SECURITY OF LAPTOPS, MEMORY KEYS AND PORTABLE DEVICES

WORKING AT HOME

1. If working at home, employees may use remote access from their personal computer to access information at the office.

2. (a)   Employees are encouraged to use their own computers with the remote access from home.

   (b)   IT support services will be available to consult with employees at home to ensure remote access.

3. Individual laptops are not to be taken from the office unless signed out in accordance with procedures set out in this policy.

LAPTOPS

1. Laptops will be available to sign out if needed by employees to work at home or on the road.

2. Laptops when signed out must be used in accordance with the following:

   (a)   No data shall be stored on the laptop (C drive).

   (b)   Folders shall be password protected.

   (c)   Cache shall be cleaned off the computer after use.

   (d)   There shall be no software installed on the laptop unless the employee has received prior approval from IT support services.

   (e)   No person other than the employee shall use the laptop.

3. When the laptop is returned to the office it will be checked by IT support services and all information will be deleted. It is the responsibility of the employee to ensure that any required copies of information are made.

4. If an employee wishes to take a laptop out of Province or the country IT support services must be advised and will provide directions concerning storage and care of the laptop.

Priorities

1. Laptop computers will be loaned to employees based on the following needs, ranked in order of importance.

   a. Classroom instruction

b. Web-based course development

c. Professional development (conference use, software instruction, etc.)

2. All requests are based on the availability of equipment and should there be more requests than available laptops, needs will be addressed on a first-come, first-served basis within the stated priorities.

Period of Loan/Renewal

1. a. Use of the computer for a month or less will be considered a short-term loan.

    b. Requests for short-term use must be submitted to IT stipulating software needs.

    c. Requests will be approved solely at the discretion of IT.

2. a. Laptop use for longer periods, including a semester and a full academic year, will be considered a long-term loan.

    b. Long term loan requests must:

          i. indicate the purpose for which the laptop will be used:

          ii. be submitted by _____ **1st**;to permit the machine to be customized before pick-up on _____ 1st.

    c. All software and hardware specifications must be noted on the laptop sign out from.

Equipment Supplied

1. Laptops will come equipped with the following:

    a. Power cord

    b. Mouse

    c. Carrying case

    d. Optional wireless card

    e. Basic Board-approved software and configurations.

Use of Laptops

1. Board acceptable use policy must be complied with at all times including but not restricted to the following:

    a. the Laptops that are checked out are not for personal use;

    b. loading of personal software is prohibited; and

  c. alterations to pre-loaded set-up is restricted to IT personnel

2. User is responsible for all data and file back-ups and all data will be stored only on encrypted USB storage devices.

3. Only the board employee who signs out the laptop shall use the laptop.

4. Any use of the laptop outside Saskatchewan of Canada Canada:

  a. must be disclosed when requesting the laptop;

  b. is subject to approval by the IT Manager who may impose whatever conditions on such use as he or she may deem advisable.

Responsibility for Loss or Damage

1. Normal use and wear is covered under the laptop warranty

2. Responsibility for the laptop when it is checked out is placed upon the employee and if the laptop is stolen or damaged due to negligence or preventable accident the employee shall be responsible for the cost of replacement of the equipment.

3. Theft of equipment must be reported immediately to police

Laptop Sign out Form

1. A Laptop Sign out must be filled out, and signed by the employee:

2. The Checkout date and Return Date on the form must be strictly observed.

Consequences of Non-Compliance

1. An employee who does not comply with this policy :

  a. may be subject to disciplinary action; and

  b. may be denied access to sign-out of board owned laptops

MEMORY KEYS

1. Memory Keys will be available to sign out from the office for the purpose of carrying information when an employee is out of the office.

2. The office memory keys will be encrypted.

3. All information will be deleted from the memory key when it is returned to the office. It is the responsibility of the employee to ensure that any required copies of information are made.

EMAIL

1. Emails must be encrypted in the following circumstances:

   (a) confidential information is being transmitted; or

   (b) personal information is being transmitted

2. All emails must contain a confidentiality notice in the signature line.

PASSWORDS

1. Passwords shall be kept confidential and must not be written down.

2. Passwords shall include numbers and letters.

3. Certain days will be designated by IT support services twice a year and all employees will be required to change passwords on the designated days.

PERSONAL DEVICES

1. Use of Personal Devices will follow the same rules as Memory Sticks and email.

CONSEQUENCES

1. All use of equipment must meet the requirements of Policy # _____(Acceptable Uses Policy) and any violation of this Security policy will be treated as a violation of the Acceptable Uses Policy.

2. Patterns of behaviour indicating lack of care may result in an individual employee being denied the ability to take out a laptop or memory key