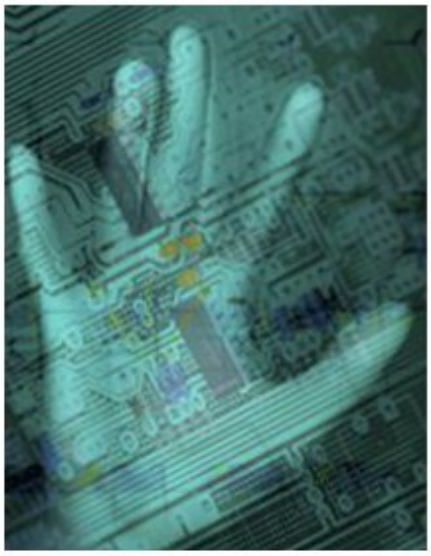
ATTACHMENT #3

Horizon School Division

PROTECTION OF PERSONAL INFORMATION ADMINISTRATIVE GUIDELINES



INTRODUCTION

Section 38 of the FOIP Act requires a public body to protect sensitive and confidential information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction. These guidelines and procedures address Horizon's privacy obligations regarding the protection of personal information and specifically the security of digital data on portable computing devices (e.g. laptop computers) and portable storage devices (e.g. USB sticks), and web based applications. Furthermore, it makes specific recommendations to reduce such risks.

Practices within Horizon School Division regularly include the collection of confidential student information (e.g. student names, addresses, phone numbers, grades, etc), which are backed up (in some cases off-site) to comply with data redundancy and disaster recovery guidelines. Teachers and especially administrators and counselors regularly store sensitive information on personal USB sticks or utilize the synchronization utility on their laptops to transfer data between servers and local hard drives. When these devices are then transported off site, data is at risk of a privacy breach should the device be lost or stolen.

Computing devices, such as laptops, as well as storage media, such as CDs, DVDs, and USB drives, all have the potential of falling into the wrong hands, particularly when they are not stored in a secure location. The highly publicized case in England where 25 million people's sensitive and confidential information was compromised as well as other high-profile privacy rulings relating to the inappropriate disclosure by a public body of sensitive and confidential information located on lost or stolen portable storage devices (e.g. USB sticks and laptop computers) has compounded the need to address this issue. In these rulings, the courts found that loss and theft of portable computing and storage devices are well known and publicized, making the risk real and foreseeable. Password protection while an essential part of a data security plan is not adequate protection by itself.

DEFINITIONS:

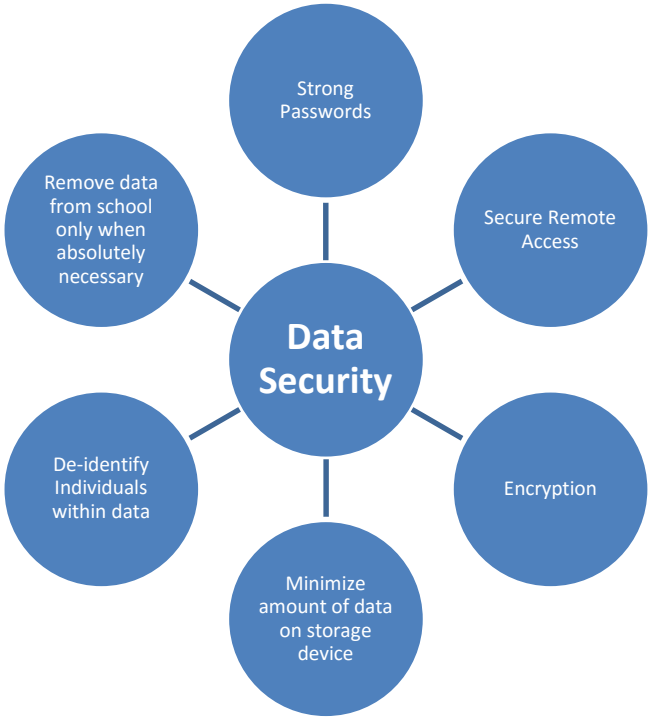
The term personal information is a critical element within the FOIP Act. The definition according to the Act follows:

Personal Information means recorded information about an identifiable individual, including

(a) the individual's name, home or business address or home or business telephone number,
(b) the individual's race, national or ethnic origin, colour or religious or political beliefs or associations,
(c) the individual's age, sex, marital status or family status,
(d) an identifying number, symbol or other particular assigned to the individual,
(e) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,
(f) information about the individual's health and health care history, including information about a physical or mental disability,
(g) information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given,
(h) anyone else's opinions about the individual, and

(i) the individual's personal views or opinions, except if they are about someone else; (Alberta Queen's Printer, 2009)

Protecting personal information consists of six key activities (shown in the schematic and described in more detail below).



