McMaster University

Policies, Procedures and Guidelines

Complete Policy Title:
Mobile Devices Policy

Policy Number (if applicable):

Approved by:
President

Date of Most Recent Approval:
July 1, 2017

Date of Original Approval(s):
June 16, 2015

Supersedes/Amends Policy dated:
Portable Storage Policy June 16, 2015

Responsible Executive:
University Privacy Officer

Enquiries:
University Secretariat

DISCLAIMER: *If there is a Discrepancy between this electronic policy and the written copy held by the policy owner, the written copy prevails.*

PURPOSE

The purpose of this Policy is to ensure that personal information, personal health information and other confidential and/or sensitive information in the University's custody or control is properly safeguarded from those not entitled to have access, as well as protecting University systems from the introduction of malicious software. Information contained on Mobile Devices is subject to the same policies and laws as other University information. However, because of their size and portability, these devices are easily lost or stolen and therefore present increased privacy and security risks when sensitive or personal information is stored on the device.

Mobile Devices include, but are not limited to:

- smartphones (Android, Blackberry, iPhone, etc.)
- laptops, netbooks, tablets, Ultra-mobile PCs (UMPCs), mobile internet devices
- PDA (personal digital assistant), e-readers
- Portable Storage Devices (PSDs)
  - flash storage (memory sticks, SD cards, etc.)
  - USB sticks or thumb drives.
  - external hard drives
  - audio players (iPod touch, mp3 player, etc.)

SECURITY OF PERSONAL INFORMATION (PI) AND PERSONAL HEALTH INFORMATION (PHI)

Personal information and personal health information are both classified as "Confidential" under the UTS *Information Classification Matrix Policy Statement*.

All University employees must ensure that PI/PHI in the University's custody or control is protected against theft, loss and unauthorised use or disclosure and ensure that the records containing the information are protected against unauthorised copying, modification or disposal.

MINIMUM GUIDELINES WHEN USING A MOBILE DEVICE

PI/PHI should not be stored on Mobile Devices. However, in the event that there is no alternative to local storage, all such information must be encrypted using approved encryption techniques and/or password protected.

PI/PHI must not be transmitted via wireless communication to or from a Mobile Device unless approved wireless transmission protocols along with approved encryption techniques are utilised.
All remote access to McMaster University information resources must use an approved communication mechanism.

All Mobile Devices must have approved virus and malware detection/protection software along with personal firewall protection (where applicable).

USER RESPONSIBILITIES AND PROCEDURES

Password-protect your Mobile Device

Physical security is a major concern for Mobile Devices, which tend to be small and easily lost or misplaced. If your Mobile Device is lost or stolen, a device password may be all that stands in the way of someone reading your E-mail or PI/PHI of another individual(s).

Choose a strong password. Strong login passwords are comprised of at least eight characters with 14 or more being ideal. These should include a combination of upper and lower case letters, numbers and symbols. **DO NOT** use passwords that are predictable, i.e. Birthday.

Verify Encryption Mechanisms

Any PI/PHI must be encrypted**.** On its own, password protection is not sufficient should the Mobile Device become lost or stolen.

Protect your passwords and encryption key by

Not writing them down or storing them on the device
Not using the same password to log into your computer and to unlock encrypted files.

Enable Auto Lock Feature

Enable the automatic lock feature of your device after five minutes or less of idle time.

Physical Security

Do not leave your Mobile Device unattended, or in your vehicle (*including* the trunk). Mobile Devices are easily lost or stolen. Be sure to keep your Mobile Device in your possession when in public and safely stored when at home.

Use Antivirus Software

If you have PI/PHI on your Mobile Device then at a minimum you should have personal firewall, anti-virus and anti-spyware programs that are up-to-date with the latest security patches.

Enable Lost Device Protection

Enable lost device protection on your Mobile Device which will allow you to locate, lock and/or wipe a lost device (e.g. iPhone/iPad/iPod have “Find My iPhone”, or enable in the Antivirus software).

Keep Software Up-To-Date

Ensure that software, especially security/antivirus software, is up-to-date. Turn on automatic updates where possible.

Public Wi-Fi, Hotspots, and Bluetooth Security

Public Wi-Fi and Hotspots are **not** secure. Public networks allow anyone to connect as they do not require a password, which exposes you to security risks from other people using the same public network.

Enable security features on Bluetooth devices, as appropriate (set to only exchange data with “trusted devices”; set the mode to “non-discoverable”; disable when not in use).

Storage

Portable Storage Devices (PSDs) should be used for the temporary storage of information only and must not be used as permanent document repositories to store University information. Confidential data or personal information contained on Portable Storage Devices may only be a copy of data stored on a secure University system.

Delete When Done

When you are done with PI/PHI or confidential information and no longer require access to it on the Mobile Device, delete it.

Data Erasure and Disposal of PSDs

Confidential and personal data held on PSDs must be erased sufficiently to prevent information recovery using tools normally available on the university system. Simple deletion or erasure of the files or reformatting does not clear the Portable Storage Device, because commands such as undelete or un-format may permit the recovery of the information. Contact University Technology Services for additional information

Promptly Report a Lost or Stolen Device:

If your Mobile Device has been lost or stolen promptly report this to the McMaster University Security Services. Additionally, advise the **Privacy Office** if the device has any PI/PHI on it. Keep a record of the Mobile Device’s make, model, serial number,

Storage Case

Ensure that the case does not bear any visible identification of the University. Include an “if found, return by calling [phone number]” card inside the case with no other identifying information.