Many of you will have seen reports from sister institutions of sensitive information being disclosed, leading to reputational embarrassment and damage, and substantial remedial work in notifying those whose personal information was disclosed.

A significant area of vulnerability involves mobile devices (laptops, tablets, smartphones), many of which contain information classified by Policy 8 as restricted, such as student marks, your personal information, and so on. In order to protect this information in the event that your mobile device is lost or stolen, its internal storage, as well as any peripheral storage devices used, must be encrypted.

Information about how to encrypt your device(s), including laptops, iPads, Playbooks, and Blackberrys, can be found at http://ist.uwaterloo.ca/security/encryption. Your local help desk or computing support provider may also be able to assist you with encryption. Finally, you may drop off your mobile device(s) at the IST CHIP (x84357, helpdesk@uwaterloo.ca) and they will encrypt your device(s) for you. It would be helpful to call ahead to arrange a time.

More generally, while much of the current focus is on security of digital information, it is equally important to ensure that sensitive information that is in paper or other non-electronic form is also kept secure, and that only those who are authorized to access such information are able to do so.