TOPIC:	**Protecting Board-owned Mobile Devices**
EFFECTIVE:	**January 2013**
CROSS-REFERENCE:	**Privacy and Information Management – Policy**
REVISION DATE:	**September 2017**
RESPONSIBILITY:	**Chief Information Officer**

INTENT STATEMENT

Mobile technologies are regularly used by Halton District School Board employees. These devices are essential to enhance staff effectiveness 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 procedure "Mobile Devices" – includes, but is not limited to, all portable electronic devices that contain or access data including cell phones, smart phones, portable computers, tablets, 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 each time. Enable the automatic locking after defined idle time.
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. When the device is returned to Information Services, the data will be removed.
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. 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. (a suggested practice - privacy screen)
8. Specific mobile device settings
    a. Personally assigned portable computers or tablet
        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 smart phone, 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 cannot be named]
        i. Encrypted. (When purchasing the device, ask if the device provides encryption)

Appendix A

Suggested Practices

1. Lock your Windows laptop when not in use – Press Windows L, or CTL/ALT/DEL

2. **When transporting personal/confidential information, you should either**
    a. store within the file stores provided (G:, O: etc) and use myHDSB to access information
    OR
    b. encrypt the files OR
    c. encrypt the hard drive or encrypt the memory key OR
    d. store within CHATT (watch for the folder permissions) OR
    e. use of the Halton Cloud (see attached). This information is safeguarded under the agreement we have
        i. Data does not need to be transported. USB keys are not required
        ii. Accessible from anywhere/any time
        iii. Data is password protected
        iv. Data is protected from hardware failure

3. **Do not use services** such as Drop Box, iCloud (unless those important files are encrypted) since those vendor agreements may not provide the confidentiality required.

4. Also NOTE:
    a. Older versions of Word and Excel (before Office 2007) do not provide satisfactory encryption when those documents are password protected, however newer versions (Office 2007 and newer) provide good encryption.
    b. zipping a file does not encrypt it unless it is password protected as well.