AP I1 Responding to Breaches of Privacy

Legislative References: *Freedom of Information and Protection of Privacy Act (FOIPPA)* section 36.2 & 36.3
Policy Reference: None
Collective Agreement References: None
Date: April 25, 2023

Purpose

Section 36.3 of the *Freedom of Information* and *Protection of Privacy Act* requires the head of a public body to notify an affected individual if a privacy breach could reasonably be expected to result in significant harm to the individual, including identity theft or other significant harms as described in section 36.3. Section 36.3 also requires the head of a public body to notify the Information and Privacy Commissioner (the Commissioner) when the significant harm threshold is met.

As a public body, School District No. 64 (Gulf Islands) 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 Practice is to set out the District's process for responding to significant privacy breaches and to comply with its notice and other obligations under the *Freedom of Information and Protection* of *Privacy Act* (FOIPPA).

Scope & Responsibility

This practice applies to all employees, contractors and volunteers of the District who hereinafter will be referred to as "Staff". All Staff of the District are expected to be aware of and follow this Administrative Practice in the event of a privacy breach.

Responsibility of the Head

The administration of this Administrative Practice is the responsibility of the Secretary Treasurer of the District, who is the "head" for all purposes under FOIPPA (the "Head"). The Head may delegate any of their powers under this Practice or FOIPPA to other District personnel by written delegation.

Definitions

"**head**" means the Secretary Treasurer and includes any person to whom the Head has delegated their powers by written instrument.
"**personal information**" means any recorded information about an identifiable individual that is within the control of the District, and includes information about any student or any Staff. 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.
"**privacy breach**" means the theft or loss of or the collection, use or disclosure of Personal Information not authorized by FOIPPA, 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.
"**privacy officer**" means the Director of Corporate Services or other person designated by the Head as Privacy Officer for the District;
"**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;
"**staff**" means the employees, contractors and volunteers of the District.

Responsibilities of Staff

a. All Staff have a legal responsibility under FOIPPA to report Privacy Breaches to the Head.
b. All Staff must without delay report all actual, suspected or expected Privacy Breach incidents of which they become aware in accordance with this Practice.
c. Privacy Breach reports may also be made to the Privacy Officer, who has delegated responsibility for receiving and responding to such reports.
d. 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.
e. All Staff must provide their full cooperation in any investigation or response to a Privacy Breach incident and comply with this Practice for responding to Privacy Breach incidents.
f. Any member of Staff who knowingly refuses or neglects to report a Privacy Breach in accordance with this Practice may be subject to discipline, up to and including dismissal.

All questions and concerns regarding privacy can be reported to the District Privacy Office at: sd64privacy@sd64.org

Privacy Breach Response

1. Step One – Report and Contain

1.1. Upon discovering or learning of a Privacy Breach, all Staff shall:
- 1.1.1. Immediately report the Privacy Breach to the Head.
- 1.1.2. Take any immediately available actions to stop or contain the Privacy Breach, such as by:
  - 1.1.2.1. isolating or suspending the activity that led to the Privacy Breach; and
  - 1.1.2.2. making every effort to recover the confidential or personal information, records or affected equipment to lessen the impact on the individuals involved.
- 1.1.3. Preserve any information or evidence related to the Privacy Breach to support the District's incident response.

1.2. Upon being notified of a Privacy Breach, 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 measures.

2. Step Two – Assessment and Containment

2.1. The Privacy Officer shall take steps to, in consultation with the Head, shall assess the Privacy Breach by making the following assessments:
- 2.1.1. the cause of the Privacy Breach;
- 2.1.2. if additional steps are required to contain the Privacy Breach, and, if so, to implement such steps as necessary;
- 2.1.3. 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;
- 2.1.4. identify the individuals affected by the Privacy Breach, or whose Personal Information may have been involved in the Privacy Breach;
- 2.1.5. determine or estimate the number of affected individuals and compile a list of such individuals, if possible; and
- 2.1.6. make preliminary assessments of the types of harm that may flow from the Privacy Breach.

2.2. The Head shall be responsible to, without delay, assess whether the Privacy Breach could reasonably be expected to result in significant harm to individuals.

2.3. The determination of whether a privacy breach could result in significant harm depends on a number of factors. Several of the considerations below can help assess the likelihood of harm. They also depend on and inform each other.

2.3.1. The sensitivity of the information involved

2.3.1.1. The sensitivity of personal information often but not always depends on context, the relationship between the individuals, and/or the individuals affected. Determining the sensitivity and being mindful of the context can help inform the potential for harm. Breaches with personal information that is highly sensitive are more likely to result in significant harm.

