

TOPIC:	Protecting Board-owned Mobile Devices
EFFECTIVE:	June 15, 2010
CROSS-REFERENCE:	Privacy and Information Management – Policy
REVISION DATE:	September 2011
RESPONSIBILITY:	Chief Information Officer

INTENT STATEMENT

Mobile technologies are regularly used by Halton District School Board employees. These devices enhance the quality of work and life for employees but dramatically increase the risk for data loss and personal information disclosure.

The following procedures are intended to reduce this risk. For the purposes of this procedures

- *“Mobile Devices” – includes, but is not limited to, all portable electronic devices that contain or access data including cell phones, personal digital assistants (PDAs), portable computers, memory storage, USB sticks/drives,*

Procedure

The following procedures should be used to protect information on mobile devices:

1. To the greatest extent possible, avoid storing Personal Information on mobile devices.
2. This procedure focuses on Board provided devices that are assigned to an individual. This does not include devices that are shared by groups of individuals since personal data is not stored within them.
3. Mobile devices ***MUST*** be password protected and/or securely encrypted. The password must be entered manually and this step should not be automated.
4. The data should be backed up to ensure it is not the sole instance.
5. When retiring or disposing of mobile devices, care must be given to erase or destroy the personal information so that there is no possibility of subsequent data recovery.
6. Reasonable care should be taken to protect the device.
 - a. Devices should not be left in insecure areas unattended.
 - b. Do not leave devices in your vehicle. If necessary, lock in your trunk or if there is not trunk, well out of sight.
 - c. Enable the automatic locking after defined idle times.
 - d. Write on the device a return phone number, so a lost device may be returned when found
7. Keep the screen from the view of others. (privacy screens)
8. Specific mobile device settings
 - a. Personally assigned portable computers
 - i. Password protected
 - ii. Encryption of hard drive for all machines assigned to administrators and central staff
 - iii. Users should not store personal data on unencrypted section of the Hard drive.
 - iv. 20 minute idle lockout (password required to unlock)
 - b. Personally assigned PDA, cell phone
 - i. Password protection
 - ii. 20 minute idle timeout
 - c. Memory Storage, USB stick/drive

[NOTE: USB models change regularly and hence specific models can not be named]

 - i. Encrypted. (When purchasing the device, ask if the device provides encryption)