Encryption: Any procedure used in cryptography to convert plain-text into cipher-text in order to prevent anyone except the intended recipient from reading that data. There are many types of data encryption, and they are the basis of network security.

Encryption Key: A sequence of characters used by an encryption algorithm to encrypt plain-text into cipher-text.

Key Management: In cryptography, keys are required for decipherment and authentication. These procedures provide no security when the keys have been handled incorrectly. Key management implies the effective creation, storage, transmission, installation and eventual destruction of keys

Https: The protocol for accessing a secure Web server. Using HTTPS in the URL instead of HTTP directs the message to a secure port number rather than the default Web port. The session is then managed by a security protocol.

Secure Remote Access (VPN): A virtual private network (VPN) is a private data network that makes use of public infrastructure, maintaining privacy through the use of a tunnel protocol and security procedures.

GUIDELINES

1. The Board of Trustees shall designate the Superintendent of Schools as Head for Horizon School Division. The Head is responsible and accountable for all decisions taken under the FOIP Act and has the authority to delegate duties to comply with this Act.

2. The Board of Trustees shall designate the Secretary-Treasurer as Coordinator for Horizon School Division. The FOIP Coordinator will perform the administrative duties required within this Act for Horizon School Division's operations.

3. Students, parents, Horizon School Division employees, independent service contractors, and vendors provide personal information to Horizon School Division with the understanding that the Division will use the information only as necessary to carry out the Division's mandate

4. All information must be maintained in confidence and disclosed only if authorized by regulation or law including, but not limited to, the Education Act, the Freedom of Information and Protection of Privacy Act, the Child Welfare Act, and the Income Tax Act.
    a. All digital images and recordings of an individual at school during the course of regular school day activities become a collection of personal information and therefore must comply with the Freedom of Information and Protection of Privacy (FOIP) Act.
    b. At events open to the public, Horizon School Division cannot be reasonably expected to limit the recording and distribution of personal images.
    c. While at school and school sponsored functions, with the exception of independent students, parents must grant permission prior to the dissemination of student images and confidential information beyond the secure school or network environment of Horizon School Division.
        i. At the time a student registers at a school in Horizon School Division, the parent of the student shall be provided with the opportunity to give written consent for the publication of the student's name and photograph in school related activities and operation while a student in the Division.
    d. Only authorized persons may use, disclose, take, alter, copy, interfere with, or destroy information, and must do so according to law and Horizon School guidelines, procedures, and practices.

5. Records management guidelines shall be followed by schools and Division departments.

DATA STORAGE GUIDLINES

1. All records created by Horizon School Division employees in the course of their work are subject to the Freedom of Information and Protection of Privacy Act and are under the custody and control of the Division at all times.

a. The Freedom of Information and Protection of Privacy Act and the orders provided by the privacy commissioner set the standards for the security of personal information. The Board will administer the Freedom of Information and Protection of Privacy Act as legislated by the Province of Alberta.

2. The security of information has the potential of being compromised when the information is stored on portable devices, personal information devices or when the information is transported to and from the worksite.

    a. Each person using confidential information 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.

    b. Each employee is to ensure the risk of unauthorized disclosure of personal or other confidential information is minimized. Records that are maintained in digital format must comply with guidelines delineated in this document.

    c. The FOIP Act requires protection of personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction. School principals shall ensure that an adequate level of security is provided for all personal information that is in their control and custody and shall ensure that the staff they supervise are aware of their responsibility as outlined in the attachments within this policy.

