# ALGONQUIN AND LAKESHORE CATHOLIC DISTRICT SCHOOL BOARD

## ***PRIVACY BREACH PROTOCOL***

### Purpose

The Algonquin and Lakeshore Catholic District School Board is committed to the protection of personal information under its control and to an individuals' right of privacy regarding personal information that is collected, used, disclosed, and retained in the school system.

While protection of this information is paramount, and is a priority of the Board, the Board recognizes unintentional breaches can occur. To that end, the following procedures outline the immediate actions to be undertaken in the case of a privacy breach.

### Procedures

**1. Definition of a Privacy Breach**.

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. The Algonquin and Lakeshore Catholic District School Board is governed by the following privacy statutes: *Municipal Freedom of information and Protection of Privacy Act* (MFIPPA), *Personal Health Information Protection Act* (PHIPA), and *Personal Information Protection and Electronic Documents Act* (PIPEDA).

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.

**The following are some examples of privacy breaches:**

| | Student Records | Employee Records | Business Records |
|---|---|---|---|
| **Inappropriate disclosure/use of personal information** | Two school staff members discussing (and identifying) a student in the local grocery store.<br><br>Student's report card mailed to the wrong home address. | Employee files containing social insurance numbers left in unlocked boxes near the open shipping/ receiving area.<br><br>Budget reports (containing employee numbers and names) | A list of names, including credit card numbers, left on the photocopier.<br><br>Personal information disclosed to trustees who did not need it to effectively decide on a matter. |

| | | | |
|---|---|---|---|
| | Digital images of individuals taken and displayed without consent.<br><br>Hard-copy student assessments kept in openly accessible file cabinets that are not secured or controlled.<br><br>Confidential student health records inadvertently blown out of a car trunk and scattered over a busy street. | found in their entirety in recycle bins and garbage bins.<br><br>Theft from car of a briefcase containing a list of home addresses of staff. | |
| **Technology/ computer error** | Lost memory key containing student data.<br><br>Theft from staff member's car of a laptop containing student records on the hard drive. | Sending very sensitive personal information to an unattended, open-area printer.<br><br>Password written on a sticky note stuck to a monitor.<br><br>Résumés faxed or emailed to a wrong destination or person. | Stolen laptop containing names and addresses of permit holders.<br><br>Tender information scanned and not cleared from multifunctional office machine.<br><br>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. |

## 2. Roles and Responsibilities in Responding to Privacy Breaches

The following personnel may need to be involved when the Board responds to a privacy breach. Some of the following roles and responsibilities may be undertaken concurrently.

| Individuals | Roles | Responsibilities |
|---|---|---|
| **Employees** | All school board employees need to be alert to the potential for personal information to be compromised, and therefore potentially play a role in identifying, notifying, and containing a breach. | All school board employees have the responsibility to:<br>• notify their supervisor immediately, or, in his/her absence, the Board's FOI Officer upon becoming aware of a |

| Individuals | Roles | Responsibilities |
|---|---|---|
| | Employees dealing with student, employee and/or business records need to be particularly aware of how to identify and address a privacy breach. | breach or suspected breach;<br>• contain, if possible, the suspected breach by suspending the process or activity that caused the breach. |
| **Senior Administration, Managers, and Principals** | Senior administration, managers, and principals are responsible for alerting the FOI Officer of a breach or suspected breach and will work with the Officer to implement the five steps of the response protocol. | Senior administration, managers, and principals have the responsibility to :<br>• obtain all available information about the nature of the breach or suspected breach, and determine what happened;<br>• alert the FOI Officer and provide as much information about the breach as is currently available;<br>• work with FOI Officer to undertake all appropriate actions to contain the breach;<br>• ensure details of the breach and corrective actions are documented. |
| **FOI Officer** | The FOI Officer plays a central role in the response to a breach by ensuring that all five steps of the response protocol are implemented. | The FOI Officer will follow the following five steps:<br><br>Step 1 – Respond<br>Step 2 – Contain<br>Step 3 – Investigate<br>Step 4 – Notify<br>Step 5 – Implement Change |
| **Accountable Decision Maker** | The responsibility for protecting personal information affected by a privacy breach is assigned to the Director of Education/designate who is the accountable decision maker. | The Director of Education has the responsibility to :<br>• brief senior management and trustees as necessary and appropriate;<br>• review internal investigation reports and approve required remedial action;<br>• monitor implementation of |

