ADMINISTRATIVE REGULATION 1161.4

CRITICAL INCIDENT AND PRIVACY BREACH

PURPOSE

The Board of Education of School District No. 61 (Greater Victoria School District) ("School 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 Administrative Regulation is to set out the School 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).

If a school district experiences a breach incident, it is important that it acts quickly to assess the nature and extent of any harm that might arise from disclosure. Understanding how affected individuals may be impacted by a privacy breach places the district in the best position to determine how to mitigate any negative consequences flowing from the breach.

"Harm" must be assessed with a view to all of the surrounding circumstances, including the nature and sensitivity of the personal information, the nature of the breach (e.g., malicious actor or inadvertent breach), and the likelihood of the information being used for unauthorized purposes.

Public bodies have a mandatory obligation to notify affected individuals and to report privacy breaches without unreasonable delay in any circumstances where the breach incident gives rise to a risk of "significant harm". Significant harm includes financial loss, physical harm and identity theft, but it also includes other types of harm like physical harm, humiliation, damage to reputation, and loss of employment. The phrase "significant harm" is defined in section 36.3 of the Act as follows:

WHAT IS A 'PRIVACY BREACH'

A "privacy breach" refers to the theft or loss, or the collection, use or disclosure of personal information that is not authorized under FIPPA. If a privacy breach occurs in relation to personal information within the control of the school district, then the district is responsible for responding to the breach and mitigating any harmful effects arising from the incident.

The term "privacy breach" is defined in section 36.3 of FIPPA, Privacy breaches should be responded to with urgency to ensure impacted individuals are able to take immediate action to protect themselves from potential harm.
How can staff report a Privacy Breach or Critical Incident?

There are multiple ways for staff to report a privacy breach or critical incident

1. Email the Privacy Officers at privacy@sd61.bc.ca
2. Submit a Help Desk ticket to the IT for Learning Department explaining the concern. Click the orange button on the Tech For Learning website to submit a ticket or email helpdesk@sd61.bc.ca
3. Phone the IT For Learning Help Desk at (250) 475-4188 (working hours apply)

Scope & Responsibility

All Staff of the School District are expected to be aware of and follow this Regulation in the event of a privacy breach.

Definitions

1. “Head” means the Superintendent, and includes any person to whom the Head has delegated their powers by written instrument.
2. “Personal Information” means any recorded information about an identifiable individual that is within the control of the School District, and includes information about any student or any Staff member of the School District. Personal Information does not include business contact information, such as email address and telephone number, that would allow a person to be contacted at work. Personal information may also be identifiable through the 'mosaic effect'. The mosaic effect is a concept that illustrates how elements of information may be non-identifiable on their own but when combined could become personally identifiable. For example, a male in his 20s who lives in Vancouver and drives a black Honda would not be identifiable. However, a male in his 60s who lives in Smithers and drives a yellow Lamborghini would be identifiable.
3. “Privacy Breach” means 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.
4. “Significant Harm” means significant harm to the individual, including identity theft or significant
    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 a credit record, or
    g. damage to, or loss of, property
5. “Privacy Officers” means the positions designated by the Head as Privacy Officers for the School District, which are the Secretary Treasurer and the Director of IT for Learning;
6. “Records” means books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or other mechanism that produces records;
7. “Staff” or “Employees” refers to all employees of the School District who are required to comply with FIPPA and all relevant School District policies and regulations;
8. “Contractors” refers to a service provider retained under a contract to perform services for the School District. Contractors are required to comply with FIPPA and all relevant School District policies and regulations;
9. “Volunteers” refers to community members carrying out volunteer activities on behalf of the School District. Volunteers are required to comply with FIPPA and all relevant School District policies and regulations.

RESPONSIBILITIES OF THE HEAD

The implementation of this Administrative Regulation is the responsibility of the Superintendent, who is the "Head" of the School District, including for all purposes under FIPPA. The Head is also responsible for ensuring there is a process for completing and documenting Privacy Impact Assessments and, as required, Information Sharing Agreements. The Head may delegate any of their powers under this Regulation or FIPPA to other School District Employees by written delegation.

