Fact Sheet

Using and Managing Email

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

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. This document is designed to help you ensure that, as a Queen's employee, your email practices comply with FIPPA, as well as with the University's records management requirements.

Email is a Record

Whenever an email message is sent in the course of University business, that email becomes an official record of the University. Such records can be subject to disclosure in response to an Access to Information Request under FIPPA or subject to subpoena by the courts. So it's important that you take care when sending emails for a business purpose.

Access to Information

Under FIPPA, anyone can request access to records of the University, including emails. The exceptions to disclosure are limited and can't be applied until after records have been reviewed by University staff.

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

Use Your Queen's Email Account

In today's world, we all have multiple email accounts. Some are personal (such as a Gmail or Hotmail account), and some will be institutional (such as your Queen's employee account). Always use your Queen's University **employee email account** for University business.

If you use a non-Queen's employee account to create, respond to, or store work-related information you are increasing the risk of causing an inadvertent privacy breach by using a non-authorized service provider. In addition, those emails are still subject to FIPPA so you run the risk that your own personal emails will be drawn into an access to information request. For these reasons, it is imperative that you keep your personal and work-related correspondence separate.

Do

✓ Use your Queen's employee email account for work-related correspondence

✓ Use your personal email account for personal correspondence

Do Not

X Forward your Queen's business-related emails to a personal email account (such as Gmail or Hotmail)

X Use the alias function in a personal email account to compose messages so that they look like they are coming from your Queen's address but are really created, sent, and stored using your personal account

Students employed by Queen's, see
Students Employed by Queen's: How to Manage Email and Other Records

Create Email Records with Access in Mind

Because the public (including the media) has the right to access the emails that you create in the course of your job, it is important that all work-related emails be composed in a professional tone, and with the basic assumption that they might be made public under an Access to Information request.

Consider whether a record is necessary

Use email when you need a record of the communication. Use the phone for preliminary discussions, or when a record is not strictly necessary.

> *Take time to learn how to use the email system properly*
>
> ITServices tutorials: http://www.queensu.ca/its/
>
> The Human Resources Office offers a Learning Catalogue of workshops and programs free to Queen's employees.

When you need a record:

- ✓ To officially confirm something previously discussed
- ✓ To demonstrate due diligence

When you do not need a record:

- ✓ Preliminary discussions before an official decision is made
- ✓ Discussions involving opinions about others, *unless an official record of those opinions is necessary*

Create professional records

Don't put anything in an email that you would be embarrassed to see on the front page of the newspaper.

Always

- ✓ Use a professional and neutral tone
- ✓ Clearly distinguish between opinion and fact
- ✓ Include only as much information as needs to be officially recorded
- ✓ Include a clear subject line and limit messages to one topic
- ✓ Copy only those who need to know

Avoid

- X Editorializing by including unnecessary personal remarks
- X Including personal information directly in the body of your email
- X Mixing personal and University business in a single email
- X Using the "Reply All" function

Protect personal and confidential information

There may be times when you may need to transmit sensitive and confidential information, including personal information. With email, there is always a risk that messages will be accidentally forwarded to an unauthorized individual or opened and saved on a mobile device that is later lost, or stolen. Personal information that is lost, stolen, or disclosed to an unauthorized individual constitutes a privacy breach under FIPPA.

> ### Privacy Breach
>
> A privacy breach occurs whenever someone's personal information is disclosed to an unauthorized individual, either on purpose or by accident.

Ontario's Information and Privacy Commissioner has taken the position that if personal information is encrypted, then it is not a privacy breach if it is lost or stolen.

For this reason, when you need to transmit personal information, ask yourself first whether there is another, more secure way to deliver the information than by email, such as **by hand**, or by using a **document sharing service**, such as QShare, or OneDrive for Business, that requires users to authenticate their identity to obtain access to the document(s).

If you must use email to communicate personal or confidential information,

- ✓ remove as much personal information as possible
- ✓ put the information in an attachment and encrypt the attachment before sending
- ✓ include a confidentiality statement at the bottom of your email
- ✓ verify the email addresses of all recipients

Encrypting Email Attachments

You can encrypt email attachments by assigning them a password.

- ✓ Give the recipient the password over the telephone or in a separate communication.
- X Do not provide the password in the same message as the attachment.
- ✓ Visit ITServices' online tutorials for instructions on how to encrypt Word, Excel, and PDF documents.

Keep and File Email Records Appropriately

Retain messages that are sent and received only if they relate to University business; all other messages can be treated as transitory and deleted (see Fact Sheet on Transitory Records).

- ✓ When retaining a series of replies or forwards, keep only the last message as long as the thread is complete and hasn't been changed in the course of the exchange.
- ✓ Make sure to retain information in the header regarding the sender, recipients, date and time; this helps preserve the context of the message.
- ✓ The email system is not a recordkeeping system. A recordkeeping system organizes records according to a file plan, provides shared access to those who need it, and applies retention and disposition rules. Here are some options for filing email messages:
  - If you have an electronic recordkeeping system, file email (and attachments) in that system.
  - If you have a paper-based recordkeeping system, periodically print and file the email (and attachments) and then delete them from the email system.
  - As a temporary measure before filing in a proper recordkeeping system, create folders within the email system that reflect your department's file plan. Move email to these folders every day.

Remember…

If a file becomes the subject of an Access to Information request or a legal discovery order, all emails associated with that file *must* be retained until the request is completed.