Living Sky School Division No. 202

Procedure Type: **Human Resources**

Procedure Number: **5.40**

Procedure Title: **Privacy Breach Protocol**

Legal References: ***Local Authority Freedom of Information and Protection of Privacy***

Approval Date: **September 18, 2019**

Revision Date:

Background

The focus of this procedure is on information privacy, or the right of an individual to determine for him or herself when, how, and to what extent his or her personal information will be shared.

The *Local Authority Freedom of Information and Protection of Privacy Act (LAFOIP)* is the provincial statute that applies to all local authorities, including boards of education. Personal information is defined in section 23 of *LAFOIP* and includes such information as a person's health history, home address, age and marital status.

Generally, personal information may only be used by the board of education for the purpose for which it was obtained or compiled, or for a use that is consistent with that purpose. Only division staff who require the personal information in order to complete their duties should be allowed to use the information.

A privacy breach happens when there is unauthorized collection, use or disclosure of private information.

Typically, Living Sky School Division will not consider a breach of privacy to have occurred if the information involved is sufficiently de-identified, provided as statistics only, or as aggregate data.

Procedures

Five Key Steps in Responding to a Privacy Breach

Respond immediately to the breach.

Step 1: Contain the breach.
Step 2: Investigate the breach.
Step 3: Assess and analyze the breach.

These first three steps should be carried out as quickly as possible.

Step 4: Provide proper notification of the breach.
Step 5: Prevention - Provide recommendations for longer term solutions and prevention strategies.

STEP 1: CONTAIN THE BREACH

Take immediate steps to contain the breach. These steps may include:

- Stop the unauthorized practice;
- Immediately contact the Director or designate, who should coordinate the following activities:
  - Recover the records;
  - Shut down the system that was breached;
  - Revoke access or correct weaknesses in physical security, and/or
  - Contact the police if the breach involves theft or other criminal activity, and contact affected individuals if they may need to take further steps to mitigate or avoid further harm.

STEP 2: INVESTIGATE THE BREACH

Once the breach has been contained, there will be an internal investigation by the Director or designate. It may be conducted on an informal or formal basis depending on the nature of the breach.

An internal investigation includes the following elements:

- Individuals with information about the breach should document details of the privacy breach and provide them to the Director or designate as quickly as possible.
- Evaluate the immediate and ongoing risks.
- Inventory and review safeguards in place prior to the incident.
- Provide findings and recommendations.
- Write a report or summary, as appropriate.

Questions to consider asking when conducting an internal investigation:

- What were the circumstances that led to the breach?
- Could the incident have been avoided?
- Was the breach accidental or intentional?
- What measures need to be put in place to avoid a future similar incident?
- Will we need to prepare an internal investigation report or just a summary/memo?

The findings of an internal investigation are recorded in an Investigation Report and include the following information:

- A summary of the incident and immediate response to contain the breach and reduce harm;
- Steps taken to contain the breach;
- Background of the incident;
- Timeline and a chronology of events;
- Personal information involved (data elements and sensitivity of, number affected, etc.);
- A description of the investigative process;
- The cause of the incident (root and contributing);
- A summary of interviews held (complainant, internal, external);
- A review of safeguards and protocols;
- A summary of possible solutions and recommendations;
- A description of necessary remedial actions, including short-term and long-term strategies to correct the situation (staff training, rework policies/procedures, etc.);
- A detailed description of what the next steps will be;
- Responsibility for implementation and monitoring, including timelines, and
- Names and positions of individuals responsible for the implementation.

STEP 3: ASSESS AND ANALYZE THE BREACH AND ASSOCIATED RISKS

To determine what other steps are immediately necessary and assess the risks associated with the breach, consider the following:

Is Personal information involved?

- What data elements have been breached?
  - Generally, the more sensitive the information, the higher the risk.
  - Social insurance numbers and/or financial information that could be used for identity theft are examples of sensitive information.
- What possible use is there for the information?
- Can the information be used for fraudulent or otherwise harmful purposes?

What is the cause and extent of the breach?

- What is the root cause of the breach?
- Is there a risk of ongoing or further exposure of the information?
- What short-term and long-term steps have been taken to minimize the harm?
- What is the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?
- Is the information encrypted or otherwise not readily accessible?
- Is the information de-identified, statistical or aggregate only?

How many are affected by the breach?

- How many individuals are affected by the breach?
- Who is affected by the breach: employees, public, contractors, clients, service providers, other organizations?

What is the foreseeable harm resulting from the breach?

- Is there any relationship between the unauthorized recipients and the data subject?
- What harm to the individuals will result from the breach?
  - Harm may include:
    - Security risk (e.g. physical safety);
    - Identity theft or fraud;
    - Loss of business or employment opportunities, and/or
    - Hurt, humiliation, damage to reputation or relationships.
- What harm could result to the organization as a result of the breach?
  - Harm may include:
    - Loss of trust in the organization, public body or custodian;
    - Loss of assets, and/or
    - Financial exposure.
- What harm could result to the public as a result of the breach?
  - Harm could include:
    - Risk to public health, and/or
    - Risk to public safety.