2.3.2. The amount of personal information involved

2.3.2.1. The number of data elements involved in the breach may increase sensitivity if each element contributes to a complete picture of an individual. The more data elements involved in the breach, the greater the overall risk of misuse of any or all of the data elements. For example, first and last name may not be considered sensitive on their own but when paired with birth date, home address, and financial information, the sensitivity of a name may increase because more is known about the individual. This could result in a risk of significant harm, including identity theft.

2.3.3. The individuals affected

2.3.3.1. Different groups of people may be affected by breaches in different ways. Understanding the type of individuals affected may inform how to notify. For example, if a child's information has been breached, the District may need to consider who to notify consistent with relevant legislation.

2.3.3.2. If there are a large number of people that received the breached personal information or if the recipients are unknown, there may also be an increased potential for harm.

2.3.4. The relationships of those involved

2.3.4.1. Consider the relationship between the recipient of the breached information and the individual whose information was breached. An adverse relationship may result in the potential for harm to the individual or misuse of their information. For example, a letter containing sensitive personal information sent to a hostile ex-spouse who is threatening to publish it on social media would increase the potential for significant harm.

2.3.4.2. The key consideration is what is known about the person that caused the breach or received the breached personal information. For

example, if there is evidence that the person receiving the breached information intends to use the information in a malicious way, this would increase the potential for harm.

2.3.5. Ability to contain the breach

2.3.5.1. If a breach cannot be quickly contained by the District, this may increase the likelihood of significant harm. On the other hand, if the person receiving the breached information agrees to destroy or return the personal information involved in the breach, then the likelihood of significant harm is lower. For example, Staff who receive a misdirected email from a colleague within the District, who is subject to the same employment confidentiality requirements, could be quickly contained by deleting the email from the recipients' inbox and from their deleted folder. However, how quickly a breach can be contained is not the only factor for determining the risk of significant harm. To continue the example above, if the misdirected email includes a sensitive human resource issue and has been sent not just to one individual by mistake but to a large distribution list, the ability to quickly contain the information has decreased and the risk of significant harm has increased.

2.3.5.2. How the information was breached will have an impact on the District's ability to contain the breach. If the information was breached through theft, this will generally increase the risk of misuse and of significant harm.

2.4. Other elements to be considered in making a determination of significant harm is to be made with consideration of the following categories of harm or potential harm:

2.4.1. bodily harm;
2.4.2. humiliation;
2.4.3. damage to reputation or relationships;
2.4.4. loss of employment, business or professional opportunities;
2.4.5. financial loss;
2.4.6. negative impact on credit record,
2.4.7. damage to, or loss of, property,
2.4.8. the sensitivity of the Personal Information involved in the Privacy Breach; and
2.4.9. the risk of identity theft.

3. Step Three – Notification

3.1. If the Head determines that the Privacy Breach could reasonably be expected to result in Significant Harm to individuals, then the Head shall make notifications without unreasonable delay:

- 3.1.1. Report the Privacy Breach to the Office of the Information and Privacy Commissioner;
  - 3.1.1.1. Notifications to the Commissioner must be in writing and must contain the same information as the notification to affected individuals. They must also include an estimate of the number of affected individuals. Contact information for the Office of the Information and Privacy Commissioner can be found here. Note that the Commissioner provides additional resources for all public bodies for responding to breaches and securing personal information.
  - 3.1.1.2. Note that under section 36.3 (4) of FOIPPA, the Commissioner may choose to notify affected individuals if they determine that it is appropriate.
- 3.1.2. Report the Breach to the Minister of Education and Child Care and School Protection Program.
- 3.1.3. 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.
  - 3.1.3.1. Section 11.1 (1) (b) of the FOIPPA Regulation further describes the elements that must be included in a notification to an affected individual.

3.2. Breach Notifications

- 3.2.1. As noted in the FOIPPA Regulation, the breach notification must be in writing and must be provided directly to each affected individual. Note that there are specific circumstances that exist that allow indirect notification in accordance with section 11.1 (2) of the FOIPPA Regulation.
- 3.2.2. Elements to be included within the notification
  - 3.2.2.1. Name of the public body
  - 3.2.2.2. The breached personal information may be in the custody or under the control of more than one public body (e.g., two public bodies share a database that is hacked). In these circumstances, a good practice is to include the name of all public bodies involved in the breach.
  - 3.2.2.3. Description of the nature of the personal information involved in the privacy breach. For example, categories such as names, addresses,

phone numbers, dates of birth, personal health information, bank account information, etc. can be used.

