Administrative Procedure 125 PORTABLE TECHNOLOGY SECURITY

All staff using Division information at a Division location or otherwise 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, memory sticks must be kept to an even higher 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 the appropriate passwords.

2. All files containing sensitive or confidential information that are stored on portable technology must be encrypted.

3. Any information that is no longer required on portable technology is to be transferred immediately to more secure electronic storage.

4. All security measures adopted for other technology use within the Division apply to portable technology.

5. Staff are directed not to put pertinent Division information on their personal portable technology.

6. The hard drives from photocopiers and printers are to be removed and destroyed prior to the photocopier being removed from the school/central office sites.

Created: March 2018 April 2020

Reference: Section 196, 197, 53, 52, 204, 222, 68, 225 Education Act
Freedom of Information and Protection of Privacy Act
Canadian Charter of Rights and Freedoms
Canada Criminal Code
Copyright Act
ATA Code of Professional Conduct