Administrative Procedure 195
Privacy Breach

The Limestone District School Board recognizes the importance of protecting personal information and is committed to ensuring that procedures and practices support the need to protect personal and confidential information. In the event of a breach of privacy, the Board will respond promptly, containing and addressing incidents involving unauthorized disclosure of personal information. To this end, everyone has a role and responsibility to assist in the containment of a privacy breach.

1. Definition

1.1. A privacy breach occurs when personal information is compromised, that is, when it is collected, used, disclosed, retained, or destroyed in a manner inconsistent with privacy legislation. Ontario school boards/authorities are governed by the following privacy statutes: Municipal Freedom of information and Protection of Privacy Act (MFIPPA) and Personal Health Information Protection Act (PHIPA).

1.2. Personal information can be compromised in many ways. Some breaches have relatively simple causes and are contained, while others are more systemic or complex. Privacy breaches are often the result of human error; such as an individual's personal information being sent by mistake to another individual (e.g., fax number, email address, etc.). In today's environment in which technology increasingly facilitates information exchange, sometimes a privacy breach can be more wide-scale, such as when an inappropriately executed computer programming change causes the personal information of many individuals to be compromised.

2. Examples of Privacy Breaches

2.1. Inappropriate Disclosure or Use of Personal Information

2.1.1. Student Records

- Two teachers discussing (and identifying) a student in the local grocery store.

- Student's report card mailed to the wrong home address.
- Digital images of individuals taken and displayed without consent.
- Hard-copy psychological assessments kept in openly accessible file cabinets that are not secured or controlled.
- Confidential student health records inadvertently blown out of a car trunk and scattered over a busy street.
- Lost memory key containing student data.
- Theft from teacher's car of a laptop containing Special Education student records on the hard drive.

2.1.2. Employee Records

- Employee files containing social insurance numbers left in unlocked boxes near the open shipping/ receiving area.
- Theft from car of a briefcase containing a list of home addresses of teaching staff.
- Sending sensitive personal information to an unattended, open-area printer/fax.
- Password written on a sticky note stuck to a monitor.
- Resumes faxed or emailed to a wrong destination or person.

2.1.3. Business Records

- A list of names, including credit card numbers, left on the photocopier.
- Personal information disclosed to trustees who did not need it to effectively decide on a matter.

- Stolen laptop containing names and addresses of permit holders.
- Tender information scanned and not cleared from multifunctional office machine.
- Disposal of equipment with memory capabilities (e.g., memory keys, disks, laptops, photocopiers, fax machines, or cell phones) without secure destruction of the personal information it contains.

3. Roles and Responsibilities

3.1. All Board employees are responsible for:

- Ensuring protection of personal information;
- Notifying their supervisor immediately, or, in their absence, the Manager of Human Resources, upon becoming aware of a breach or suspected breach;
- Containing, if possible, the suspected breach by suspending the process or activity that caused the breach.

3.2. The Board is responsible for:

- Educating and training employees on personal information and protection of privacy;
- Obtaining all available information about the nature of the breach or suspected breach, and determining what happened;
- Taking all necessary steps to contain the breach;
- Investigating and documenting details of the breach and implementing corrective actions, as necessary.
- Monitoring and evaluating implementation of remedial action;

- Ensuring individuals whose personal information has been compromised are informed as required.

4. Third Party Service Providers

4.1. This procedure applies to all third party service providers, which may include commercial school photographers, bus companies, external data warehouse service providers, outsourced administrative service providers such as shredding companies, Family and Children's Services, Public Health Units (PHU), external researchers, and external consultants.

4.2. The Board retains the responsibility for protecting personal information in accordance with privacy legislation and therefore service providers must adhere to the Privacy Breach Protocol if a privacy breach occurs when they have custody of personal information.

4.3. Third party service providers are responsible for:

- Informing the Board contact as soon as a privacy breach or suspected breach is discovered;
- Taking all necessary actions to contain the privacy breach as directed by the Board;
- Documenting how the breach was discovered, what corrective actions were taken and report back;
- Undertaking a full assessment of the privacy breach in accordance with the third party service provider's contractual obligations;
- Implementing all necessary remedial action to decrease the risk of future breaches;
- Fulfilling contractual obligations to comply with privacy legislation.

5. Privacy Breach Protocol

5.1. The following steps must be initiated as soon as a privacy breach or suspected breach has been reported.

5.2. Step 1 – Respond

It must first be determined if a privacy breach has occurred, including the possible extent of the breach. Where a breach has occurred, the responsible supervisor must be notified who will then notify the Manager of Human Resources who will provide advice and direction, as necessary.

5.3. Step 2 – Contain

Once identified, the breach must be contained, which could include retrieving hard copies of any personal information that has been disclosed, determining if the breach enables further unauthorized access to additional personal information, changing passwords and identification numbers and/or temporarily shutting down the system if necessary to contain the breach.

All actions taken must be documented and a communication strategy developed as necessary. The Privacy Breach Checklist (Appendix A) has been developed to assist in this regard.

5.4. Step 3 – Investigate

Once the privacy breach is contained, an investigation must be conducted in order to identify what caused the breach, evaluate the actions taken to contain the breach, and to make recommendations aimed at preventing future breaches.

