ADMINISTRATIVE PROCEDURE 257 SECURITY INCIDENT AND PRIVACY BREACH

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

Definitions

- Personal Information – any recorded information about an identifiable individual that is within the control of the district and includes information about any student or staff. Personal information does not include an individual's business contact information.
- Privacy Breach – 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.
- Privacy Officer – the Secretary Treasurer or designate.
- Records – any paper of electronic media used to store or record information, including all paper and electronic records, books, documents, photographs, audio or visual recordings, computer files, email and correspondence. Does not include a computer program or other mechanism that produces records.
- Staff – the employees, contractors, and volunteers of the School District.

Responsibility of the Privacy Officer

The Privacy Officer is responsible for ensuring compliance with this procedure.

Responsibilities of Staff

All staff must, without delay, report all actual, suspected or expected privacy breach incidents of which they become aware in accordance with this procedure. 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.

All staff must fully cooperate in any investigation or response to a privacy breach incident. Any staff who knowingly refuses or neglects to report a privacy breach in accordance with this procedure may be subject to discipline.

Privacy Breach Response

1. Report and Contain

Upon discovering or learning of a privacy breach, all staff shall:

- Immediately report the breach to the Privacy Officer.
- Take any immediately available actions to stop or contain the breach, such as by:
  - isolating or suspending the activity that led to the breach
  - taking steps to recover personal information, records or affected equipment.
- Preserve any information or evidence related to the breach in order to support the district's incident response.

The Privacy Officer shall then implement all available measures to stop or contain the breach. Containing the breach shall be the first priority of the response, and all staff are expected to provide their full cooperation with such initiatives.

2. Assessment and Containment

The Privacy Officer shall take steps to contain the privacy breach by:

- Identifying the type and sensitivity of the personal information involved.
- Assessing the cause.
- Determining if additional steps are required to contain the breach.
- Identifying the individuals affected, or whose personal information may have been involved in the breach.
- Determining or estimating, if possible, the number of affected individuals and compiling a list of such individuals.
- making preliminary assessments of the types of harm that may flow from the breach.

The Privacy Officer, without delay, will assess whether the privacy breach could reasonably be expected to result in significant harm to individuals. This determination shall be made with consideration of the following categories of harm or potential harm:

- bodily harm
- humiliation
- damage to reputation or relationships
- loss of employment, business, or professional opportunities
- financial loss
- negative impact on credit record
- damage to, or loss of, property

- the sensitivity of the personal information involved
- the risk of identity theft

3. Notification

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:

- report the privacy breach to the Office of the Information and Privacy Commissioner.
- 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, physical or mental health, or threaten another individual's safety or physical or mental health.

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 affected individual if it is determined 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.

Notifications of a privacy breach shall be made 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.

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.

Contact Information

Questions or comments about this procedure may be addressed to the Privacy Officer at privacy@sd33.bc.ca.