ADMINISTRATION 1 – Security of Personal and Division Information

Date: Feb. 12, 2010 Revised: Responsible Administrator: Assoc. Superintendent, Student Services

1.0 Board Regulation, Administration 1 - Security of Personal and Division Information shall be administered in compliance with Policy E/IV/1 and Admin Practice *Student Services 5*.

2.0 PROCESS

2.1 Principals and Supervisors 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 staffs they supervise are aware of the following responsibilities.

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

2.1.1 use secure remote connections to access personal information on the division network rather than storing personal information on PIDs whenever possible; and

2.1.2 refrain from loading personal information on PIDs unless it is impossible to carry out their duties without this information; and

2.1.3 only copy, download or transport the personal information that is required for specific tasks; and

2.1.4 keep the paper records and PIDs secure; and

2.1.5 maintain an inventory of the personal information while it is temporarily stored at home or on PIDs under their control; and

2.1.6 destroy or remove transitory paper, digital or electronic records and or return division records containing personal information about students, parents and staff of Sturgeon School Division when it is no longer needed to carry out their duties.

2.1.6.1 Paper records are destroyed at the worksite by shredding or through an approved vendor.

2.1.6.2 Electronic records are deleted from the source when electronic devices are terminated or transferred.

2.1.6.3 Electronic memory is processed through the technology department to ensure that deleted information is not retrievable.

References: *Board Policy(s): D/I/3 Security of Personal and Divisional Information*
Admin Practice(s): Student Services 5, Student Records Management

2.2 PID configuration specifications

2.2.1 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, consult with Division Technology Department.

2.3 Division staff using PIDs or paper records that contain personal information shall follow these security procedures:

2.3.1 do not leave paper records or portable devices or portable storage in non-secured areas; and

2.3.2 do not leave paper records, portable device(s) or portable storage in an unlocked vehicle; place the devices and storage in a locked trunk and if possible, secure with a cable lock

2.3.3 any personal information on PID must be encrypted; and

2.3.4 ensure that PIDs are protected by strong passwords; and

2.3.5 ensure that computers are shut down during transit

2.3.6 confer with division technical staff for specific technology support, including procedures for the encryption of data.

2.4 Employees shall report incidents involving personal information as follows:

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

2.4.1.1 immediately report theft of PIDs or records containing personal information to local police; and

References: *Board Policy(s): D/I/3 Security of Personal and Divisional Information*
Admin Practice(s): Student Services 5, Student Records Management

2.4.1.2 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.

2.4.2 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.

2.4.3 The Principal or Supervisor shall send out notification letters to all individuals whose personal information was subject to an inadvertent disclosure as soon as possible.

2.5 Violations of this policy shall result in disciplinary action for individuals, up to and including termination.

3.0 GUIDELINES

3.1 Definitions

3.1.1 Personal Information

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

3.1.1.1 the individual's name, home or business address or home or business telephone number,

3.1.1.2 the individual's race, national or ethnic origin, colour or religious or political beliefs or associations,

3.1.1.3 the individual's age, sex, marital status or family status,

3.1.1.4 an identifying number, symbol or other particular assigned to the individual,

3.1.1.5 the individual's fingerprints, other biometric

References: *Board Policy(s): D/I/3 Security of Personal and Divisional Information*
Admin Practice(s): Student Services 5, Student Records Management

3.1.1.6 information, blood type, genetic information or inheritable characteristics,

3.1.1.7 information about the individual's health and health care history, including information about a physical or mental disability,

3.1.1.8 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

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

3.2 Portable Information Devices (PID) and Portable Information Storage Media

3.2.1 Portable information devices and portable information storage media include (but are not limited to) the following:

3.2.2 electronic computing and communication devices and media designed for mobility, including laptop, desktop, and in-vehicle personal computers, blackberries, personal data assistants, cellular devices, and other devices that have the ability to store data electronically,

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

References: *Board Policy(s): D/I/3 Security of Personal and Divisional Information*
Admin Practice(s): Student Services 5, Student Records Management