USE OF PORTABLE INFORMATION & STORAGE DEVICES

Background

The Division supports the use of technology and networks for the purpose of supporting and enhancing teaching and learning. As well it is recognized that technology has a prominent role in information and records management. As a result, personal information is stored in electronic format.

All personal information is sensitive; therefore, privacy shall be protected during the collection, storage, use, sharing and transmission of personally identifiable information.

Definitions

For the purposes of this procedure:

1. Portable information devices and portable information storage media (PIDs) include, but are not limited to, the following:

    a. Electronic computing and communication devices and media designed for mobility, including laptop, and in-vehicle personal computers, blackberry type devices, personal data assistants, cellular devices, and other devices that have the ability to store data electronically;

    b. CDs, DVDs, flash memory drives, zip drives, backup tapes, and other information storage media or devices that provide portability or mobility of data; and

    c. Devices used for school business purposes whether it is division or personal technology.

2. Under the *FOIP Act,* personal information means recorded information about an identifiable individual, including:

    a. Name, home or business address, or home or business telephone number;

    b. Race, national or ethnic origin, colour or religious or political beliefs or associations;
    c. Age, sex, marital status or family status;

    d. An identifying number, symbol or other particular assigned to the individual;

e. Fingerprints, other biometric information, blood type, genetic information or inheritable characteristics, and photo likeness;

f. Information about the individual's health and health care history, including information about a learning, physical or mental disability;

g. Information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;

h. Another's opinion about the individual; and

i. The individual's personal views or opinions, except if they are about someone else.

Guidelines

1. Principals and department managers shall ensure that an adequate level of security is provided for personal information that is within their control and custody and shall ensure that the staff they supervise is aware that all employees who use personal information in the execution of their duties shall:

   a. Use secure remote connections, whenever possible, to access personal information on the Division network rather than storing personal information on PIDs;

   b. Not save or store, when using secure remote connections, personal information on a PID unless it is encrypted and password protected, or save or store personal information on a home computer;

   c. Refrain from loading personal information on PIDs unless it is impossible to carry out their duties without this information;

   d. Copy, download or transport only the personal information that is required for specific tasks;

   e. Keep the paper records and PIDs secure;

   f. Ensure that division information on a PID can be replaced if the storage device is lost or stolen;

   g. Destroy or remove transitory paper and digital or electronic records and/or return division records containing personal information about students, parents and staff of Greater St. Albert Catholic Schools when it is no longer needed to carry out their duties.

2. If personal information must be placed on a portable information device, then that information must be password protected and encrypted.

Technical details about passwords, encryption, device deactivation, remote information deletion and other technical solutions, are available from the Learning Technology Services.

3. Division staff using PIDs that contain personal information shall follow these security procedures:

   a. Ensure the portable device is labeled with appropriate contact information in case of loss;

   b. Ensure portable devices or portable storage are stored in secured areas;

   c. Ensure any personal information on a PID is encrypted;

   d. Ensure that PIDs are protected by strong passwords; and

   e. Confer with division technical support for specific technology help, including procedures for the encryption of data.

4. Employees shall report incidents involving personal information as follows:

   a. Immediately report loss, theft or unauthorized access of personal information and other security related incidents to a supervisor and to the superintendent of schools;

   b. Immediately report theft of PIDs or records containing personal information to local police; and

   c. Document the details of any loss, theft, unauthorized access of PIDs, or personal information security related incident, including an inventory of the personal data involved.

5. The principal or department administrator shall send out notification letters to all individuals whose personal information was subject to an inadvertent disclosure as soon as possible.

6. Employees who are required to use cellular phones as part of their duties shall ensure that for school division staff and students all personal information such as the individual's name, home or business address, or home or business telephone number that is stored on the device are encrypted and password protected.

   Information that does not require secure action is:

   a. Public information such as that which is posted in a public telephone directory; and

   b. Information for which written consent to store unsecured has been received. Written consent must be kept on file.

Implementation Date: March 7, 2014
Revised November 30, 2019