PROCEDURE #5700.3
PRIVACY BREACH MANAGEMENT

1. PURPOSE

1.1 The Board of Education of School District No. 36 (Surrey) (the "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.

1.2 The purpose of this procedure is to set out the district 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") of BC.

1.3 All district staff are expected to be aware of and follow this procedure in the event of a Privacy Breach.

2. DEFINITIONS

2.1 "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 staff member of the district. Personal information does not include business contact information, such as email address and telephone number, that would allow a person to be contacted at work.

2.2 "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.

2.3 "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.

2.4 "staff" means the employees, contractors, and volunteers of the district.

3. DISTRICT RESPONSIBILITIES

3.1. The Superintendent is the "Head" of the district for all purposes under the *Freedom of Information and Protection of Privacy Act* (FIPPA) of BC including Privacy Breaches.

3.2. The Superintendent has delegated to the Privacy Officer responsibility for the management of critical incidents and Privacy Breaches.

3.3. It is the responsibility of the Privacy Officer to notify and consult with the Superintendent regarding the management of all Privacy Breaches.

4. RESPONSIBILITIES OF STAFF

4.1. Staff have a legal responsibility under FIPPA to report without delay to the Privacy Officer all actual, suspected or expected Privacy Breaches of which they have become aware.

4.2. 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.

4.3. All staff must provide their full cooperation in any investigation or response to a Privacy Breach incident and comply with this procedure for responding to Privacy Breach incidents.

4.4. Any district staff member who knowingly refuses or neglects to report a Privacy Breach in accordance with this procedure may be subject to discipline up to and including dismissal.

5. PRIVACY BREACH RESPONSE

Upon discovering or learning of a Privacy Breach, all staff shall:

5.1. Step 1 – Report and Contain

a) Upon discovering or learning of a Privacy Breach, all staff shall immediately report the Privacy Breach to the Privacy Officer.

b) Take immediately available actions to stop or contain the Privacy Breach, such as by:

i. Isolating or suspending the activity that led to the Privacy Breach.

ii. Taking steps to recover Personal Information, Records or affected equipment.

c) Upon being notified of a Privacy Breach the Privacy Officer, in consultation with the Superintendent, 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.

5.2. Step 2 – Assessment and Containment

a) The Privacy Officer, in consultation with the Superintendent, shall take steps to contain the Privacy Breach by making the following assessments:

i. The cause of the Privacy Breach.

ii. If additional steps are required to contain the Privacy Breach and, if so, to implement such steps as necessary.

iii. 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.

iv. Determine or estimate the number of affected individuals and compile a list of such individuals, if possible.

v. Make preliminary assessments of the types of harm that may flow from the Privacy Breach.

b) The Privacy Officer, in consultation with the Superintendent, 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:

i. Bodily Harm.
ii. Humiliation.
iii. Damage to reputation or relationships.
iv. Loss of employment, business, or professional opportunities.
v. Financial Loss.
vi. Negative impact on credit record.
vii. Damage to , or loss of, property.
viii. The sensitivity of the Personal Information involved in the Privacy Breach.
ix. The risk of identity theft.

5.3. Step 3 – Notification

a) If the Superintendent determines that the Privacy Breach could reasonably be expected to result in Significant Harm to individuals, then the Privacy Officer shall plan to:

i. Report the Privacy Breach to the Office of the Information and Privacy Commissioner.

ii. Provide notice of the Privacy Breach to affected individuals unless the Superintendent 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.

b) If the Superintendent 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 affected individuals if the Superintendent determines that notification would be in the public interest or if a failure to notify would be inconsistent with district obligations or undermine public confidence in the district

c) 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.

5.4. Step 4 – Prevention

a) The Privacy Officer, in consultation with the Superintendent, shall complete an investigation into the causes of each Breach Incident reported under this procedure and make recommendations to prevent recurrences of similar incidents in the future.

b) District staff will make any necessary changes to operating procedures to prevent recurrences of similar Privacy Breach incidents in the future as instructed by the Superintendent or their delegate.

6. REFERENCES AND RELATED DOCUMENTS

6.1 Policy 5700
6.2 Procedure 5700.1

7. AUTHORITY AND RESPONSIBILITY

7.1 Superintendent of Schools
7.2 Privacy Officer - Questions or comments about this procedure may be addressed to the Privacy Officer at privacy@surreyschools.ca.

8. HISTORY

Approved: 2023-09-13