PORTABLE TECHNOLOGY SECURITY

Background

All staff using Division information are responsible for the management and safekeeping of information under their control by ensuring that there is adequate security to prevent unauthorized access, collection, use, disclosure, or disposal of information.

Sensitive and confidential information stored on portable technology such as laptops, personal organizers, cell phones or memory sticks must be kept to an enhanced standard due to the higher risk of equipment theft.

Procedures

1. All password protection mechanisms available on portable technology must be activated and utilized consistently and to the greatest extent possible. Industry standards/methods are to be deployed in the selection of appropriate passwords.
2. All files containing sensitive or confidential information that are stored on portable technology must be encrypted.
3. Information that is no longer required on portable technology is to be transferred to secure digital storage.
4. Security measures adopted for other technology within the Division also apply to portable technology.

Reference: Section 33, 52, 53, 68, 196, 197, 204, 222, 225 Education Act