Fact Sheet

Data Security and Encryption: Handling Confidential & Personal Information

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 we security strategy and is an integral part of
nation 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