Breaches PIM Toolkit, 38, 211, 288-289

What is a privacy breach?

A privacy breach occurs when personal information is collected, retained, used, or disclosed in ways that are not in accordance with the provisions of the *Municipal Freedom of Information and Protection of Privacy Act*. Among the most common breaches of personal privacy is the unauthorized disclosure of personal information, contrary to section 32 of the Act. For example, personal information may be lost, stolen (especially from laptop computers, a prime example), or inadvertently disclosed through human error, and upon learning of a privacy breach, immediate action should be taken. Users should contact their FOI Coordinator immediately or refer to their Board's Privacy Breach Procedure.

How does a school or school board manage the risk of a privacy breach?

Risks to information are managed and practices and processes are in place to protect information assets:

- **a.** Risks to records and information are identified and managed.
- **b.** Practices are in place to protect confidential, sensitive, and personal records and information from unauthorized collection, use, disclosure, or destruction.
- **c.** All records are managed to meet rules of evidence and legal discovery.
- **d.** Contractual arrangements include provisions for the protection and appropriate use of records
  and information to mitigate risks.
- **e.** Records and information are managed to support business continuity and recovery in the event of disaster.
- **f.** Records and information are managed to protect privacy and confidentiality.

A newspaper reporter brings to your attention that school records (Visa receipts from a former school employee) were found strewn about the school yard and the surrounding homes. What steps do you take?

Follow your board's procedures for privacy breaches:

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 Ontario school board/authority (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 and use the privacy breach checklist for record keeping, 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 Ontario school board's/authority'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;
- Refer to page 36 of the PIM Toolkit, “How do you determine if Notification is required?” 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 Ontario school board's/authority's handling of their personal information, along with contact information for the IPC.
- Notify appropriate managers and employees within your Ontario school boards/authorities 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.

Principal's Best Practice: Put "information security" and "privacy breaches" on a staff meeting agenda at the beginning of the year. Conduct a self-awareness exercise with your staff. Ensure that everyone understands how to secure and dispose of confidential and personal information. Determine whether or not you have the necessary hardware to compliment your procedures. If not, update equipment and seek assistance from your Superintendent of Education if necessary. Check to see all shredders are compatible with board requirements. Attach a message to each paper bin, "All paper is this box must be shredded".