        - Confidential **data should be retained and removed from schools only when necessary**.
        - When retention is required, **data should be password protected and encrypted whenever it is stored in locations that are not physically secured with physical and technical access controls appropriate to the sensitivity of the data**.

            - The purpose of encryption is to prevent unauthorized access to confidential or sensitive information while it is either in storage or being transmitted.
            - In order to accomplish this, proper key management is crucial. If a key gets into the wrong hands, unauthorized access to information can result. Conversely, if a key is lost or destroyed, critical information may become unavailable to authorized personnel. Care should be taken to ensure the integrity of the key repository. This repository is confidential data in itself, so strong protections and access control, must be implemented. Encryption is not, however, a panacea. It is not a substitute for other security measures, such as authentication, authorization, and access control, and must be used in conjunction with other measures including:

- Keeping the **amount of** sensitive and confidential **information** stored **on** mobile computing and storage **devices to a minimum**, based on need;
- De-identification of sensitive and confidential information if possible (e.g. removal of identifying characteristics such as name);
- **Not using the synchronization process, or if utilized, configuring the process so that only a limited number of files are transferred**, containing current works in progress, thereby reducing the amount of information on laptops to essential data;
- **Protection of files and folders by not sharing logon passwords** and in the case of cloud storage (e.g. Dropbox, Google drive), not sharing account usernames and or passwords.
- Ensuring that the portable device is **labeled with appropriate contact information** in the case of loss;
- Ensure portable storage devices are **not left in non-secured areas**.

ENCRYPTION

Microsoft Windows includes the ability to encrypt data directly on volumes that use the NTFS file system so that no other user can use the data. You can encrypt files and folders if you set an attribute in the object's **Properties** dialog box.

USB sticks can also be purchased containing vaults which can store encrypted data.

1. How files are encrypted
    a. Files are encrypted through the use of algorithms that essentially rearrange, scramble, and encode the data. A key pair is randomly generated when you encrypt your first file. This key pair is made up of a private and a public key. The key pair is used to encode and decode the encrypted files.
    b. If the key pair is lost or damaged and you have not designated a recovery agent then there is no way to recover the data.

2. How to encrypt a folder

    a. Although you can encrypt files individually, generally it is a good idea to designate a specific folder where you will store your encrypted files, and to encrypt that folder. If you do this, all files that are created in or moved to this folder will automatically obtain the encrypted attribute.
        i. Locate and right-click the folder that you want, and then click **Properties**.
        ii. On the **General** tab, click **Advanced**.
        iii. Click the **Encrypt contents to secure data** check box, and then click **OK**.
        iv. In the **Confirm Attribute Changes** dialog box that appears, use one of the following steps:
            - If you want to encrypt only the folder, click **Apply changes to this folder only**, and then click **OK**.

- If you want to encrypt the existing folder contents along with the folder, click **Apply changes to this folder, subfolders and files**, and then click **OK**.

b. The folder becomes an encrypted folder. You will know if files are encrypted as they will appear green. Note that this does not prevent others from viewing the contents of the folder. This prevents others from opening items in the encrypted folder.

3. How to encrypt a USB stick

   a. Although you can encrypt files individually, generally it is a good idea to designate a specific folder where you will store your encrypted files, and to encrypt that folder. If you do this, all files that are created in or moved to this folder will automatically obtain the encrypted attribute.
   b. **NOTE**: You can encrypt files and folders only on volumes that use the NTFS file system. Since USB sticks typically are formatted as FAT or FAT32 the first thing to do is reformat them to NTFS.
      i. Right-click **USB drive** [e.g. Kingston (E:)] and click on **Format**.
      ii. Locate **File System** and change from **FAT to NTFS**, click **OK**
      iii. You can now create and encrypt folders on the USB device similar to folders. (See "How to encrypt a folder" above for details.)
   c. Note: the encrypted USB stick as done above will only allow that USB stick to be used on computers that are logged in with your username and password. If you go to a different computer (e.g. your home computer and log one with a different account you may not be able to open the USB stick. To encrypt a USB and allow it to open on multiple computers you may need to purchase USB sticks that have encryption built into them.

