PRIVACY MANAGEMENT PROGRAM

Background

As a public body subject to the *Freedom of Information and Protection of Privacy Act* (hereafter referred to as "the Act"), the Board of Education of School District #39 (hereafter referred to as "the District") acknowledges its requirement to develop a Privacy Management Program in accordance with the directions of the Minister responsible for the Act. A Privacy Management Program is developed by a public body to enable systematic and collaborative privacy protection throughout the District.

Definitions

A Privacy Impact Assessment (PIA) is an in-depth, multi-stage review of any new or significantly revised Initiative, project, activity, or program to ensure that is it compliant with the provisions of FIPPA, and that identified risks to individual privacy can be mitigated with safeguards and processes that are proportional to those risks.

An Initiative means any enactment, system, project, or activity of the District (e.g., the acquisition and use of a new online software or application).

A Supplemental Review means an enhanced process for reviewing the privacy and data security measures in place to protect sensitive Personal Information in the case of Initiatives involving the storage of Personal Information outside of Canada.

An Information Sharing Agreement (ISA) documents the terms and conditions of a regular and systematic exchange of Personal Information between the District and other public sector organization or external agency in compliance with the Act and other applicable legislation.

A Privacy Breach occurs when there has been and/or the potential exists of 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 are considered "unauthorized" if they are contrary to the provisions of the 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.

The Privacy Officer refers to Staff responsible for all investigation and subsequent documentation in relation to any reported privacy breach incidents. All reported incidents, along with any action taken, will be documented. The Privacy Officer will assess whether the reported incident requires immediate action and/or reporting to the impacted individual(s) and the Office of the Information and Privacy Commissioner (hereafter referred to as the "OIPC") and offer recommendations to prevent any recurrence of a similar incident.

Procedures

1. Roles and Responsibilities

    1.1. School District Staff are responsible for:

        1.1.1. Making reasonable efforts to familiarize themselves with this procedure and the requirements of the Act, including participating in privacy training initiatives offered by the District;

        1.1.2. Following responsible information management practices to ensure that the District collects, uses, and discloses personal information in compliance with the Act and other applicable laws;

        1.1.3. Taking reasonable measures to protect Personal Information against unauthorized collection, use, and disclosure, including sharing Personal Information on a need-to-know basis;

        1.1.4. Cooperating with District procedures to facilitate the appropriate release of records within its custody or control in response to access requests received from members of the community under the Act;

        1.1.5. Completing a Privacy Impact Assessment (hereafter referred to as “PIA”) when they are responsible for implementing a new or significantly revised Initiative;

        1.1.6. Ensuring that an Information Sharing Agreement (hereafter referred to as “ISA”) is in place prior to routinely and systematically sharing personal information with another public body or external agency and, when applicable, working with the Privacy Officer and other relevant parties to develop an ISA in the absence of one.

        1.1.7. Reporting Privacy Breaches in accordance with the procedure set out in this procedure.

2. Privacy Impact Assessments and Information-Sharing Agreement

    2.1. Staff responsible for overseeing a new or significantly revised Initiative that collect personal information are required to complete all stages of a PIA before entering any binding commitment to participate in said Initiative.

    2.2. When applicable, Staff are expected to collaborate in the completion of PIAs to offer cross-departmental expertise for identifying, evaluating, and mitigating privacy risks in accordance with the Act.

    2.3. Staff will not engage in any new or significantly revised initiative that involves the storage of Personal Information outside of Canada until the Privacy Officer has determined whether a Supplemental Review is required and, if so, completed a Supplemental Review in accordance with the Act.

    2.4. Upon completion of the PIA, Staff responsible for overseeing a new or significantly revised Initiative must familiarize themselves with it and ensure that the Initiative is carried out in accordance with the recommendations in the PIA.

2.5. Staff considering sharing Personal Information with another public body regularly and systematically must ensure that there is an ISA in place, and that the Personal Information in question can be shared in accordance with that ISA.

2.6. In cases where there is no ISA in place, Staff are required to develop an ISA — with the support of the Privacy Officer — prior to sharing any Personal Information with another public body or external agency.

3. Privacy Breaches

3.1. District Staff are expected to be aware of and follow this procedure in the event of a Privacy Breach.

3.2. Responsibilities of Staff:

Upon becoming aware of an actual or a suspected Privacy Breach, all Staff shall:

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

3.2.2. Act, where possible, to contain the breach and limit its impact by:

3.2.2.1. Isolating or suspending the activity that led to the Privacy Breach;

3.2.2.2. Taking immediate steps to recover the Personal Information, records, or equipment where possible;

3.2.2.3. Determining if any copies have been made of the Personal Information at risk and recovering these copies when possible.

3.3. Responsibilities of Supervisors/ Managers/ Administrators:

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

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

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

3.3.1.2. Identifying the type and sensitivity of Personal Information breached and any steps taken to minimize the harm from the breach;

3.3.1.3. Estimating the number of individuals, and identifying the individuals affected by the breach;

3.3.1.4. Determining the cause of the breach; and

3.3.1.5. Identifying the foreseeable harm that could stem from the breach.

3.4. Responsibilities of the Privacy Officer:

The Privacy Officer shall be responsible for the detailed investigation of incidents of actual or suspected privacy breaches. The Privacy Officer's investigation shall include:

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

3.4.2. Taking any further steps required to minimize or reduce the harm;

3.4.3. Assessing foreseeable harm from the breach.

3.5. District Action and Notification

3.5.1. In the event of a Privacy Breach that could reasonably be expected to result in significant harm to the impacted individual(s), both the impacted individual(s) and the OIPC will be notified in accordance with the Act.

3.5.2. The Privacy Advisor will assess whether a Privacy Breach could reasonably be expected to result in significant harm by considering outcomes that could arise from the breach, including but not limited to:

3.5.2.1. Identity theft;

3.5.2.2. Bodily harm;

3.5.2.3. Humiliation and/or damage to the reputation of relationships of the impacted individual(s);

3.5.2.4. Loss of employment, business, or professional opportunities;

3.5.2.5. Financial loss(es) and/or negative impact on credit record;

3.5.2.6. Damage to or loss of property;

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

3.5.3. When notification of the individual(s) is determined to be necessary, the notification is to come from the relevant supervisor/ manager/ administrator as soon as possible following the breach.

3.5.4. When notification of the individual(s) is determined to be necessary, the Privacy Officer will notify the OIPC in accordance with the Act.

3.5.5. If a law enforcement agency has been informed of the breach, and is conducting a criminal investigation, consultation and cooperation is to occur to facilitate the investigation.

3.5.6. Whenever feasible, affected individuals will be notified directly, by the 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.

4. Privacy Awareness and Education Activities

4.1. The Privacy Department will offer routine privacy training and workshops pertaining to privacy and access to information. This will help Staff identify what is considered personal information, review their obligations under the Act, and highlight the Privacy Breach procedure.

5. Informing Service Providers of Privacy Obligations

    5.1. Staff must inform service providers that handle personal information of their privacy obligations under the Act.

    5.2. Prior to engaging a service provider that collects Personal Information as part of their services, Staff are responsible for completing all required stages of a PIA (with the support of the Privacy Officer if needed) before entering into any binding agreement.

6. Monitoring and Updating

    6.1. The Privacy Officer will review the Privacy Management Program regularly and ensure it remains relevant to District's activities and personal information holdings.

    6.2. The Privacy Officer and relevant department will maintain an updated Personal Information Bank for the District, which will be reviewed and updated annually. Staff are expected to support this annual review and provide any relevant information to the Privacy Officer as requested.

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, April 19, 2023