the personal information necessary to accomplish their work, such as the delivery of academic programs.

"If our activities around collecting personal information are necessary for doing our jobs, there's no issue with FIPPA," Eskenazi said. "The place where FIPPA steps in is if we are doing anything with personal information that is unnecessary to deliver our programs and has the potential to invade personal privacy."

To manage FIPPA questions or issues, each division within U of T has a freedom-of-information liaison officer and a deputy (FOILs) who serve as a point of contact for employees with questions related to the university's obligations under FIPPA. The university community can also contact the FIPPA office directly.

"IT ALLOWS THE PUBLIC A WINDOW INTO HOW WE CONDUCT OURSELVES."

Eskenazi said the common sense test is a good standard for most FIPPA questions or concerns. For example, given the legislation's emphasis on protecting personal privacy, when instructors are circulating class lists for attendance they should limit the amount of personal information required to what is absolutely necessary. Common sense is important since what is necessary will change depending on the context — what might be appropriate in a small seminar setting could be quite different from what can be done in a large classroom setting.

Access Student Records Carefully

Ontario's privacy legislation is specifically designed to give employees access to information they need to carry out their jobs. The university's long-standing policies generally strike a good balance between access to student records and giving employees access to the information they need to carry out their jobs.

Since early June last year, all public universities in Ontario have been subject to the Freedom of Information and Protection of Privacy Act (FIPPA). For its part, U of T's current Policy on Access to Student Academic Records has been in place since 1998. Together, they govern who has the right to access students' academic information.

"We take our responsibility to protect students' privacy rights very seriously and we always have," said Karel Swift, university registrar. "FIPPA is another set of legal standards. But in practice, it's not something entirely new to us because requirements within FIPPA are extremely close to our existing policies and practices on accessing students' academic records."

Under FIPPA, students have the right to access their official student records and related academic information. They can of course review a good portion of their academic records online (password protected) through U of T's Repository of Student Information (ROSI) system. For other information, they may contact their college or faculty registrar.

One type of information to which students can be denied access is letters of reference in the custody of the university, written on their behalf for admission, scholarships or other academically related purposes. Such letters are typically submitted in confidence by their authors.

Faculty and staff should access students' academic and other personal information records on a need-to-know basis — or as is necessary to carry out their duties to accomplish university functions. This means that instructors do not normally have the right to access a student's entire academic record.

"Certainly in terms of staff working with student records, it's pretty clear — records are private and they are confidential. They have access up to the point required to carry out their responsibilities and to support the university's core business," Swift said.

As for outside requests for access to student information, whether from media, parents or other sources, the short answer is no — the university is not permitted to release student information. Swift explained that the vast majority of information held by the university on its students is regarded as personal information and therefore must be protected from a privacy perspective.

"Without a student's explicit consent we do not release any information," Swift said. "That was our stance with our existing academic policy and that is required by FIPPA. With FIPPA, any individual enrolled in university who is 16 or over has the right to decide who may have access to their personal information."

The one piece of information about former students the university may continue to provide under both FIPPA and existing U of T policies is confirmation of the degree, or degrees, earned by a student.

"This will not change. This is public information and a core part of our business," Swift said. "Plus you can think of lots of situations where somebody needs to confirm that a graduate does have his or her degree."

FIPPA Tips

- Only collect personal information as necessary for program delivery.
- Only use personal information for the purposes for which it was collected.
- Only disclose personal information to faculty and staff on a need-to-know basis.
- Keep personal information for at least a year after the date of its last use.
- Do your best to respect the privacy rights of the individual.
- Keep personal information for staff, faculty and students in a secure location where it can be accessed only by those who need that information to do their jobs.
- E-mail should be used with caution, especially where personal information is involved, as it is not a secure medium.
- Be cautious about forwarding personal information through e-mail, especially when that personal information belongs to students.
- Remember that voice mail may be accessible by more than one person.
- Remember to password protect laptops, USB keys, BlackBerries, etc.

Protect Students' Classroom Privacy

PROFESSOR EDITH HILLAN, VICE-provost (academic), sees no need for faculty to be apprehensive about FIPPA requirements for classroom management practices.

Existing classroom practices and techniques at the University of Toronto achieve a high standard of safeguarding the privacy of students' personal information, Hillan said. "FIPPA is not about a sea change in the ways we interact with students. But faculty should now be cognizant of FIPPA and that some practices might need to be reviewed as a result, though most of our classroom practices are going to be fine."

While FIPPA allows universities to collect the personal information necessary to deliver their programs, the act also sets standards for handling personal information. Students' work, their grades, identification numbers, phone numbers and e-mail addresses are all personal information. Under FIPPA, university employees are responsible for protecting the individual's right to privacy when handling students' personal information.

Professor Kenneth Bartlett, director of the Office of Teaching Advancement, suggests that when taking attendance faculty should use a class list that doesn't show any unnecessary personal information. They might simply request students' names or initials and perhaps the last four digits of their student numbers.

Best practices when returning tests, papers and assignments should include a means for returning assignments personally (for example, in class), not leaving them unattended in a public place for general pickup. Furthermore, assignments should only be returned to the student who prepared the work; grades, comments and evaluations should be written on an inside page where they're not immediately visible to others.

"WE DO OWE IT TO STUDENTS TO PROTECT THEIR PRIVACY."

"In the past, sometimes classroom practices were done because it was convenient," Bartlett said. "With FIPPA, there will be patterns of practice that will have to be reviewed to ensure compliance with this legislation."

E-mails from and to students that contain personal information used by faculty to evaluate or advise students must be retained for a minimum of one year. "If a student e-mails a faculty member with any kind of personal information, they have to be careful that e-mail is not forwarded or shared unnecessarily with other people without consent of the student," said Pamela Gravestock, assistant director of the Office of Teaching Advancement.