4. How to encrypt data within Dropbox

   a. While third party cloud storage providers such as Dropbox encrypt data there have been data breaches reported in the past. To mitigate the likelihood of confidential data being accessed when entrusted in third party data storage solutions it is strongly encouraged to:
      i. Limit the extent of confidential data stored in the cloud
      ii. When stored provide a second level of encryption under the control of the owner of the data. Third party products such as Secretcrypt (https://getsecretsync.com/ss/) will encrypt data prior to being placed and synced via Dropbox.

5. Encryption of data within other service providers
   a. Staff storing confidential data on external service providers hardware should be cognizant of the level of encryption provided.
   b. Google drive for instance is the same level of encryption as gmail.

c. Sites lacking adequate levels of encryption should not be utilized to store confidential data

STRONG PASSWORDS

"PASI" means the Provincial Approach to Student Information and entails an application maintained by Alberta Education. PASI is jointly controlled by multiple parties and all users who have access to PASI have access to Alberta students' confidential information. As such, all parties require a common understanding around the protection of this confidential information.

PASI requires Horizon to enter into a "PASI Acceptable Usage Agreement" which requires us to have an "Information Security Guidelines" which addresses the need for the protection of personal information.

To comply with the provincial "PASI Acceptable Usage Agreement" all those Horizon employees whom have access to personal information as defined under FOIP are required to implement physical and technical safeguards for all workstations that access electronic protected information.

Jurisdictions will implement physical and technical safeguards for all workstations that access electronic protected information. Appropriate measures should include:

- Restricting physical access to workstations to only authorized personnel. Securing workstation (Ctrl-Alt-Del and click on lock) prior to leaving area to prevent unauthorized access.
- Enabling password protected screen savers with short timeout periods (15 minutes) to ensure unattended workstations will be protected

Passwords are a means of controlling access to information. Unauthorized access can compromise information confidentiality, integrity and availability resulting in liability, loss of trust or embarrassment to Horizon School Division. Staff are expected to use strong passwords and ensure password confidentiality and protect the data within the Horizon School Division Network.

Strong Password: A strong password is constructed so that another user or a "hacker" program cannot easily guess it. It is typically a minimum number of characters in length and contains a combination of alphabetic, numeric, or special characters. Combine short, unrelated words with numbers, special characters, or mixed case. For example: eAt42peN

Password requirements:

All passwords, including initial passwords, must be constructed, implemented, and maintained according to the Horizon School Division password guidelines. Password guidelines vary dependent on the User within the Horizon School Division Network.

All passwords must

- Be treated as confidential information (Are never shared except with admin or tech support when required)
- Be changed immediately if the security of the password is in doubt (compromised or you are aware others know it)
- Be encrypted when stored or transmitted.
- Contain both upper and lower case characters (i.e. a-z, A-Z) as outlined in the table below
- Have digits as well as letters (i.e. 0-9) as outlined in the table below
- Are at least 5 alphanumeric characters long
- Not be written down in an unsecured locaton
- Never be shared, and when protecting confidential information should be unique to that account (do NOT use a generic password that is used for nonwork purposes).

Those with access to highly confidential information (school secretaries, principals, and counselors) are encouraged to change their passwords on a regular bases (etc yearly)

Passwords should not be easily related to such personal information as:

- Your logon Name or employee ID
- Your nickname
- Your social security or driver's license number
- Your birthday
- Word or number patterns such as aaabbb, zyxwvut, 123321, etc.
- Obscenities
- School names, school mascot, or school slogans
- Being the same as other passwords selected for personal use outside of the office, or passwords commonly used on public web sites.

The following chart specifies the password complexity requirements for different users' accounts:

	Minimum Length	Complex Password	Minimum Alpha Characters (Letters)	Minimum Upper Case Alpha Characters (Letters)	Minimum Digits (Numbers)	Minimum Special Characters
System Accounts	8	Yes	1	1	2	1
Senior Admin Staff and Trustees	8	Yes	1	1	1	0
Administrators, Admin Support Staff, and Teaching Staff	8	Yes	1	1	1	0
Other Staff	8	Yes	1	0	1	0
K-6 Students	5	No	1	0	0	0
6-12 Students	8	Yes	1	0	1	0

Constructing a Strong Password

To construct a strong password staff and gr. 7-12 students must use the first three of the following character sets and have a minimum of 10 characters:

- Upper case alpha characters/letters (A – Z)
- Lower case alpha characters/letters (a – z)
- Numbers (0-9)
- Special Characters (#$%&* etc.)

