# Fact Sheet

## Students Employed by Queen's: How to Manage Email and Other Records

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

## Email

As a Queen's University student who is also a Queen's employee, you have been given a separate NetID from your student NetID to be used for your employment. ***It is very important to keep your employee identity separate and distinct from your student identity.***

Whether you are a Teaching Assistant or any other kind of student employed by Queen's, you may have access to confidential or sensitive information. Confidential information could include legal or financial documents, research data, patent applications, or draft policy documents.

Confidential information could also include ***personal information*** of students or others. If you are a TA, for example, you could have access to student numbers, grades, completed tests and term papers.

Queen's University, like all universities in Ontario, is subject to the *Freedom of Information and Protection of Privacy Act* ("*FIPPA*") which governs the way personal information is collected, used, disclosed, retained and destroyed. Under FIPPA, it is a violation of privacy to disclose a student's personal information to another student; however, it is not a violation of privacy to disclose a student's personal information to an employee who has a legitimate need to know for purposes of their employment. It is imperative, therefore, that the capacity in which a person is sending and receiving personal information is clear. This can only be achieved if your student and employment identities are kept distinct and separate.

You should not, therefore, forward your employee email to your student account, or any other personal email account. This creates risk both for the University *and you as a student employee* in terms of privacy breaches and complaints.

In addition to privacy concerns, you should know that the records you create and receive as an employee, including emails, are university records. They belong to Queen's University and are subject to any rules and procedures pertaining to university records including the Records Management Policy (https://www.queensu.ca/secretariat/policies/administration-and-operations/records-management-policy) and provincial access and

Personal information is anything that can be used to identify someone, including their:

- race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital status
- educational, medical, psychiatric, psychological, criminal or employment history
- name, address, telephone number, fingerprints, or blood type
- identifying number (SIN, student ID, employment ID), symbol, or other particular assigned to them

Personal information is NOT:

- a name, title, or contact information that identifies someone in their business, professional, or official capacity, *even if they conduct their business from home*

privacy legislation (http://www.queensu.ca/accessandprivacy/). It is possible that a request for access to those records (including emails) could be made in which case you will be asked to search for and produce records responsive to the request. Keeping your work-related emails separate from your own personal emails eliminates any risk that your personal emails will get drawn into a search for records.

When you cease to be a Queen's employee, you should not retain any of the work email you have sent or received. ITServices can easily disable your access to the Queen's employee account without interfering with your student email account.

*Do…*

- ✓ Use your **employee** NetID and employee email account for your Queen's employment

*Do not…*

- X Use your **student** NetID and student email account for your Queen's employment
- X **Forward** your employee email account to your student email account

*Think about it…*

As a student yourself, would you want *your* student information—such as your student number and grades—to end up in your TA's personal email account forever?

# Beyond email

The directive to maintain a separate employment persona carries over to all other work-related records, not just to email. Accordingly, you should ensure that any work-related files (such as Word documents, Excel spreadsheets, etc.) are maintained in designated folders on a Queen's University shared drive, or if maintained in a personal folder (such as on OneDrive for Business or on a personal computer), that they are not retained after employment terminates.

If you require access to information that could contain confidential or personal information of others, there are several options for protecting the files. ***In all cases, be sure to access files with your employee NetID.***

- **Use Office 365 to edit documents online and save files directly to OneDrive for Business.** This will ensure the files do not reside on your personal device. Do not sync files to a personal device without encrypting the files or the device (see below).
- Use **Windows File Service** to save work files on a Queen's-hosted drive, or, for even more security, use **Windows Terminal Services**. Both services can be accessed remotely using **VPN** (Queen's ITS - Virtual Private Network). These services must be requested by the department you are employed with. See Queen's ITS – Windows File Service.
- **Encrypt documents** if there is any chance they will reside on your personal device or on a USB drive. See Queen's ITS Encryption Tutorials
- **Encrypt personal devices.** If you do not encrypt the documents themselves, then you must encrypt your devices, including USB drives. See End User - Encryption Service