| Individuals | Roles | Responsibilities |
|---|---|---|
| | | remedial action;<br>• ensure that those whose personal information has been compromised are informed as required. |
| **Third Party Service Providers** | Contracted third party service providers carry out or manage programs or services on behalf of the Board.<br><br>Typical third party service providers are commercial school photographers, external data warehouse services, shredding companies, Children's Aid Societies (CAS), Public Health Units (PHU), external researchers, and external consultants.<br><br>In such circumstances, the Board retains responsibility for protecting personal information in accordance with privacy legislation.<br><br>Therefore, third party service providers need to know their roles and responsibilities if a privacy breach occurs when they have custody of personal information.<br><br>All third party service providers must take reasonable steps to monitor and enforce their compliance with the privacy and security requirements defined in the contracts or service agreements, and are required to inform the Board of all actual and suspected privacy breaches. | The third party service providers have the responsibility to:<br><br>• inform the Board contact as soon as a privacy breach or suspected breach is discovered;<br><br>• take all necessary actions to contain the privacy breach as directed by the Board;<br><br>• document how the breach was discovered, what corrective actions were taken and report back;<br><br>• undertake a full assessment of the privacy breach in accordance with the third party service providers' contractual obligations;<br><br>• take all necessary remedial action to decrease the risk of future breaches;<br><br>• fulfill contractual obligations to comply with privacy legislation. |

**** Everyone has a role and responsibility to notify and contain a privacy breach depending on the situation.***

**3. Response Implemented by the FOI Officer**

Step 1 – Respond

- Assess the situation to determine if a breach has indeed occurred and what needs to be done;

- When a privacy breach is identified by an internal or external source, contact the appropriate area to respond to the breach;
- Provide advice on appropriate steps to take to respond to the breach;
- Report the privacy breach to key persons within the Board (including the Director of Education or designate) and, if necessary, to law enforcement;
- Evaluate effectiveness of response to the breach and implement improvement as necessary.

**Step 2 – Contain**

- Identify the scope of the breach and contain it (e.g., retrieve the hard copies of any personal information that has been disclosed, determine if the breach would allow unauthorized access to any other personal information [e.g., electronic information system], change passwords and identification numbers and/or temporarily shut down the system if necessary to contain the breach);
- Document the breach and containment activities;
- Develop briefing materials;
- Brief the accountable decision maker, senior management, and key persons on the privacy breach and how it is being managed.

**Step 3 – Investigate**

Once the privacy breach is contained:

- Conduct an investigation with the involvement of other parties as necessary:
    - Identify and analyze the events that led to the privacy breach;
    - Evaluate what was done to contain it; and
    - Recommend remedial action so future breaches do not occur.

- Document the results of internal investigation including:
    - background and scope of the investigation;
    - legislative implications;
    - how the assessment was conducted;
    - source and cause of the breach;
    - inventory of the systems and programs affected by the breach;
    - determination of the effectiveness of existing security and privacy policies, procedures, and practices;
    - evaluation of the effectiveness of the Board's response to the breach;
    - findings including a chronology of events and recommendations of remedial actions;
    - the reported impact of the privacy breach on those individuals whose privacy was compromised.

**Step 4 – Notify**

- Notify, as required, the individuals whose personal information was disclosed.

The purpose of providing notice of a privacy breach to the individuals whose personal information was involved in the incident is to provide them with information about:

- what happened;
- the nature of potential or actual risks or harm;
- what mitigating actions the board is taking;

- appropriate action for individuals to take to protect themselves against harm.

If personal information that could lead to identity theft has been disclosed, affected individuals should be provided with information on steps they can take to protect themselves. If the office of the Information and Privacy Commissioner (IPC) is investigating the privacy breach, indicate that to the affected individuals. Give an explanation of the individual's right to complain to the IPC about the Board's handling of their personal information, along with contact information for the IPC.

- 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.

**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 accountable decision maker.