# SCHOOL DISTRICT NO. 53 (Okanagan Similkameen)
# POLICY

No. G-2

**Amended: June 25, 2008**
**Amended: February 22, 2012**
**Reviewed: January 24, 2018**
**Amended: June 21, 2023**

## PUBLIC ACCESS TO INFORMATION AND PROTECTION OF PRIVACY

**Preamble:**

As a public body that is subject to the British Columbia *Freedom of Information and Protection of Privacy Act* (the "Act" or "FIPPA"), the Board of Education of School District No. 53 (Okanagan Similkameen) is committed to upholding the principles of privacy, transparency, and accountability. The School District recognizes the importance of maintaining the privacy and security of the Personal Information it collects, uses and discloses in the course of its operations. The School District acknowledges and supports transparency with the community by facilitating access to School District records and information in accordance with the requirements of the Act.

**Policy:**

The Board of Education will follow the provisions of the *Freedom of Information and Protection of Privacy Act* (hereafter referred to as the "Act"):

1. To collect, use, protect and where permitted provide access to the personal information of private individuals including students and Board employees.
2. To govern the right of access by the public to information or records in the custody or control of the Board.
3. To implement a District Privacy Management Program.
4. To follow mandatory Privacy Breach reporting requirement.

The Board designates the Superintendent of Schools as the 'Head'/ CEO of the School District for the purposes of the Act to make operational decisions and to issue any procedures to support the administration of the Act.

The Superintendent of Schools designates the Secretary Treasurer as the District Privacy Officer.

The management, safekeeping and confidentiality of such information is the responsibility of each employee as designated by the Superintendent of Schools.

Fees charged to provide information under the Act will be assessed in accordance with the provisions set out in Section 75 Fees of the Act.

Freedom of Information and Protection of Privacy Act (gov.bc.ca)

**SCHOOL DISTRICT NO. 53 (Okanagan Similkameen)**

**REGULATIONS**

**No. G-2**

Adopted: June 21, 2023

## PUBLIC ACCESS TO INFORMATION AND PROTECTION OF PRIVACY

### I. Management of Personal Information:

**'**Personal Information' means recorded information about an identifiable individual but excludes a person's business contact information.

#### 1. Purposes for Collecting Personal Information:

The School District collects Personal Information of its students in the ordinary course of carrying out its activities for purposes, including:

- Registration, enrolment, and transfer of students.
- To provide educational programs and services.
- To accommodate students with special needs.
- To communicate with students and respond to inquiries or complaints.
- To prepare and provide assessments of student performance.
- To supervise and ensure the safety and security of the School District (e.g. through the use of video surveillance).
- To investigate and respond to accidents, safety events, misconduct.
- To ensure compliance with applicable School District policies and bylaws.
- To make all required reports and filings to the Ministry of Education and Child Care.
- For other purposes set out in this procedure or required under applicable laws.

The School District collects prospective, current and former staff in the ordinary course of carrying out its activities for purposes, including:

- To hire and recruit.
- To administer and manage the employment relationship.
- To administer employment compensation and benefits.
- To evaluate performance and manage disciplinary incidents.
- To communicate with authorized union representatives.
- To supervise and ensure the safety and security of the School District (e.g. through the use of video surveillance).
- To investigate and respond to accidents, safety events, misconduct.
- To ensure compliance with applicable School District policies and bylaws.
- For other purposes set out in this procedure or required under applicable laws.

#### 2. Collection, Use and Disclosure of Personal Information

The School District limits the Personal Information it collects to what is related to and necessary to carry out its activities or for other purposes authorized by the Act.

Personal Information will be collected by fair, lawful and transparent means; personal information will be collected directly from the individual, except where otherwise authorized by the Act.

The School District will inform individuals from whom it collects Personal Information the purposes for which the information is being collected, the legal authority for collecting it and the name and contact information of someone at the School District who can answer questions about the collection and use of the information. The internal and external use and sharing of Personal Information will be limited to what is required and authorized by the Act or consented to by the individual.

