

EHA-APM – Information Security Procedure

Administrative Procedure

INTRODUCTION

A student, parent or staff member provides their personal information to the district trusting that the district will use it only as necessary to carry out the district's mandate. The security of personal information is compromised when the information is stored on portable information devices or when the information is transported to and from work and home.

All district records created by staff in the course of their work are subject to the [*Freedom of Information and Protection of Privacy Act*](#) and are under the custody and or control of the district at all times. The [*Freedom of Information and Protection of Privacy Act*](#) and the orders of the privacy commissioner provide standards for the security of personal information.

DEFINITIONS

Personal Information - Under the Freedom of Information and Protection of Privacy Act, "personal information" means recorded information about an identifiable individual, including:

- a. the individual's name, home or business address or home or business telephone number,
- b. the individual's race, national or ethnic origin, colour or religious or political beliefs or associations,
- c. the individual's age, sex, marital status or family status,
- d. an identifying number, symbol or other particular assigned to the individual,
- e. the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,
- f. information about the individual's health and health care history, including information about a 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, anyone else's opinions about the individual, and
- h. the individual's personal views or opinions, except if they are about someone else.

Portable Information Devices (PID) and Portable Information Storage Media include (but is not limited to) the following:

- a. electronic computing and communication devices and media designed for mobility, including laptop, desktop, and in-vehicle personal computers, smartphones, 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.

ADMINISTRATIVE PROCEDURE

1. School Administrators and Executive shall ensure that an adequate level of security is provided for personal information that is in their control and custody and shall ensure that the staff they supervise are aware of the following responsibilities.

All employees who use personal information in the execution of their duties shall:

- a. use secure remote connections to access personal information on the district network rather than storing personal information on PIDs whenever possible; and
 - b. refrain from loading personal information on PIDs unless it is impossible to carry out their duties without this information; and
 - c. only copy, download or transport the personal information that is required for specific tasks; and
 - d. keep the paper records and PIDs secure; and
 - e. maintain an inventory or copy of the personal information temporarily stored at home or on PIDs under their control; and
 - f. ensure that district information on a PID can be replaced if the storage device is lost or stolen; and
 - g. destroy or remove transitory paper, digital or electronic records and or return district records containing personal information about students, parents and staff of Peace Wapiti Public School Division when it is no longer needed to carry out their duties.
2. PID configuration specifications - If personal information must be placed on a PID, then that information must be password protected and encrypted. For further technical details about passwords, encryption, device deactivation, remote information deletion and other technical solutions, refer to the Technology Handbook:
<https://sharepoint.pwsd76.ab.ca/Departments/Technology/Shared%20Documents/TechnologyHandbook.docx>
 3. District 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; and
 - b. do not leave portable devices or portable storage in non-secured areas; and
 - c. do not leave portable device or portable storage in an unlocked vehicle; place the devices and storage in a locked trunk; and
 - d. any personal information on PID must be encrypted; and
 - e. ensure that PIDs are protected by strong passwords; and

EHA-APM – Information Security Procedure

Administrative Procedure

- f. confer with district technical support for specific technology help, including procedures for the encryption of data.
4. Employees shall report incidents involving personal information as follows (The personal information could be contained on laptops, blackberries, paper files, cameras, misdirected e-mails, e-mails that contain the home e-mail addresses of staff, parents or students, etc.) :
 - a. immediately report loss, theft or unauthorized access of personal information and other security related incidents to a supervisor and to the Superintendent: and
 - i. immediately report theft of PIDs or records containing personal information to local police; and
 - ii. 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.
 - b. Any person aware of an unreported loss, theft or compromise of personal information shall make a report to their supervisor and the superintendent of schools as soon as possible.
 - c. A FOIP Risk assessment shall be prepared and if applicable, notification letters to all individuals whose personal information was subject to an inadvertent disclosure shall be sent out as soon as possible.
5. Violations of this regulation shall result in disciplinary action for individuals, up to and including termination.