Pembina Hills
PUBLIC SCHOOLS

Information Security

AP 80-10

Definitions

In this administrative procedure:

1. **PHPS** means 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's 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.

Purpose

The purpose of this administrative procedure is to define standards for protecting PHPS's information, especially sensitive and personal information, from unauthorized collection, use, disclosure, retention or destruction.

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.

Information Security Principles

1. Only authorized persons may have access to information.
2. All information must be maintained in confidence and disclosed only if authorized by regulation or law including, but not limited to, the *School Act*, the *Freedom of Information and Protection of Privacy Act*, the *Child, Youth and Family Enhancement Act* and the *Income Tax Act*.
3. Only authorized persons may use, disclose, take, alter, copy, interfere with, or destroy information, and must do so according to law and PHPS records management standards, procedures, and practices.
4. Each person using PHPS's information at a PHPS location or otherwise, is responsible for the management and safekeeping of information under their control by ensuring that there is adequate security to prevent unauthorized access, collection, use, disclosure or disposal of information.
5. Security measures must be used for
   - electronic information;
   - access to recorded messages, voice mail and telephone answering machines;
   - and access to and within buildings.
6. The nature of security measures must be adequate and appropriate for the sensitivity of the information to be protected.
7. Employees will be provided with training and awareness materials as necessary to ensure that they understand their security obligations.

Cellular Telephones, Emails and Faxes

Caution must be used when conveying confidential information over insecure technologies such as cellular telephones, email and faxes.

Clean Desks

Records containing sensitive or confidential information must not be kept on desks or in places where unauthorized persons or members of the public may see or have access to them.

Secure Storage of Information

Sensitive or confidential information must be stored in a secure location with restricted access, such as secure electronic storage, a locked room, or a locked filing cabinet. Security measures must be appropriate for the sensitivity of the information being stored regardless of the physical or electronic medium on which it is stored.

Care must be taken when transporting or transferring sensitive or confidential information so that it reaches its intended destination intact and without unauthorized access or disclosure.

All keys used for encryption and decryption must meet complexity requirements described in the Passwords section of this administrative procedure.

Where at all possible, student and Division information should be not be stored on personal devices. Due to the possibility of loss or theft, these devices should be viewed as representing a greater risk. As such they should not be used for storage. Instead their primary purpose should be for immediate connectivity and creation of data.

Division approved cloud based services like Google Apps, Discovery Education, and FreshGrade should be used with secure credentials and access restricted to staff accounts. In situations where local copies may be necessary, they should be deleted off of personal devices as soon as possible.

Sensitive documents, such as student assessments and plans should only be stored on division servers. This includes internal file servers, PowerSchool (Dossier), and Docushare. **Google services should NOT be used as a storage location for personal and financial information.** This includes both Gmail and Drive. While these services may be used for collaboration purposes, final copies should be transferred to the secure locations listed above and the drafts deleted (these may also be transferred).

Disposal of Information

Any information that is no longer required for either administrative, educational, financial, legal or historical purposes, and the retention of which is not regulated by any provincial or federal law, may only be destroyed in accordance with records management procedures and practices.

Privacy Complaints

All privacy complaints must be forwarded to the PHPS Freedom of Information and Protection of Privacy Coordinator.

Remote Access

Remote access implementations that are covered by this administrative procedure include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

1. It is the responsibility of each of PHPS's employees, contractors, vendors and agents with remote access privileges to PHPS's corporate network to ensure that their remote access connection is as secure as the user's on-site connection to PHPS.
2. At no time should any PHPS employee provide their login or email password to anyone, not even family members.
3. All hosts that are connected to PHPS internal networks via remote access

technologies must use the most up-to-date anti-virus software, including personal computers.

4. Personal equipment that is used to connect to PHPS's networks must meet the requirements of PHPS-owned equipment for remote access.
5. Organizations or individuals who wish to implement non-standard Remote Access solutions to PHPS production network must obtain prior approval from PHPS.

Email Use

Refer to Administrative Procedure 80-05 Technology Acceptable Use.

Mobile Employee Endpoint Responsibility

This administrative procedure applies to any mobile device, or endpoint computer issued by PHPS or used for PHPS business which contains any stored data owned by PHPS.

