Pembina Hills
PUBLIC SCHOOLS

Information Security Breach

AP 80-11

Definitions

In this Administrative Procedure:

1. **PHPS** means Pembina Hills Regional Division No. 7, also known as Pembina Hills Public Schools.

2. **Information** means all information in the custody or under the control of PHPS, whether in electronic or other recorded format, and includes administrative, financial, personal and student information, and information about those who interact or communicate with PHPS.

3. **Personal information** means recorded information about an identifiable individual, including
   (i) the individual's name, home or business address or home or business telephone number;
   (ii) the individual's race, national or ethnic origin, colour or religious or political beliefs or associations;
   (iii) the individual's age, sex, marital status or family status;
   (iv) an identifying number, symbol or other particular assigned to the individual;
   (v) the individual's fingerprints, blood type or inheritable characteristics;
   (vi) information about the individual's health and health care history, including information about a physical or mental disability;
   (vii) information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;
   (viii) anyone else's opinions about the individual;
   (ix) the individual's personal views or opinions, except if they are about someone else; and
   (x) student records.

4. **Employee** has the meaning given in the *Freedom of Information and Protection of Privacy Act* and includes employees, contractors, volunteers, and others providing services to, or on behalf of, PHPS.

5. **Student information** means personal information about a student, whether enrolled with PHPS or not, including information about any student contained in PASI.

6. **PASI** means the Provincial Approach to Student Information database and application maintained by Alberta Education.

7. **Risk** means any factor that could be detrimental to the confidentiality, availability, integrity or privacy of information in the custody or control of PHPS.

8. **Internal** network refers to the segments that have direct access to PHPS core services including (but not limited to) Student Information System (SIS), Transportation and Finance. This includes most of the “wired” network (CAT5 and CAT6) and the Internal wireless network.

9. **Breach** refers to loss, damage or unauthorized access to data in the care of PHPS.

Purpose

The purpose of this Administrative Procedure is to describe how to categorize and respond to losses of personal information in PHPS control, especially sensitive and personal information. This is part of the PASI initiative to secure student data.

Accountability

The Superintendent of PHPS is accountable for general PHPS compliance with this Administrative Procedure and for maintaining and updating the Administrative Procedure as necessary. The Site Administrator of each school operated by PHPS is accountable for that school's compliance with this Administrative Procedure.

Enforcement

Any employee found to have violated this Administrative Procedure may be subject to disciplinary action, up to and including termination of employment. Depending on the severity of the situation, this may result in criminal and civil legal action.

Types of Breaches

Information breaches can occur in terms of loss and access. Loss indicates that a device, document or other media has been misplaced and cannot be accounted for. Access includes both physical and electronic means which could include a break-in or other unauthorized co-location with sensitive documents, hacking, or transfer of data by insecure means. It can also include accidentally sending information to the wrong recipient.

Sensitivity of Information

Different pieces of information have different ranks as defined by the Office of the Information and Privacy Commissioner:

- High
  - SIN, date of birth, driver's license, credit card numbers, signatures, counselling notes, human resources documentation
- Moderate
  - Names, phone numbers, email addresses, bank account and RRSP account numbers.
- Note: Items ranked moderate could be deemed more sensitive if there is a potential for violence or other harm as a result of a breach.

Evaluating Risk

In order to determine the risk generated by a breach, the following need to be considered:

- Does the loss of information put the individual at risk personally or financially?
- Who has obtained access to the information?
- Is the information highly sensitive?

- How long was the information exposed?
- Is there evidence of malicious intent or purpose associated with the breach?
- Could the information be used for criminal purposes such as identity theft or fraud?
- Was the information recovered?
- How many individuals are affected by the breach?
- Are the individuals involved vulnerable, such as children or seniors?

Breach Response Plan

When dealing with an information breach, it is imperative that the following steps be taken immediately:

1. **Site Administration is made aware of Breach:**

Site Administrator immediately:
- notifies FOIP Coordinator
- notifies Director of Information Technology
- shares details of breach including as much information as possible
    - who
    - what
    - where
    - when
    - why
    - how

2 a. **If Breach is suspected to involve Electronic Media:**

Director of Information Technology immediately:
- initiates an investigation to ascertain if the breach involves electronic media, then works to contain the breach (if possible),
- takes action to correct the conditions that led to the breach,
- stops breach as quickly as possible, and
- documents all investigatory work.

Director of Information Technology notifies FOIP Coordinator, Superintendent, and Secretary Treasurer of:
- the nature of the breach,
- the information that was exposed,
- to whom it was exposed,
- for how long it was exposed,
- initial and ongoing investigation details.

2 b. I**f Breach Does Not Involve Electronic Media:**

FOIP Coordinator immediately:
- initiates an investigation, and works to contain the breach,
- takes action to correct the conditions that led to the breach,
- stops breach as quickly as possible, and

- documents all investigatory work.

FOIP Coordinator notifies Superintendent and Secretary Treasurer of the nature of:
- the nature of the breach,
- the information that was exposed,
- to whom it was exposed,
- for how long it was exposed,
- initial and ongoing investigation details.

The Superintendent will inform Regional Services Administration and the Board of the breach, if the situation warrants.

3. **Create Action Plan to support the situation:**

FOIP Coordinator is the 'point' person.
- FOIP Coordinator will be apprised of all relevant information for collection.
- FOIP Coordinator will contact the FOIP Administrator, if situation warrants.

If situation warrants, Regional Services Administration notifies:
- Alberta Education
- Local law enforcement
- Legal counsel

If the breach is staff related:
- impacted staff will be notified
- other staff will be notified, if situation warrants.

If the breach is student related:
- parents and independent students will be notified.

Affected parties may be kept apprised of ongoing investigation (if not FOIP restricted – or restricted by a parallel investigation of RCMP or Alberta Education).

4. **Capture Breach Information and Damage Analysis:**

- Determine what information was compromised.
- Assess what the chances are that the compromised information will be used illegally.
- Assess what steps can be taken to mitigate the effects of the compromised information.
- Identify cause and potential solutions.
- If criminal intent or gross misconduct is suspected, a parallel investigation of the RCMP may result.
- Summarize lessons learned.
- Implement any procedure changes.

Reference

Child, Youth and Family Enhancement Act
Freedom of Information and Protection of Privacy Act
Health Information Act

Income Tax Act
School Act R.S.A. 2000, c.S-3,ss 23, 60(3)(c)
Student Record Regulation
AP 30-50 Records Management
AP 30-55 Record Retention Schedule
AP 80-05 Technology Acceptable Use
AP 80-10 Information Security
AP 80-20 Mobile Devices (Employees)