Fact Sheet

Access and Privacy: A Primer for Faculty Members

Records Management and Privacy Office
Kingston, ON K7L 3N6
Tel. (613) 533-6095
access.privacy@queensu.ca

Queen's University is subject to Ontario's *Freedom of Information and Protection of Privacy Act* which provides a right of access to the University's records and information, and mandates us to protect the privacy of the individuals whose personal information we collect and keep. The Act pertains to all employees, including faculty members.

This fact sheet is not comprehensive; it is intended to give faculty members a few key take-aways to help them in their daily work. For more information about access and privacy, see the Records Management and Privacy Office website: http://www.queensu.ca/accessandprivacy/.

Access to Information: Your records may be requested under FIPPA.

It's important to know which records are in and out of scope of a FIPPA request. What is NOT in scope are **teaching materials** (such as your PowerPoint slides, notes you use for your teaching, and the like) and **records respecting research** (with the exception that the University must disclose the subject matter and amount of funding for research). Your personal communications are also NOT in scope.

What IS in scope is everything else that pertains to your work supporting the business of the University—including records pertaining to your **teaching activities**. Emails between you and a student are in scope and may be requested by the student as they are the student's personal information; this includes emails sent or received using a personal email account. It is always best to use your Queen's email account for Queen's University business. You should also know that FIPPA requires us to keep records containing personal information (such as emails with students) for a minimum of 1 year.

Access to Information

Under FIPPA, anyone can request access to records in the custody or under the control of the University, including emails. The exceptions to disclosure are limited and specific, and can't be applied until after records have been reviewed by the University's Privacy Office staff.

- ✓ Keeping your personal and work-related email separate will ensure that personal emails don't get drawn into a records search.

- ➢ **Take-away: Create records with access in mind.**

Protection of Privacy: Yes, students do care about privacy.

Students care about their privacy, even if they blog or Tweet about their most personal issues. They can, and do, make privacy complaints. Privacy is about having control over your own personal information and how, where, and when you choose to share it. So in general, we should not be sharing a student's personal information without their consent.

However, FIPPA is not meant to prevent us from doing the work we've been hired to do, and so the Act does allow us to share someone's personal information on a "need-to-know" basis where that disclosure is necessary and proper.

The Records Management and Privacy Office website has a number of FAQs (http://www.queensu.ca/accessandprivacy/faqs) providing guidance on how to respect student privacy in the context of your teaching.

- **Take-away: Be mindful of student privacy rights.**

Mobile Devices: They are easily lost or stolen.

No one wants to be responsible for a privacy breach, but breaches occur more often than you may realize. Frequently they involve the loss or theft of the myriad devices that have become an essential part of our daily lives: the laptop accidentally left on an airplane; the cellphone stolen out of a gym locker; the external hard drive you use to back up files that inexplicably goes missing. In all of these cases, if the device has been encrypted, there is a greatly reduced risk of a privacy breach as no one will have direct access to any personal information on it. Even if you do all of your work in the cloud, you should still encrypt your devices because chances are some information is being downloaded and stored locally on those devices.

Privacy Breach

A privacy breach occurs whenever someone's personal information is collected, used or disclosed in an unauthorized manner, either on purpose or by accident.

ITS has easy-to-follow tutorials (see http://queensu.ca/its/security) instructing people how to encrypt any number of devices, from phones and tablets to laptops, desktops and even USB drives. The tutorials also show you how to wipe your device remotely.

- **Take-away: Encrypt all devices.**

Cloud Computing: Not all web tools are created equal.

Increasingly we are using third-party cloud-computing (web-based) tools and services in support of teaching. We need to be sure that those third parties are reputable and competent, and that we have taken steps to limit exposure and mishandling of our students' personal information—not only to protect the privacy of our students, but also to protect the security of our own computer systems. If you are thinking of incorporating the cloud into your teaching, ask the following questions: What personal information does the third party collect? How do they use it? With whom do they share it? How long do they retain it? How do they protect it? When Queen's adopted the Microsoft Office 365 cloud solution across campus, a rigorous privacy and security assessment was undertaken, asking these kinds of questions and many more.

Cast a critical eye over web-based tools and services, read the accompanying Privacy Policy and Terms of Use, and seek advice before using them. The Information Security Office can provide assistance with reviewing cloud tools and services: https://www.queensu.ca/its/security-assessment-process

Take-away: Investigate web-based tools before using them.