The School District only uses or discloses Personal Information for the purpose for which it is collected, except with the individual's consent or as otherwise required or permitted by the Act or other legislations.

**3. Securing Personal Information**

The School District protects Personal Information by ensuring it has reasonable security safeguards in place which are appropriate to the sensitivity of the information. Security safeguards will include consideration of physical, organizational and electronic security. All staff have a duty to protect the privacy and security of Personal Information collected and used by them as part of their ongoing employment responsibilities, including by complying with this regulation and all related regulations.

The School District will provide training to all staff, ensuring they have the requisite knowledge to ensure compliance with this regulation and the Act.

**4. Retention and Disposal of Personal Information**

The School District does not seek to retain Personal Information longer than necessary to satisfy its operational, instructional, financial, and legal needs.

Personal Information that is no longer required for the aforementioned needs shall be securely destroyed in accordance with appropriate standards and practice.

**5. Access to Information**

The School District will make information available to the public as permitted or required by the Act.

The School District recognizes that individuals may request for access to Records that are in the custody and control of the School District. The School District's response to such requests will be in accordance with this Regulation and the Act.

The School District recognizes that individuals have a right to access their own Personal Information within the custody and control of the School District and will facilitate such access in accordance with this Regulation and the Act.

## II. Privacy Breach

'Privacy Breach' means the theft or loss of or the collection, use or disclosure of Personal Information not authorized by the Act. This includes cyber and ransomware attacks and other situations where there are reasonable grounds to believe that any such unauthorized activities have occurred or there is reasonable belief that they will occur.

A 'Record' means books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or the mechanism that produces a record.

**1. Responsibilities of Staff**

a. All staff must without delay report all actual, suspected or expected Privacy Breach incidents of which they become aware in accordance with this regulation. All staff have a legal responsibility under the Act to report Privacy Breaches to the Privacy Officer.
b. If there is any question about whether an incident constitutes a Privacy Breach or whether the incident has occurred, Staff should consult with the Privacy Officer.
c. All Staff must provide their full cooperation in any investigation or response to a Privacy Breach incident and comply with this regulation for responding to Privacy Breach incidents.
d. Any Staff member who knowingly refuses or neglects to report a Privacy Breach in accordance with this regulation may be subject to discipline, up to and including dismissal.

**2. Privacy Breach Response**

a. Step one - Report and Contain
    i. Upon discovery or learning of a Privacy Breach, all Staff shall:
        1) Immediately report the Privacy Breach to the Privacy Officer.
        2) Take any immediately available actions to stop or contain the Privacy Breach, such as:
            - Isolating or suspending the activity that led to the Privacy Breach; and
            - Taking steps to recover Personal Information, Records or affected equipment.
        3) Preserve any information or evidence related to the Privacy Breach in order to support the School District's response.
    ii. Upon notification of a Privacy Breach the Privacy Officer shall implement all available measures to stop or contain the Privacy Breach. Containing the Privacy Breach shall be the priority of the Privacy Breach response, and all Staff are expected to provide their full cooperation with such initiatives.

b. Step two – Assessment and Containment
    i. The Privacy Officer shall take steps to contain the Privacy Breach by making the following assessments:
        1) The cause of the Privacy Breach.
        2) If additional steps are required to contain the Privacy Breach, and, to implement such steps as necessary.
        3) Identify the type and sensitivity of the Personal Information involved in the Privacy Breach, and any steps that have been taken or can be taken to minimize the harm arising from the Privacy Breach.

4) Identify the individuals affected by the Privacy Breach or whose Personal Information may have been involved in the Privacy Breach; determine or estimated the number of affected individuals and compile a list of such individuals.
5) Make preliminary assessments of the types of harm that may flow from the Privacy Breach.

ii. The Privacy Officer shall be responsible to assess whether the Privacy Breach could reasonably be expected to result in Significant Harm to individuals. Determining Significant Harm shall be made with consideration of the following categories of harm or potential harm:
1) Bodily harm.
2) Humiliation.
3) Damage to reputation or relationships.
4) Loss of employment, business or professional opportunities.
5) Financial Loss.
6) Negative impact on credit record.
7) Damage to or loss of property.
8) The sensitivity of the Personal Information involved in the Privacy Breach.
9) The risk of identity theft.