3.2.2.3.1. When providing a description, take care to provide sufficient information without revealing the actual personal information itself. This will help minimize the potential for another breach if the notification is read by someone else because it was intercepted or sent to an address that is no longer correct.

3.2.2.4. Steps the public body has taken or will take to mitigate the risk of harm

3.2.2.4.1. Public bodies must advise the individual about steps, if any, that they have taken or will take to reduce the risk of harm. Examples could include Containment efforts, including correcting errors in a database where account errors have occurred (e.g., one person's personal information was accidentally added to another person's account); recovering physical documents when they are disposed of incorrectly; or confirming deletion of an email when information is sent to the wrong person.

3.2.2.4.2. Prevention measures to help ensure this type of incident does not reoccur. Prevention can include training or technical/system changes (for situations where the breach originated at the system level).

3.2.2.5. Steps the affected individual can take to mitigate the risk of harm

3.2.2.5.1. A key reason for notifying individuals of a privacy breach is to advise them of the risk of harm and inform them of steps they may take to mitigate that risk. Examples include providing contact information for a credit reporting bureau so the individual can monitor for suspicious activity.

3.2.3. A best practice is for the public body to make all reasonable efforts to outline the risks they are aware of at the time of notification. The public body may also consider following up with affected individuals if they receive further information about potential risks that could be mitigated.

3.2.4. Public bodies need to consider which method of notification is appropriate. While physical letters are the obvious example of notification provided "in writing," email notification may be preferable for individuals with no permanent housing. Public bodies should be cautious using text messages for notification as they may be mistaken for false or fraudulent communications, rather than an official communication from the District.

3.2.5. Verbal notification

3.2.5.1. There may be circumstances where public bodies contact the affected individual by phone, then follow up in writing. For example, if there is an imminent threat of physical harm, a written notification may cause unreasonable delay.

3.2.5.2. Affected individuals may need verbal notification for accessibility reasons or personal circumstances (e.g., limited access to a personal computer for emails or only having a shared email address). In these cases, verbal notifications should still be followed by a written notification.

3.2.6. Indirect notifications

3.2.6.1. As per section 11.1 (2) of the FOIPPA Regulation, indirect notification may be used if:

3.2.6.1.1. The District does not have accurate contact information for the affected individual. For example, when a breach occurs, the District may learn that they do not have the correct or up-to-date contact information to reach the individual. The District's email may be returned as undelivered, their call might go to a disconnected phone line, or their mail might be returned to sender. The District may also have other reasons to lack confidence that the contact information is correct.

3.2.6.1.2. The Head reasonably believes that providing the notice directly to the affected individual would unreasonably interfere with the operations of the District by being beyond the limits of what is reasonable or equitable in time and resources and the impact which this use of resources would have on the District's day-to-day activities.

3.2.6.1.3. The head reasonably believes that the information in the notification will come to the attention of the affected individual more quickly if it is given in an indirect manner. For example, when many people are affected, the notification may reach affected individuals sooner if it is communicated to the public rather than by contacting each affected individual directly.

3.2.6.2. An indirect notification must contain the same information that is required for direct notification of an affected individual.

3.2.6.3. When choosing the method for indirect notification, consider the circumstances of the breach, potential harms and risks to the affected individual, and the likelihood of the notification reaching the affected individual without unreasonable delay. For example,

consider posting a notification on a website or social media or via some form of public announcement.

3.3. Privacy breaches that may result in physical harm of an individual warrant immediate notification, even if all requirements for notification are not yet known (such as the date of the breach or all information elements involved). Instances where it is difficult to contain the breached information and where there is likelihood of significant harm may also warrant immediate notifications.

3.3.1. The District can follow up with more details as they become known.

3.4. 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 District's obligations or undermine public confidence in the District.

3.5. 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.

3.6 The Secretary Treasurer or designate shall notify School Protection Program of any breach of the district's network where it is reasonable to consider possible access or use of personal information, not authorized under FOIPPA, has occurred.

4. Step 4 – Remediation and Prevention

4.1. The Head, or the Privacy Officer in consultation with the Head, shall complete an investigation into the causes of each Breach Incident reported under this Practice.

4.2. The Head, or the Privacy Officer in consultation with the Head, shall implement measures to resolve the breach and prevent recurrences of similar incidents.