RESPONSIBILITIES OF ALL EMPLOYEES

1. All Staff must without delay report all actual, suspected or expected Privacy Breach incidents of which they become aware in accordance with this Regulation. All Staff have a legal responsibility under FIPPA to report Privacy Breaches to the Head.

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 Regulation 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 Regulation may be subject to discipline, up to and including dismissal.

PRIVACY BREACH RESPONSE

1. **Step One – Report and Contain**
    a. Upon discovering or learning of a Privacy Breach, all Staff shall:
        i. Immediately report the Privacy Breach to the Head or to the Privacy Officers.

        ii. Take any immediately available actions to stop or contain the Privacy Breach, such as by:

            1. isolating or suspending the activity that led to the Privacy Breach; and

            2. taking steps to recover Personal Information, Records or affected equipment.

            3. preserve any information or evidence related to the Privacy Breach in order to support the School District's incident response.

    b. Upon being notified of a Privacy Breach the Head or the Privacy Officers in consultation with the Head, 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.

2. Step Two – Assessment and Containment

a. The Privacy Officers shall take steps to, in consultation with the Head, contain the Privacy Breach by making the following assessments:

   i. the cause of the Privacy Breach;

   ii. if additional steps are required to contain the Privacy Breach, and, if so, to implement such steps as necessary;

   iii. 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;

   iv. identify the individuals affected by the Privacy Breach, or whose Personal Information may have been involved in the Privacy Breach;

   v. determine or estimate the number of affected individuals and compile a list of such individuals, if possible; and

   vi. make preliminary assessments of the types of harm that may flow from the Privacy Breach.

b. The Head, in consultation with the Privacy Officers, 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:

   i. bodily harm;
   ii. humiliation;
   iii. damage to reputation or relationships;
   iv. of employment, business or professional opportunities;
   v. financial loss;
   vi. negative impact on credit record,
   vii. damage to, or loss of, property,
   viii. the sensitivity of the Personal Information involved in the Privacy Breach; and
   ix. the risk of identity theft.

3. Step Three – Notification

a. If the Head determines that the Privacy Breach could reasonably be expected to result in Significant Harm to individuals, then the Head shall make arrangements to:
   i. report the Privacy Breach to the Office of the Information and Privacy Commissioner; and
   ii. provide notice of the Privacy Breach to affected individuals, unless the Head 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.

b. If the Head determines that the Privacy Breach does not give rise to a reasonable expectation of Significant Harm, then the Head may still proceed with notification to affected individual if the Head determines that notification would be in the public interest or if a failure to notify would be inconsistent with the School District's obligations or undermine public confidence in the School District.

c. Determinations about notification of a Privacy Breach shall be made without delay following the Privacy Breach, and notification shall be undertaken 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. **Step 4 – Prevention**

a. The Head, or the Privacy Officers in consultation with the Head, shall complete an investigation into the causes of each Breach Incident reported under this Administrative Regulation, and shall implement measures to prevent recurrences of similar incidents. These measures shall be incorporated into the regular Privacy Management Program review.

CONTACT INFORMATION

Questions or comments about this Policy may be addressed to the Privacy Officers via email: privacy@sd61.bc.ca

REVIEW

This Administrative Regulation relates to newly amended legislation for public bodies and will therefore be reviewed annually until further notice.

RELATED ACTS AND REGULATION

School Act and Regulations
Freedom of Information and Protection of Privacy Act (FIPPA) and Regulations

SUPPORTING REFERENCES, POLICIES, REGULATIONS AND FORMS

Policy 1161 Freedom of Information and Protection of Privacy
Administrative Regulation 1161.1 Fees for Access to Information
Administrative Regulation 1161.2 Privacy Management Program
Administrative Regulation 1161.3 Privacy Impact Assessments

Adopted: November 27, 2023
Revised: