PRIVACY BREACH

Background

The District is required to have a process for responding to a privacy breach in accordance with the *British Columbia Freedom of Information and Protection of Privacy Act.*

All District employees must immediately report any actual or suspected privacy breach incidents to their Supervisor/Manager in accordance with this Appendix.

Definition

A privacy breach occurs in any circumstances in which there is any unauthorized collection, use, disclosure, disposal or access to personal information, and includes the loss or theft of materials or devices containing personal information. Such activities will be considered to be "unauthorized" if they are contrary to the provisions of the *Freedom of Information and Protection of Privacy Act.* A privacy breach arises in any circumstances in which there is a reasonable basis for believing a breach is or may be occurring.

A privacy breach can be accidental or deliberate and includes the theft, loss, alteration or destruction of personal information. "Personal Information" means information about an identifiable individual.

Procedures

1. Roles and Responsibilities
    1.1. All District employees are responsible for complying with this Appendix and for performing their duties in a manner that ensures personal information to which they have access in the course of their duties is protected at all times from unauthorized access, use and disclosure (either accidental or intentional).
    1.2. The Coordinator is responsible for all investigation and subsequent documentation in relation to any reported privacy breach incidents. All reported incidents will be documented along with any action taken. The Coordinator will assess whether the reported incident requires immediate action to prevent any recurrence of a similar incident.

2. Response Process
    2.1. Responsibilities of Employee

    Upon becoming aware of an actual or a suspected privacy breach, all District employees shall:

    2.1.1. Immediately report the suspected or actual breach to their supervisor/manager/administrator;

    2.1.2. Take action, where possible, to contain the breach and limit its impact by:

2.1.2.1. Isolating or suspending the activity that led to the privacy breach;

2.1.2.2. Taking immediate steps to recover the personal information, records, or equipment where possible;

2.1.2.3. Determining if any copies have been made of the personal information at risk and recovering where possible.

2.2. Responsibilities of Supervisor/Manager/Administrator

Upon being notified of an actual or a suspected privacy breach, the supervisor/manager/administrator shall:

2.2.1. Immediately notify the Coordinator of the breach and work with the Coordinator to carry out a preliminary assessment of the extent and impact of the privacy breach, including:

2.2.1.1. Assessing whether additional steps are required to contain the breach, implementing as necessary;

2.2.1.2. Identifying the type and sensitivity of personal information breached and any steps that have been taken to minimize the harm from the breach;

2.2.1.3. Identifying who is affected by the breach;

2.2.1.4. Estimating the number of individuals affected by the breach;

2.2.1.5. Identifying the cause of the breach; and

2.2.1.6. Identifying foreseeable harm from the breach.

2.3. Responsibility of Coordinator

The Coordinator shall be responsible for the detailed investigation of incidents of actual or suspected privacy breaches. The Coordinator's investigation shall include but not be limited to:

2.3.1. Assessing all information reported by the supervisor/manager/ administrator and obtaining further clarification of events and findings if required;

2.3.2. Taking any further steps required to minimize or reduce the harm:

2.3.3. Assessing foreseeable harm from the breach including but not limited to:

2.3.3.1. Risk of harm to the individual(s);

2.3.3.2. Loss of public trust in District;

2.3.3.3. Risk to public safety;

2.3.3.4. Financial exposure;

2.4. District Actions and Notifications

The determination of whether to notify individuals, public bodies, organizations affected by the privacy breach, or the Privacy Commissioner, will be made by the Coordinator and the appropriate Director of Instruction. The considerations shall include but are not limited to:

2.4.1. Necessity to avoid or mitigate harm to the affected individual, public body or organization;

2.4.2. Legislative requirements;

2.4.3. Contractual obligations;

2.4.4. Potential risk of identity theft or fraud due to the breach of any personal identification information;

2.4.5. Any risk of physical harm due to the privacy breach such as stalking or harassment;

2.4.6. A risk of damage to reputation, hurt or humiliation such as when the privacy breach includes the release of medical or disciplinary information;

2.4.7. A risk of loss of business or employment opportunities should the privacy breach results in damage to the reputation of an individual;

2.4.8. A risk of the loss of confidence in the District, or any related public body or organization, and good District relations.

3. If notification of individuals is determined to be necessary, the notification is to occur by the Direct Supervisor/Manager/Administrator as soon as possible following the breach.

   3.1. If a law enforcement agency has been informed, and is conducting a criminal investigation, consultation and cooperation is to occur in order to facilitate the investigation.

4. Where feasible, affected individuals will be notified directly, by the Direct Supervisor/Manager/Administrator by phone, email, letter or in person, depending on the practicalities. Indirect notification using general, non-personal information will usually occur only when direct notification could cause further harm, is prohibitive in cost, or contact information is unavailable. In some circumstances, using multiple methods of notification may be considered.

Reference: Sections 22, 65, 85 School Act
Freedom of Information and Protection of Privacy Act
Freedom of Information and Protection of Privacy Regulation

Adopted: January 9, 2013
Revised: September 24, 2018