PORTABLE TECHNOLOGY SECURITY

Background

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, or 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 appropriate passwords.

2. Established passwords must be given in strict confidence to the Director or designate, and may not be shared with any other individual.

3. All files containing sensitive and confidential information that are stored on portable technology must be encrypted and are not to be stored on personal non-Division owned devices.

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

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

Reference: Sections 85, 87, 108 Education Act
The School Division Administration Regulations 45, 49
Saskatchewan Ministry of Education – Information Security and Acceptable Use Policy

Approved: December 12, 2018