



PRIVACY BREACH

Background

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.

The purpose of this Procedure 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).

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, contractors, and volunteers of the School District ("**Staff**").

Responsibility of the Privacy Officer

The administration of this Procedure is the responsibility of the Secretary Treasurer of the School District,

mechanical or other means, but does not include a computer program or other mechanism that produces records;

- e. **“Staff”** means the employees, contractors, and volunteers of the School District.

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 Personnel 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 member of 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.

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;



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 they may still proceed with notification to