It is recommended that one think of using pass phrases as opposed to passwords. Here are some examples of what constitutes a complex password:

1L0veh0r1zoN! Myd0giSwh1te Gre@tnew5!

Application Password Information

The application environment within the Horizon School Division consists of applications that authenticate to Active Directory and some that use different authentication methods that are dependent on what the particular technology allows.

In most cases, the password does not display while it is being entered. Applications hosted on the jurisdiction network have not been written to enforce a strong password. Now that password standards have been defined, the long term plan is to configure applications to authenticate against Active Directory, and to enforced password guidelines through those services.

This is a more efficient and reliable means of ensuring consistency in standards than having each application enforce standards independently. Currently applications that do not support active directory authentication must comply with existing policies and need to be enforced by the department identified as responsible for the system(s) in question.
Staff's Signature

PASSWORD PROTECTED SCREEN SAVER

Must be employed by: Senior Administrative Leadership Team, School Administration, SIS operators, and Classroom Support Teachers. This is essential for mobile devices which provide access to confidential information via email.

Windows XP

- Right Click – chose "properties" from menu
- Click "Screen Saver" tab – found along the top
- Click the down arrow and chose the screen saver you want
- Check the box "on resume, display logon screen"
- Set the time for screen saver to come on – maximum time of 30 minutes

Windows 7

- Right Click – chose "personalize" from menu
- Click "Screen Saver" – found in bottom right corner
- Click the down arrow and chose the screen saver you want
- Check the box "on resume, display logon screen"
- Set the time for screen saver to come on – maximum time of 30 minutes

IPhone Password

- Click "settings"
- Click "general"
    - Set auto-lock to 5 or less minutes
    - Turn "passcode lock" on

DATA ACCESS GUIDELINES

1. The right to access information and the protection of privacy shall be managed in compliance with the FOIP Act.

    a. A fee shall be assessed prior to processing a FOIP application for general records.

    b. Fees for a FOIP applicant requesting his/her own personal information shall be restricted to the cost of providing a copy of the information.

2. Network access is controlled through the use of login passwords. Because such passwords provide access to staff domains and sensitive and confidential student information such **passwords should be considered confidential**, even when no confidential data is being accessed or transmitted. Many technology department login

passwords provide greater access to Horizon's network and should also be considered confidential.

3. Computing devices containing or having access to sensitive and confidential information should be protected with **strong login passwords** (see Appendix C) and utilize further security features such as **password protected screen savers** (see Appendix D).

DATA TRANSMISSION GUIDELINES

1. Schools should ensure appropriate security protocols are in place whenever confidential data is removed or accessed off site. This includes **encryption** of confidential data but should also include a **determination on whether it is even necessary for such information to be removed from the control of the school jurisdiction** (e.g. should the data be stored on a USB stick, on a laptop, or in the cloud to begin with?).

2. The jurisdiction must **restrict unsanctioned onsite wireless internet and network access points** within the jurisdiction. Such connections if not secured provide ideal access points for hackers to access network data.

PRIVACY BREACH

1. School Principals and Division managers shall work with the FOIP Coordinator when issues arise under the scope of the FOIP Act including a determination for the need to notify those individuals whose personal information was subject to inadvertent disclosure.

    (a) Employees shall report incidents (loss, theft, or unauthorized access of personal information and other security incidents) involving personal information immediately to their supervisor and the Horizon FOIP coordinator.

In the event of a privacy breach (lost or stolen device and or confidential data), employees should immediately contact the Jurisdiction FOIP coordinator (John Rakai – Associate Superintendent) who will respond to the breach by:

- **Evaluating the risks** associated with the breach, including a **determination on whether notification is necessary** to avoid or mitigate harm to a student or employee;
- **Investigate the cause** of the breach;
- **Inform** Horizon's FOIP coordinator (John Rakai);
- Develop or **improve** adequate long term **safeguards** against further breaches. Such alterations and/or additions to the safeguards should be communicated to all Horizon employees.