*SCHOOL DISTRICT NO. 67 (OKANAGAN SKAHA)*

# POLICY

**POLICY #290 Freedom of Information and Protection of Privacy**

## RATIONALE

The Board of Education is a public body subject to the BC *Freedom of Information and Protection of Privacy Act* (*FOIPPA*). This statute contains 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. The District must ensure all personal information held in its custody and control is protected by reasonable security arrangements.

## POLICY

As the custodians of both student and employee personal information, the Board of Education of School District No. 67 (Okanagan Skaha) has the legal obligation to safeguard the confidentiality of personal information pertaining to private individuals. Personal information may only be obtained as authorized by *FOIPPA* and used for the specific purposes for which it is gathered. The management and safekeeping of such information is the responsibility of each designated employee. The Secretary Treasurer is the District Privacy Officer and will monitor this policy.

| | | | |
|---|---|---|---|
| ADOPTED: | January 11, 2016 | Reviewed/Revised: | |
| | | Statutory Reference: | *Freedom of Information and Protection of Privacy Act* |

*SCHOOL DISTRICT NO. 67 (OKANAGAN SKAHA)*

# REGULATIONS AND PROCEDURES

**POLICY #290 Freedom of Information and Protection of Privacy**

## 1. Descriptions:

1.1. Personal Information – Under *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, behavioral assessments, personnel evaluations, digital images, audio and video recordings, racial or ethnic origin, sexual orientation or religious beliefs.

1.2. Contact Information – Under *FOIPPA,* "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.

1.3. Employee Personal Information – Under *FOIPPA,* "employee personal information" means 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.

1.4. Student Personal Information – Under *FOIPPA,* "student personal information" includes personal information (as defined above) plus any information that identifies a student including the student's full name, address, and contact numbers, PEN (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.

## 2. Collection of Personal Information

2.1 Employees will be directly notified of this policy.

2.2 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 reasonably required to establish, maintain, manage or terminate an employment relationship without consent assuming employees have been notified of the collection of information. Personal information will be collected directly from the individual the information is about; other methods of collection may be indirectly used as governed by *FOIPPA.*

2.3 Other methods of collection may include, but not limited to, GPS or video surveillance. GPS is used by the District to track assets and may on occasion be used to locate employees as cell phones are not provided for contact. Video surveillance is used for asset, student and employee safety. Indirect collection methods may be used should a student or employee come under investigation; all use will follow *FOIPPA.*

2.4 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 posting;
- video conferencing;
- social media applications;
- honour roll lists;
- team rosters; or
- yearbooks

Parents/guardians will compete and submit the form entitled PARENTAL CONSENT upon their child's initial enrolment. Where the parent/guardian provides consent, this will allow the school or 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.

**3. Use of Personal Information**

3.1 Personal information will be used for the purpose for which it is 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.

**4. Disclosure of Personal Information**

4.1 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 19, such consent may be provided by the student's parent/guardian. Disclosure of personal information should not occur when using a mobile phone or in any physical location that may compromise confidentiality.

**5. Access to Personal Information**

5.1 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.

5.2 A parent/guardian has the right to access personal information on behalf of a child under the age of 19.

5.3 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.

## 6. Securing Personal Information

6.1 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; additionally, 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*.

6.2 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;
- All 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 (e.g.: 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 such as, locked storage, removal of personal information from work areas, and shredding of documents containing personal information.

6.3 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 devices should be fully erased prior to disposal.

## 7. Investigation of Complaints

7.1 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).

| | | | |
|---|---|---|---|
| ADOPTED: | January 11, 2016 | Reviewed/Revised: | |
| | | Statutory Reference: | *Freedom of Information and Protection of Privacy Act* |