ADMINISTRATION Policy 311-G (B)

Critical Incident and Privacy Breach Procedure

1. Purpose

The Board of Education of School District No. 38 (Richmond) ("District") is committed to ensuring the protection and security of all personal information within its control. That commitment includes responding effectively and efficiently to privacy breach incidents that may occur.

The purpose of these Guidelines is to set out the District's process for responding to significant privacy breaches and to complying with its notice and other obligations under the *Freedom of Information and Protection of Privacy Act (FIPPA)*.

2. Scope & Responsibility

All Employees of the District are expected to be aware of and follow these Guidelines in the event of a privacy breach. These Guidelines apply to all Employees.

3. District Responsibilities

3.1 The Superintendent of Schools is the "Head" of the District for all purposes under the *FIPPA*.

3.2 The Superintendent has delegated the administration of these Guidelines under *FIPPA* to the Secretary Treasurer, who is the "Privacy Officer" of the District for all purposes under *FIPPA*.

3.3 The Privacy Officer is responsible to, in consultation with the Head, ensure that all procedures are completed to respond to privacy breach in accordance with the requirements of *FIPPA* and these Guidelines.

4. Definitions

4.1 "**Employee(s)**" means the employees, contractors and volunteers of the District;

4.2 "**FIPPA**" means the *British Columbia Freedom of Information and Protection of Privacy Act*, and regulations thereto;

4.3 "**Guidelines**" means procedures enacted by the District under its Policy on Freedom of Information and Protection of Privacy;

4.4 "**Head**" means the Superintendent of Schools or any person to whom the Superintendent has delegated (in writing) their powers under these Guidelines;

4.5 "**Personal information**" means any recorded information about an identifiable individual that is within the control of the District, and includes information about any student or any Employee of the District. Personal Information does not include an individual's business contact information, such as business address, email address and telephone number, that would allow a person to be contacted at work;

4.6 "**Privacy Breach**" means the theft or loss of or the collection, use or disclosure of Personal Information not authorized by *FIPPA*, and includes cyber and ransomware attacks and other situations where there are reasonable grounds to believe that any such unauthorized activities have taken place or there is a reasonable belief that they will take place;

4.7 "**Privacy Officer**" means the Secretary Treasurer who has been designated by the Head as Privacy Officer for the District;

4.8 "**Records**" 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 other mechanism that produces records.

5. Responsibilities of Employees

5.1 All Employees must without delay report all actual, suspected or expected Privacy Breach incidents of which they become aware in accordance with these Guidelines. All Employees have a legal responsibility under *FIPPA* to report Privacy Breaches to the Head.

5.2 Privacy Breach reports may also be made to the Privacy Officer, who has delegated responsibility for receiving and responding to such reports.

5.3 If there is any question about whether an incident constitutes a Privacy Breach or whether the incident has occurred, Employees should consult with the Privacy Officer.

5.4 All Personnel must provide their full cooperation in any investigation or response to a Privacy Breach incident and comply with these Guidelines for responding to Privacy Breach incidents.

5.5 Any Employee who knowingly refuses or neglects to report a Privacy Breach in accordance with these Guidelines may be subject to discipline, up to and including dismissal.

6. Privacy Breach Response

6.1 Step One – Report and Contain

6.1.1 Upon discovering or learning of a Privacy Breach, all Employees 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 by:

- 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 District's incident response.

6.1.2 Upon being notified of a Privacy Breach the Privacy Officer in consultation with the Head, shall implement all available measures to stop or contain the Privacy Breach. Containing the Privacy Breach shall be the first priority of the Privacy Breach response, and all Employees are expected to provide their full cooperation with such initiatives.

6.2 Step Two – Assessment and Containment

6.2.1 The Privacy Officer shall take steps to, in consultation with the Head, 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, if so, 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;
5. determine or estimate the number of affected individuals and compile a list of such individuals, if possible; and
6. make preliminary assessments of the types of harm that may flow from the Privacy Breach.

6.2.2 The Privacy Officer, in consultation with the Head, shall be responsible to, without delay, assess whether the Privacy Breach could reasonably be expected to result in significant harm to individuals ("**Significant Harm**"). That determination 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; and

9. the risk of identity theft.

6.3 Step Three – Notification

6.3.1 If the Head determines that the Privacy Breach could reasonably be expected to result in Significant Harm to individuals, then the Head 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 Head 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.

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

6.3.3 Determinations about notification of a Privacy Breach shall be made without delay following the 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.

6.4 Step 4 - Prevention

6.4.1 The Privacy Officer in consultation with the Head, shall complete an investigation into the causes of each Breach Incident reported under these Guidelines, and shall implement measures to prevent recurrences of similar incidents.

6.4.2 The Privacy Officer may suggest any necessary changes to operating procedures to prevent recurrence of similar Privacy Breach incidents in the future as instructed by the Head.

7. Inquiries

7.1 Questions or comments about these Guidelines may be addressed to the Privacy Officer at privacy@sd38.bc.ca. The District will respond to all inquiries in writing.

Related Acts and Regulations:

School Act

British Columbia Freedom of Information and Protection of Privacy Act (FIPPA)

Supporting References, Policies, Procedures and Forms

Policy 311 Freedom of Information and Protection of Privacy

Policy 311-R Privacy Management

Adopted: 21 June 2023