Topic:	**Protecting Board-owned Mobile Devices**
Effective:	**January 2013**
Cross-Reference:	**HDSB Privacy and Information Management Policy**
Revision Date:	**May 2019**
Review Date:	**May 2022**
Responsibility:	**Superintendent of Education – Information Services**

INTENDED PURPOSE:
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.

PROCEDURES:
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. Schools and administrative buildings shall use the eWaste vendor to dispose of all hardware.
5. 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 a trunk, well out of sight.