ADMINISTRATIVE PROCEDURE

PRIVACY BREACH MANAGEMENT PROCEDURE

.....

REFERENCE POLICY TITLE: 25 BURNABY SCHOOL DISTRICT PRIVACY POLICY

PURPOSE

1.

Scope and Responsibility

All staff of the 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 District Staff.

Responsibility of the Secretary-Treasurer

The administration of this Procedure is the responsibility of the Secretary -Treasurer for the purposes under FIPPA. The Secretary -Treasurer may delegate any of their powers under this Procedure or FIPPA to other District personnel by written delegation.

Responsibilities of Staff

1. 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 Secretary -Treasurer.

2. Privacy breach reports may also be made to the privacy officer, who has delegated responsibility for receiving and responding to such reports.

3. 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. 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.

5. 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

Step One – Report and Contain

1. Upon discovering or learning of a privacy breach, all staff shall:
    a. Immediately report the privacy breach to the Secretary -Treasurer or to the privacy officer.
    b. Take any 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; and
        ii. Taking steps to recover personal Information, records or affected equipment.
    c. Preserve any information or evidence related to the privacy breach in order to support the District's incident respo nse.

2. Upon being notified of a privacy breach the Secretary -Treasurer or the privacy officer in consultation with the Secretary -Treasurer, shall implement all available measures to stop

or contain the privacy breach. Containing the privacy breach shall b e the first priority of the privacy breach response, and all staff are expected to provide their full cooperation with such initiatives.

Step Two – Assessment and Containment

1. The privacy officer shall take steps to, in consultation with the Secretary -Treasurer, contain the privacy breach by making the following assessments:
    a. The cause of the privacy breach;
    b. If additional steps are required to contain the privacy breach, and, if so, to implement such steps as necessary;
    c. 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;
    d. Identify the individuals affected by the privacy breach, o r whose personal Information may have been involved in the privacy breach;
    e. Determine or estimate the number of affected individuals and compile a list of such individuals, if possible; and
    f. Make preliminary assessments of the types of harm that may flow fro m the privacy breach.

2. The Secretary -Treasurer, in consultation with the privacy officer, shall be responsible for, without delay, assessing 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:
    a. Bodily harm;
    b. Humiliation;
    c. Damage to reputation or relationships;
    d. Loss of employment, business or professional opportunities;
    e. Financial loss ;
    f. Negative impact on credit record, ;
    g. Damage to, or loss of, property ;
    h. The sensitivity of the personal Information involved in the privacy breach; and
    i. The risk of identity theft.

Step Three – Notification

1. If the Secretary -Treasurer determines that the privacy breach could reasonably be expected to result in Significant Harm to individuals, then the Secretary -Treasurer shall make arrangements to:
    a. Report the privacy breach to the Office of the Information and Privacy Commissioner; and
    b. Provide notice of the privacy breach to affected individuals, unless the Secretary - Treasurer 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.

2.