5.5. Step 4 – Notify Affected Individuals

Where a privacy breach has occurred, any individual whose personal information was disclosed must be notified. This includes

- What happened;
- Potential or risk of harm;
- Mitigating actions the board is taking;
- Appropriate action for individuals to take to protect themselves against harm;
- Notify appropriate managers and employees within the Board of the breach;
- Report the privacy breach to the office of the Information and Privacy Commissioner (IPC) as appropriate.

5.6. Step 5 – Implement Change

When determining what changes and remedial actions need to be implemented, consider whether it is necessary to:

- Review the relevant information management systems to enhance compliance with privacy legislation;
- Amend or reinforce the existing policies, procedures, and practices for managing and safeguarding personal information;
- Develop and implement new security or privacy measures, if required;
- Review employee training on legislative requirements, security and privacy policies, procedures, and practices to reduce potential or future breaches, and strengthen as required;
- Test and evaluate remedial actions to determine if they have been implemented correctly and if policies, procedures, and practices need to be modified;

- Recommend remedial action to the Manager of Human Resources (FOI Coordinator).

6. How to Determine if Notification is Required

There are several factors that should be considered when determining whether notification is required. Decisions in this regard must be made in consultation with the Manager of Human Resources.

6.1. Risk of Identity Theft

Individuals must be notified where a risk of identity theft or other potential for fraud exists. For example, access to unencrypted information such as names in conjunction with social insurance numbers, credit card numbers, driver's license numbers, personal health numbers, or any other information that can be used for fraud by third parties (e.g., financial).

6.2. Risk of Physical Harm

Where an individual is at risk of physical and/or psychological harm as a result of a privacy breach, notification is required in order that protective measures may be implemented.

6.3. Risk of Hurt, Humiliation, Or Damage to Reputation

Where the loss or theft of personal information could lead to hurt, humiliation, or damage to an individual's reputation, notification is required. Examples include loss or theft of mental health records, medical records, or disciplinary records.

6.4. Risk of Loss of Business or Employment Opportunities

Where the loss or theft of information could result in damage to an individual's reputation, affecting their business or employment opportunities, notification is also required.

7. Additional Resources

AICA/CICA Privacy Taskforce, *Incident Response Plan 2003*
(American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants)
Government of Ontario, Ontario Shared Services, *Privacy Review 2005*
Information and Privacy Commissioner/Ontario, *Breach Notification Assessment Tool, December 2006*
Information and Privacy Commissioner/Ontario*, What to do if a Privacy Breach Occurs: Guidelines for Government Organizations,* May 2003
The Office of the Chief Information and Privacy Officer, *Taking the Right Steps – A Guide to Managing Privacy and Privacy Breaches,* revised April 18, 2007

Reference:

Municipal Freedom of Information & Protection of Privacy Act
Freedom of Information & Protection of Privacy Act
Personal Health Information Protection Act

APPENDIX A

LIMESTONE DISTRICT SCHOOL BOARD
PRIVACY BREACH CHECKLIST

BREACH REPORT # _____

1. **Person Reporting Suspected Breach:**

First name:_____ Last name:_____
Job title: _____
Location (school/department): _____
Name of immediate supervisor: _____
Phone number:
_____

2. **When Incident Occurred: Date _____ Time _____**

3. **Incident Details:**

Number of individuals whose information was accessed without consent or authorization:
_____
_____

Type of personal information that was accessed without consent or authorization, e.g., health/medical information, student marks, biographical information (such as home address, phone numbers, names and contact information of family members), behaviour concerns,
_____
_____
_____ _____ _____

To whom the personal information belongs (e.g., student, employee, third party someone who is neither a student nor employee of the board, such as a parent/ guardian or volunteer
_____
_____
_____
_____

Who had unauthorized access to the personal information, and how access was made:
_____
_____

Steps taken to contain the privacy breach *(e.g., suspending the process/activity that caused the breach)*

_____
_____
_____
_____
_____

Date _____ **Time** _____

3. **Investigate**

Following a report of a suspected privacy breach, ensure that the activity/process has been contained where possible. An investigation must be conducted based on the information provided above and in conjunction with current privacy legislation (MFIPPA, PHIPA, PIPEDA) and Board procedures.

Summary of Investigation

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

If a breach HAS NOT occurred:
Contact the person who reported the suspected breach and his/her immediate supervisor to advise him/her of your determination. No further action is required by the employee or supervisor.

4. **Notification Requirements**

If a breach HAS occurred, notify the following individuals, as appropriate and in consultation with the Manager of Human Resources:

❑ Manager of Human Resources ❑ Individuals whose privacy was breached

❑ Senior administration/managers/principals ❑ Legal counsel

❑ IPC ❑ Other

5. **Implement Change**

Steps taken to correct the problem
❑ Develop, change, or enhance procedures and practices
❑ Improve security and privacy controls

Provide additional notices (as deemed appropriate)
❑ Relevant third parties
    ❑ Consider public announcement (e.g., statement and/or apology)
❑ Other Ontario school boards/authorities (where shared responsibilities exist)
❑ Advise IPC of investigation findings and corrective action, as necessary

Prevent future breaches:
❑ Provide employee training on privacy and security
❑ Evaluate the effectiveness of remedial actions

6. **Sign-off**

The Manager of Human Resources is required to sign below to formally acknowledge that the breach was handled in accordance with privacy legislation and with the Board procedures.

_____ _____
Print Name/Title *Date*

_____
Signature