POLICY 611: PRIVACY – CRITICAL INCIDENT AND PRIVACY BREACH ADMINISTRATIVE PROCEDURES

1. PURPOSE

The Board of Education ("School 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 this Procedure is to set out the School District's process for responding to significant privacy breaches and to complying with its notice and other obligations under the British Columbia *Freedom of Information and Protection* of *Privacy Act* ("FIPPA").

2. SCOPE & RESPONSIBILITY

All Staff of the School District are expected to be aware of and follow this Procedure in the event of a privacy breach. This Procedure applies to all employees, independent contractors and volunteers of the School District ("Staff").

3. DEFINITIONS

a. **"FIPPA"** means the British Columbia *Freedom of Information and Protection of Privacy Act* and regulations thereto.

b. **"Head"** means the Secretary Treasurer of the School District or any person to whom the Secretary Treasurer has delegated their powers under this Procedure.

c. **"Personal Information"** means any recorded information about an identifiable individual that is within the control of the School District and includes information about any student or any Staff of the School District. Examples include:

- Name, address, phone number, personal email address
- Image (picture or video)
- Date of birth, grade, school
- Race, national/ethnic origin
- Religious or political beliefs or associations
- Age, sex, sexual orientation, marital status
- Fingerprints, blood type, DNA information, biometrics
- Health care, educational, financial, criminal, employment information

Personal Information does not include business contact information, such as business address, email address and telephone number that would allow a person to be contacted at work.

d. "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.

e. **"Privacy Officer"** means the Secretary Treasurer of the School District or any person to whom the Secretary Treasurer has delegated their powers under this Procedure.

f. "Records" include any paper or electronic media used to store or record information, including all paper and electronic records, books, documents, drawings, maps, letters, photographs, audio or visual recordings, computer files, email and correspondence, but does not include a computer program or other mechanism that produces records.

g. "Staff" means all persons employed or engaged by the School District to carry out its operations, and includes independent contractors and volunteers.

4. RESPONSIBILITY OF THE HEAD

The Secretary Treasurer has been designated by the Board of Education as the "Head" of the Board for the purposes of FIPPA. As Privacy Officer, the Secretary Treasurer is responsible for the administration of this Procedure and may delegate any of their powers under this Procedure or FIPPA to other School District Staff by written delegation.

5. 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 Procedure. All Staff have a legal responsibility under FIPPA 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 Procedure for responding to Privacy Breach incidents.

d. Any Staff 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.

6. PRIVACY BREACH RESPONSE

a. Step One – Report and Contain

i. Upon discovering 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 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 to support the School District's incident response.

ii. Upon being notified 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 first 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, 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.

ii. The Privacy Officer 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.

c. Step Three – Notification

i. If the Privacy Officer determines 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 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 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. 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.

d. Step 4 - Prevention

The Privacy Officer shall complete an investigation into the causes of each Privacy Breach Incident reported under this Procedure, and shall implement measures to prevent recurrences of similar incidents.

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

7. Contact Information

Questions or comments about this Procedure may be addressed to the Privacy Officer at secretarytreasurer@sd44.ca.

8. RELATED ACTS AND REGULATION

British Columbia School Act
*Bri*tish Columbia Freedom of Information and Protection of Privacy Act (FIPPA)

9. SUPPORTING REFERENCES, POLICIES, PROCEDURES AND FORMS

Policy 611: Privacy
Policy 611: Privacy - Administrative Procedures: Personal Information Management Program
Policy 611: Privacy - Administrative Procedures: Privacy Impact Assessments
Policy 611: Privacy - Administrative Procedures: Social Media
Office of the Information and Privacy Commissioner of British Columbia