Gravestock said regardless of the form a student's personal information takes, the underlying issue of protecting the individual's right to privacy is the same. "We have to be cautious about the types of personal information we distribute. We do owe it to students to protect their privacy."

The university has developed a FIPPA question and answer sheet for faculty, now available at www.provost.utoronto.ca/English/Guidelines.html. In addition, those wanting more information about meeting FIPPA requirements within the academic environment can contact their division's freedom of information liaison officer (ask your manager to identify him/her), the university's FIPPA office or the provost's office.

FIPPA Means Filing With Care

U OF T EMPLOYEES SHOULD GIVE A BIT OF THOUGHT to how they go about creating and maintaining their files and documents, now that all university records are subject to freedom of information requests.

Under the terms of the Freedom of Information and Protection of Privacy Act (FIPPA), the general public has the right to seek access to records — whether paper or electronic — in the custody of Ontario's public universities. This includes all records in the custody of the university, not just those created after June 2006.

"From the perspective of employees what this means is everything is a record and we must all manage records accordingly," said Heather Kelly, director of graduate student services for the School of Graduate Studies and her division's freedom of information liaison officer (FOIL). "Employees should create and manage all records knowing it's at least possible that any single record might fall within a freedom of information request and end up being released."

When Kelly said "everything is a record" under FIPPA, take that literally. The legislation specifies that the term "record" encompasses e-mail, voice mail, documents, letters, memos, draft versions of a document, drawings and graphics as well as any other workplace materials that record information, whether in hard copy or electronic form.

"We don't tend to think that our voice mail is a record or the notes we take in a meeting but those are official records. Everything we create on university time is a record subject to FIPPA," Kelly said.

None of this means university employees should panic, it simply means they should exercise prudence when it comes to creating and managing their files and records, said Rafael Eskenazi, director of the university's Freedom of Information and Protection of Privacy office.

Eskenazi advises that when creating or adding to files and workplace records, employees should focus on addressing the operational requirements of the job at hand. Usually this means excluding personal observations or opinions that don't directly advance the task. Employees should ask themselves how the record they are creating now would look on the front page of a newspaper — how it would reflect on them and on the university.

"There's a need in all institutions for professional record keeping and that's the context we are talking about with FIPPA. You want to create the records needed to do your work, to keep them focused and professional and to limit records to their operational purposes," Eskenazi said.

Rodney Branch, director of information systems with the School of Graduate Studies, recommends that employees familiarize themselves with the file management and retention policies in their division, department or area. These plans specify the types of files that should be created and maintained, the length of retention, their general organization, content and permanent location.

For more information, employees can visit www.library.utoronto.ca/utarms/, which has an entire section devoted to record management policies and practices at U of T.

Each division has a freedom of information liaison officer like Heather Kelly of the School of Graduate Studies.

Classroom Procedures for Instructors Under FIPPA

Q. What practices should I follow for handling assignments submitted physically?

- Write grades and comments inside test books, papers and other materials where they cannot be easily seen by others.
- Where possible, fold, staple or tape test books, papers and other materials closed to ensure that grades and comments are not visible to other students when materials are returned.

Q. How should I collect students' work?

- Students' work should be collected with adequate supervision and security so that students cannot see the content of each other's assignments.
- Ideally, collect assignments in class under supervised conditions.
- If this cannot be done, arrange for drop off in your departmental office, TA office or some place where assignments can be collected and held securely for your retrieval.

Q. How should I return students' work?

- Assignments should be returned in class if at all possible and not be left in a public place for general pickup. Assignments should only be returned to the student who prepared the work and not to other individuals, unless written permission has been given.
- Under FIPPA you should retain all unclaimed student work, including final exams, for one full year and then arrange for it to be properly destroyed. Divisions should have or develop policies on the confidential disposal of unclaimed work.

Q. What practices should I follow for posting grades?

- When posting grades, remember that student identifiers, including names and student numbers, are personal information, as are student marks. Posting is a courtesy; the official mark for the course is provided through ROSI.
- Where possible, use secure electronic media (such as Blackboard) so individuals see only their own grades.
- If no alternative exists, post results in hard copy using truncated student numbers (e.g., last four digits only) to reduce the ability of students to identify one another's grades.

Q. How should I take attendance in class?

- Collect only the information that you need to verify a student's presence. The presence or absence of a student is the personal information of that student.
- In all cases, students should be informed at the start of the course how their personal information, including attendance, will be collected and used.
- Student personal information should not be released to anyone except in the performance of their academic administrative responsibilities. Do not release personal information to anyone else. If you receive an inquiry from someone other than the student, all such inquiries should be referred to the student's registrar.

Q. How can I now take students' attendance at final exams?

- Where written proof of attendance is necessary, students should provide it in such a way that their personal information (including their presence or absence) is not made known to another student.
- A good practice is to use individual attendance cards that are given to each student and that ask for the date, their full name, full student number, course number and session, instructor's name and their signature.
- Students should sign their individual attendance cards in the presence of the invigilator as the cards are collected. Signed cards for each examination should be kept in a secure place for at least one year after the date of the exam and then destroyed, along with the exams.

Q. How should I have students sign up for group work?

- Employ practices that do not require students to unnecessarily reveal personal information to other students. Ideally students should have access to a secure, confidential electronic portal function for group sign-up.
- Where group work practices are established or necessary parts of the curriculum, students should be informed at the start of the term that their personal information will be collected and used to develop group work schedules. Collect only the information that is necessary to facilitate group work.

Visit www.fippa.utoronto.ca for more detailed information.

PASCAL INDUSTRI