STEP 4: NOTIFICATION: WHO, WHEN AND HOW TO NOTIFY

The key consideration in deciding whether to notify affected individuals should be whether notification is necessary in order to avoid, mitigate or address harm to an individual whose personal information has been inappropriately collected, used or disclosed.

Notifying Affected Individuals

Notification of affected individuals should occur if it is necessary to avoid, mitigate or address harm to them. Some considerations in determining whether to notify individuals affected by the breach include:

- Risk of identity theft or fraud: How reasonable is the risk? Identity theft is a concern if the breach includes unencrypted information such as names in conjunction with SINs, credit card numbers, driver's license numbers, personal health numbers, or any other information that can be used to commit fraud by third parties.
- Risk of physical harm: Does the breach place any individual at risk of physical harm, stalking or harassment?
- Risk of hurt, humiliation or damage to reputation: This type of harm can occur when personal information such as mental health records, medical records or disciplinary records are breached.
- Risk of loss of business or employment opportunities: Could the breach result in damage to the reputation of an individual, affecting business or employment opportunities?

When and How to Notify

- When: Notification of individuals affected by the breach should occur as soon as possible. However, if law enforcement authorities have been contacted, those authorities should be consulted to determine whether notification should be delayed in order not to impede a criminal investigation. Ensure all such discussions are documented.
- How: The preferred method of notification is direct (by telephone, letter or in person) to affected individuals. This method is preferred in circumstances such as those listed:
  - The identities of individuals are known;
  - Current contact information for the affected individuals is available;
  - Affected individuals require detailed information in order to properly protect themselves from the harm arising from the breach, and/or
  - Affected individuals may have difficulty understanding an indirect notification due to mental capacity, age, language, or other factors.
- Indirect Notification
  - Website information, posted notices, media – should generally only occur when direct notification could cause further harm, is prohibitive in cost, contact information is lacking, or when a very large number of individuals is affected by the breach such that direct notification could be impractical.
  - Using multiple methods of notification in certain cases may be the most effective approach.
- What: Notifications should include the following information:
  - Impacts of the breach on affected individuals - an apology;
  - Date of the breach;
  - Description of the breach (a general description of what happened);
  - Description of the breached personal information (e.g. name, credit card numbers, SINs, medical records, financial information, etc.);
  - The steps taken to mitigate the harm to date;
  - Next steps planned and any long-term plans to prevent future breaches, and
  - Steps individuals can take to further mitigate the risk of harm:
    - Provide information about how individuals can protect themselves, e.g. how to contact credit reporting agencies (to set up a credit watch), how to change a health services number or driver's license number;
    - Provide contact information of an individual within the organization who can answer questions and provide further information, and
    - Inform individuals that they have a right to complain to the OIPC. Provide contact information.

Others to Contact

The following authorities or organizations may also be informed:

- OIPC: Proactive disclosure of a privacy breach to the OIPC may better prepare the organization to respond to queries from MLAs, the media, and the public.

- The following factors are relevant in deciding when to report a breach to the OIPC:
  - The sensitivity of the personal information;
  - Whether the disclosed personal information could be used to commit identity theft;

- Whether there is a reasonable chance of harm from the breach;
- The number of people affected by the breach, and
- Whether the personal information was fully recovered without further disclosure, or if any further unauthorized use has been thwarted.

Local authorities can also contact the Access and Privacy Branch of the Ministry of Justice and Attorney General for advice in regard to responding to an incident.

- Police: if theft or other crime is suspected;
- Insurers or others: if required by contractual obligations;
- Professional or other regulatory bodies: if professional or regulatory standards require notification of these bodies, and
- Credit card companies and/or credit reporting agencies: It may be necessary to work with these companies to notify individuals and mitigate the effects of fraud.

STEP 5: PREVENTION

Once the immediate steps are taken to mitigate the risks associated with the breach, the Privacy Officer will thoroughly investigate the cause of the breach. This will ultimately result in a plan to avoid future breaches. This may require an audit of physical, administrative and technical safeguards. The plan will also include a process to ensure that the prevention plan has been fully implemented.

As a result of such evaluations, the Privacy Officer will develop, or improve as necessary, adequate long-term safeguards against further breaches. Policies and safeguards will be reviewed and updated to reflect and implement the recommendations gleaned from the investigation. Policy review and updates will occur regularly, at least biannually, after that.

Related

Privacy Breach Guidelines for Government Institutions and Local Authorities

https://oipc.sk.ca/assets/privacy-breach-guidelines-for-government-institutions-and-local-authorities.pdf

Procedure 5.38: *Local Authority Freedom of Information and Protection of Privacy Act*

Procedure 5.39: *Confidentiality*