c. Step three – Notification
i. If the Privacy Officer determines that the Privacy Breach could reasonably be expected to result in Significant Harm to individuals, then the Privacy Officer shall make arrangements to:
1) Report the Privacy Breach to the Office of the Information and Privacy Commissioner, and
2) Provide notice of the Privacy Breach to affected individuals, unless the Privacy Officer determines that providing such notice could reasonably be expected to result in grave or immediate harm to an individual's safety or physical or mental health or threaten another individual's safety or physical or mental health.

ii. If the Privacy Officer determines that the Privacy Breach does not give rise to a reasonable expectation of Significant Harm, then the Privacy Officer may still proceed with notification to the affected individual if the Privacy Officer determines that notification would be in the public interest or if a failure to notify would be inconsistent with the School District's obligations or undermine public confidence in the School District.

iii. Determining notifications of a Privacy Breach shall be made without delay following a Privacy Breach and notification shall be undertaken as soon as reasonably possible. If any law enforcement agencies are involved in the Privacy Breach incident, then notification may also be undertaken in consultation with such agencies.

d. Step four – Prevention
i. The Privacy Officer shall complete an investigation into the causes of each Privacy Breach incident reported under this regulation and shall implement measures to prevent recurrences of similar incidents.

### 3) Privacy Impact Assessments

A 'Privacy Impact Assessment' (PIA) is an in-depth review of any new or significantly revised initiative, project, activity or program to ensure that it is compliant with the provision of the Act, to identify and mitigate risks arising from the initiative and to ensure that the initiative appropriately protects the privacy of individuals.

This regulation applies to all new and significantly revised initiatives of the School District. All School District staff are expected to be aware and follow this regulation in the event that they are involved in a new or significantly revised initiative. School administration and senior management staff are responsible to plan and implement new or significantly revised initiatives in accordance with this regulation.

The Privacy Officer in consultation with the District's Privacy Committee will ensure that all PIAs are completed in accordance with the requirements of the Act.

**Staff Responsibilities:** Any staff member responsible for developing or introducing a new or significantly revised initiative that involves or may involve the collection, use, disclosure or processing of Personal Information by the School District must report that Initiative to the Privacy Officer at an early stage in its development. Staff will cooperate with the Privacy Officer and provide all requested information needed to complete a PIA.

**The Role of the Responsible Staff Member:** A staff member responsible for an initiative should:

- Ensure that new and significantly revised initiatives for which they are responsible are referred to the Privacy Officer for completion of PIA.
- Support all required work necessary for the completion and approval of PIA.
- Be familiar with and ensure that the initiative is carried out in compliance with PIA.
- Request that the Privacy Officer make amendments to the PIA when needed and when significant changes to the initiative are made.

**Initiatives Involving the Storage of Personal Information Outside Canada**

1. District staff may not engage in any new or significantly revised initiative that involves the storage of Personal Information outside Canada until the Privacy Officer has completed a PIA and any supplemental review.
2. The responsible staff member may not enter into a binding commitment to participate in any initiative that involves the storage of Personal Information outside Canada unless any required supplemental review has been completed and approved by the Privacy Officer.
3. It is the responsibility of the Privacy Officer to determine whether a supplemental review is required in relation to any initiative, and to ensure that such review is completed in accordance with the Act.
4. The following risks should be considered while reviewing and/or approving supplemental reviews:
    - The likelihood that the initiative will give rise to an unauthorized collection, use, disclosure or storage of Personal Information.
    - The impact to an individual of an unauthorized collection, use, disclosure or storage of Personal Information.

- Whether the Personal Information is stored by a service provider.
- Where the Personal Information is stored.
- Whether the supplemental review sets out mitigation strategies corresponding to the level of risk posed by the initiative.

**Contact Information:**
Questions and complaints about Privacy matters are to be direct to the School District's Privacy Officer at privacyofficer@sd53.bc.ca. The School District commits to responding to all complaints in writing.