- All employees shall assist in protecting devices issued by PHPS or storing PHPS data. Mobile devices are defined to include desktop systems in a telework environment, laptops, PDAs, and cell phones. Employees should limit the storage of PHPS data (such as email) on mobile devices, particularly those that are not issued by PHPS.
- Mobile computing and storage devices containing or accessing the information resources at PHPS should have proper screen locks (password or biometric) and be encrypted.
- Unless written approval has been obtained from PHPS, databases or portions thereof that reside on the network at PHPS **shall not be downloaded to mobile computing or storage devices. This includes personal computers, laptops, tablets and other devices**.
    - If approval is obtained, portable computing devices and portable electronic storage media that contain confidential, personal, or sensitive PHPS information must use encryption or equally strong measures to protect the data while it is being stored.
- Technical personnel and users, which include employees, consultants, vendors, contractors, and students, shall be made aware and confirm awareness that compliance with the all applicable policies, procedures, and standards related to mobile and personal computing devices is mandatory.

Risk Assessment

Risk assessments (RAs), which may include threat/risk assessments, privacy impact assessments or other assessments as necessary, shall be conducted on any new business process, system, application or service, if it involves the collection, use or disclosure of personal or otherwise sensitive personal information.

RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

Any risks identified by the risk assessment shall be mitigated by reasonable means that are effective for the purpose.

Privacy impact assessments shall be reviewed by the PHPS Freedom of Information and Protection of Privacy Act Coordinator or Privacy Officer, or by someone designated by that person.

Threat/risk assessments shall be reviewed by the manager responsible for information security for PHPS, or by someone designated by that person.

Employees are expected to cooperate fully with any risk assessment being conducted on systems, processes or services for which they are held accountable, and to assist in the development of any related risk mitigation plans or measures.

Workstation Security

Workstations include: laptops, desktops, PDAs, tablets and other computer based equipment containing or accessing PHPS information, including authorized home workstations accessing PHPS's network.

1. Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitivity information, including personal information as defined in the *Freedom of Information and Protection of Privacy Act*, health information as defined in the *Health Information Act* and student information as defined in the *Student Records Regulation*, as well as any other information of a sensitive or confidential nature.
2. Employees using workstations shall consider the sensitivity of the information that may be accessed and minimize the possibility of unauthorized access.
3. PHPS will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users (building security and valid access credentials).
4. Appropriate measures may include but are not restricted to:
    - Restricting physical access to workstations to only authorized personnel.
    - Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
    - Enabling a password-protected screen saver with a short timeout period to ensure that workstations that are left unsecured will be protected.
    - Complying with all applicable password policies and procedures.
    - Ensuring workstations are used for authorized business purposes only.
    - Never installing unauthorized software on workstations.
    - Storing all sensitive information, including all personal information, on network servers, not local drives, whenever possible.
    - Complying with all applicable encryption requirements.
    - Ensuring that anti-virus and anti-malware programs are running and up to date.
    - Ensuring that monitors are positioned away from public view.
    - If wireless network access is used, ensuring that access is secured using appropriate security measures and standards, such as Wi-Fi Protected Access (WPA) or a virtual private network (VPN).

Passwords

All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed annually.

All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least annually.

Passwords must not be inserted into email messages or other forms of electronic communication.

All passwords shall have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)

- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+=VIIH:";'<>?,./)
- Are at least 8 alphanumeric characters long
- Are not a word in any language, slang, dialect, or jargon
- Are not based on personal information
- Are never written down or stored on-line unencrypted
- Are never shared

Application Service Providers (ASP)

Any business process, system or application that is proposed to be outsourced to an ASP must be evaluated against the following:

1. In the event that PHPS data or applications are to be hosted or affected by an ASP, a binding contract with the ASP must fully specify the privacy and security measures to be employed to ensure that ASP services provide a level of protection equivalent to that provided by PHPS itself.
2. If the ASP provides confidential information to PHPS, PHPS is responsible for ensuring that any obligations of confidentiality are satisfied. This includes information contained in the ASP's application. PHPS's Business and Communications Services should be contacted for further guidance if questions about third-party data arise.

Unacceptable Use

Refer to Administrative Procedure 80-05 Technology Acceptable Use.

General Network Access Requirements

All wireless infrastructure devices that reside at a PHPS site and connect to the Internal PHPS networks must:

1. Be installed, supported, and maintained by the PHPS Information Technology Services (ITS) team.
2. Use PHPS approved authentication protocols and infrastructure.
3. Use PHPS approved encryption protocols (SSL & VPN)
4. Not interfere with wireless access deployments maintained by the PHPS ITS team.

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)
School Act, Student Record Regulation
Policy 23 Information and Technology
AP 80-05 Technology Acceptable Use
AP 80-11 Information Security Breach
AP 80-20 Mobile Devices (Employees)
AP 30-50 Records Management
AP 30-55 Record Retention Schedule