387 – FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY

Introduction

The Board of Education is a public body subject to the BC *Freedom of Information and Protection of Privacy Act* (FOIPPA) and the *School Act*. Both statutes contain provisions that regulate the public's access to information held by the District and govern the District's responsibilities to protect personal information from unauthorized access, use or disclosure. Also, the District must ensure that all personal information held in its custody and control is protected by reasonable security arrangements.

Policy

Responsibility

The Secretary-Treasurer/CFO has been designated by the Board of Education as the District lead for the purposes of FOIPPA, and has overarching responsibility for ensuring compliance with this Policy, FOIPPA and the requirements of the School Act pertaining to student records.

Personal Information

Under the FOIPPA, "personal information" means any information about an identifiable individual. Personal information may include data such as unique identifiers (PEN/SIN), school records, contact numbers, gender, medical history, education, employment, psychiatric history, behavioural assessments, personnel evaluations, digital images, audio and video recordings, racial or ethnic origin, sexual orientation or religious beliefs.

"Contact information" means information enabling an employee to be contacted at work and includes the name, position, business contact number, business address and business email.

Employee Personal Information

Employee personal information is any recorded information about an identifiable employee (see Personal Information above) other than contact information. The release and sharing of contact information is not a privacy violation.

Student Personal Information

Student personal information includes Personal Information (defined above) plus any information that identifies a student including the student's name, address, and contact numbers, Personal Education Number, assessments, results, and educational records. District employees may disclose student personal information to other District employees where such disclosure is necessary for the performance of the duties of the employee and to other School Districts where it is necessary for educational purposes.

Collection of Personal Information

The District has the legal authority to collect personal information that relates directly to and is necessary for its operating programs or activities or as otherwise authorized by statute. Personal information will be collected directly from the individual the information is about unless another method of collection is authorized by the individual or the statute.

When a school or the District collects personal information about students or families, parents/guardians should be informed of the purpose for which the information is being collected. The parents/guardians of a student must authorize the disclosure of personal information for purposes ancillary to educational programs such as:

- newsletter publications;
- website postings;
- video conferencing;
- social media applications;
- honour roll lists;
- team rosters; or
- yearbooks.

Parents/guardians will complete and submit the form entitled STUDENT REGISTRATION FORM – Freedom of Information and Protection of Privacy upon their child's initial enrollment. Where the parent or guardian provides consent, this will allow the school or the District to publish student personal information for purposes such as:

- recognition of achievement;
- promotion of events; or
- commemoration of school events.

The authorization is deemed in effect until the student changes or transitions to another school. Parents/guardians will have the ability to opt out of providing information that is not directly related to a student's educational program or necessary for the District's operational activities. Posting of personal information such as exam results should not contain student identifiers.

Use of Personal Information

Personal information will be used for the purpose for which it was collected or for a use consistent with that purpose. Should there be a need to access information for a purpose other than why it was collected or if there is uncertainty as to the confidentiality of the information; clarification will be provided from the District Privacy Officer.

Disclosure of Personal Information

Personal information may be disclosed to an external or third party if the individual who is the subject of the information has provided written consent. In the case of a student under age nineteen, such consent may be provided by the student's parent or guardian.

Consent is not required from a student or parent when information is being disclosed for worker safety. If a plan is developed to protect the health and safety of a worker, which also affects the health and safety of the student, the parent will be informed, as per requirements of the School Act. However, parental approval is not required to develop and implement plans to keep workers safe.

Disclosure of personal information should not occur when using a mobile phone or in any physical location that may compromise confidentiality.

Access to Personal Information

Employees of the District have a general right of access to any record in the custody or under the control of the District, provided that access is required to complete the duties of the work assignment.

A parent or guardian has the right to access personal information on behalf of a child under the age of nineteen.

The District governs the right of access by an individual to his/her own personal information and by the public to any information or records in its custody or control of the District.
School districts, other government ministries or law enforcement agencies may have access to personal information where obtaining this information is necessary for the provision of their services.

Securing Personal Information

Information management must be dealt with in a responsible, efficient, ethical and legal manner. Users of electronic network resources should not disseminate personal information to anyone not covered by a confidentiality agreement, also precautions should be taken to ensure information is protected from unauthorized access, use and disclosure. All District employees are expected to maintain, secure and retain appropriate student and personnel records in a manner that respects the privacy of employees, students and students' families and complies with the regulations specified in FOIPPA and the School Act.

The following safeguards, though not an exhaustive list, will assist in protecting privacy of personal information for both students and employees:

- security (e.g. passwords, encryption) must be in place for personal information, stored, printed or transferred by computers;
- all electronic mobile devices (even personally owned devices) that access or store District data must be secured by a password logon and use the highest available encryption options;
- electronic mobile devices that contain or can access District data should be kept on one's person and never be left unattended in public areas (i.e. classrooms, hotel rooms);
- passwords should not be shared nor should anyone logon to a system using an ID that has not been specifically assigned to them; and

- paper files should be safeguarded by implementing reasonable security precautions:
  - locked storage;
  - removal of personal information from work areas; and
  - shredding of documents containing personal information.

Access to any personal information should be based on employment duties requiring such access. Unauthorized access to information about colleagues, friends, or family is not permitted. Any personal information that is no longer required for administrative, financial or legal purposes will be destroyed in a confidential manner. Paper files due for destruction should be securely shredded and disposed of; computer files should be deleted in their entirety; any data storage devises should be fully erased prior to disposal (i.e. computers, Multi Functional Devices, printers).

Requirements Related to Student Privacy and Worker Health and Safety

FOIPPA allows for disclosure of personal information within an organization "if the information is immediately necessary for the protection of the health or safety of the…employee". Disclosure is required if the answer is "yes" to the question "Is disclosing this information necessary to help protect this worker's safety?"

Employers are obligated to investigate incidents that caused or could have caused injury to their workers, in conjunction with a joint Occupational Health and Safety Committee. If student information is used to complete an incident investigation or inspection report, personal identifiers must be removed so the issue is understandable but the students are not able to be identified.

The Workers Compensation Act requires that employers inform their workers about all known or reasonably foreseeable health and safety hazards, including workplace violence. The Occupational Health and Safety Regulation defines violence as "the attempted or actual exercise by a person, other than a worker, of any physical force so as to cause injury to a worker, and includes any threatening statement or behaviour which gives a worker reasonable cause to believe that he or she is at risk of injury". These behaviours do not need to have intent to injure. Within the education sector, students who inflict physical force causing injury or engage in threats are sometimes referred to as "having behavioural challenges" or "acting out".

Investigation of Complaints

Anyone suspecting or aware of the unauthorized collection, use, access, or disclosure of student or employee personal information, breach of confidentiality protocols or contraventions of this Policy must report such activities to the District Privacy Officer (Secretary-Treasurer/CFO).