Fact Sheet

Data Security and Encryption: Handling Confidential & Personal Information

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

This fact sheet is a reminder to all Queen's employees of the stewardship responsibilities we all bear when handling the personal information of Queen's students, employees, alumni, and other people who interact with the University, as well as when handling restricted and confidential information pertaining to the University and our outside partners.

Ensuring the security of data both on and off campus when using email, removable media, and mobile devices (including when transferring data to ourselves in order to work at home or while travelling) is a vital **proactive** component of the University's privacy and data-security strategy and is an integral part of the Queen's Electronic Information Security Policy Framework.

The damaging consequences of a lost or stolen USB key, external hard drive, laptop, tablet, cell phone, or other similar electronic device that may contain personal or sensitive data can be reduced dramatically by ensuring that these devices are encrypted.

Encrypt all devices

Each and every mobile device used to access, store or transfer restricted, confidential or personal information (such as USB keys, laptops, tablets, cell phones and external hard drives) **must be encrypted**.

A login password is **not** encryption and is **not** sufficient. Turning encryption on for your mobile devices is, however, **free** and easy:

- contact your department's or unit's internal IT staff for assistance with encrypting your devices; or
- call the IT Support Centre at (613) 533-6666 to have them encrypt your devices for you; or
- use IT Services' knowledge database to learn about encrypting a device.

Ensure that **each** mobile device in your faculty, department, and associated units—**including personal devices** used for Queen's purposes—is encrypted.

It is the position of Ontario's Information and Privacy Commissioner that the loss of a mobile device containing personal information, **if encrypted**, is not a privacy breach. Encrypting devices is not only a sensible privacy and security precaution, but also more operationally efficient.

Safeguarding Personal Health Information

Ontario's Information and Privacy Commissioner has **mandated encryption** for all personal health information stored on a mobile device. See the IPC's Fact Sheets:

#12: Encrypting Personal Health Information on Mobile Devices

#16: Health-Care Requirement for Strong Encryption

Help protect the information entrusted to us and the University's reputation: ***ensure encryption of ALL mobile devices used within your faculty, department, and associated units***.

Classify the data

Ensure that the data created and received by your department or unit is classified according to the University's Data Classification Standard so you can easily determine the level of security required.

Use email with caution

Email is not a secure method of transferring information. Although email sent between our ***@queensu.ca*** email addresses is encrypted, an email message can be inadvertently misaddressed and sent to the wrong individual. If you must use email to transfer personal, restricted or confidential information, put the information in an attachment and encrypt the attachment.

When emailing personal, restricted or confidential information externally to a non-***@queensu.ca*** email address, the information **must** be encrypted as we have no ability to know whether the recipient's email service is encrypted in transit, or whether the recipient is opening the email on an encrypted device.

✓ Best Practice

If emailing student personal information directly in the body of an email message, include the **student number and student's initials** rather than the full student name.

With an individual's prior consent, you may email the individual's own personal information, but be sure to inform the individual of the potential privacy risks.

For more information about email, see the Fact Sheet on Using and Managing Email.

Train regularly

Distribute this fact sheet widely to all staff and faculty with responsibility for handling restricted, confidential and personal information.

Incorporate this information into your regular training for all faculty and staff, including volunteers and students employed by Queen's.

Repeat your training at least twice a year and conduct annual audits to ensure that your faculty or department, and associated units, are taking the appropriate proactive steps to prevent a data breach.

Remember…

Most data breaches are unintentional and caused by human error. If you have questions, contact the Records Management and Privacy Office at access.privacy@queensu.ca.