HORIZON SCHOOL DIVISION

POLICY HANDBOOK

Policy Code:	JB
Policy Title:	Freedom of Information and Protection of Privacy (FOIP)
Cross Reference:	GAA, HG
Legal Reference:	FOIP Act and Regulation
Adoption Date:	March 16, 1999
Amendment or Re-affirmation Date:	**February 26, 2024**

POLICY

THE BOARD OF TRUSTEES OF THE HORIZON SCHOOL DIVISION ACCESS, COLLECT, USE DISCLOSE, AND DESTRUCT INFORMATION AS LEGISLATED UNDER THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT.

GUIDELINES

1. In accordance with section 95 of the Freedom of Information and Protection of Privacy Act, the Board designates the Superintendent as "the head of the local public body for the purposes of this Act" and gives authorization to perform all duties and exercise all functions associated with that designation.

   1.1. The Superintendent is authorized to delegate, in accordance with section 85 of the Act, these duties and functions as required.

2. Staff are 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 the data storage, access and transmission guidelines delineated in the Policy Attachment Confidential Data Security Guidelines.

3. Digital citizenship is addressed in policy HG.

4. Staff are expected to handle confidential information in an appropriate manner as per policy GAA (Code of Conduct).

REGULATIONS

1. The division is authorized and required under the provisions of the Education Act and its regulations, in accordance with the Freedom of Information and Protection of Privacy Act (FOIP), to access, collect, use and disclose the personal information necessary to provide an educational program and ensure a safe and secure school environment for students.

   1.1. Requests to access routinely available information should be made directly to the appropriate school or department.

   1.2. In most cases, the school or department can provide the information requested as long as it does not compromise personal privacy and other restrictions or limitations within FOIP. If information is withheld, and the explanation for why it was not accessible is unsatisfactory, individuals can apply for access under FOIP.

1.3. Please send the completed request to:

Horizon School Division
Attention FOIP Coordinator
6302 56 St
Taber, AB T1G 1Z9

1.4. A fee shall be assessed and communicated to the applicant requesting information prior to processing a FOIP application for general records.

1.4.1. 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. Records management guidelines shall be followed by staff and volunteers who have access to personal information.

3. 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.

4. School principals and division managers shall work with the FOIP Coordinator when issues arise under the scope of the FOIP Act.

Horizon School Division

CONFIDENTIAL DIGITAL DATA SECURITY GUIDELINES

(ATTACHMENT TO POLICY JB FOIP)

INTRODUCTION

Section 38 of the FOIP Act requires a public body to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction. This discussion paper addresses, Horizon's privacy obligations regarding the security of personal information on Horizon's network, and specifically the security of such information on portable computing devices (e.g. laptop computers) and portable storage devices (e.g. USB sticks). Furthermore, it makes specific recommendations to reduce such risks.

Practices within Horizon regularly include the storage of personal information (e.g. names, addresses, phone numbers, grades, health information etc.) which may be regularly backed up or stored on portable devices and/or become accessible off site. Backups can be misplaced, taken off site, and stolen. Outdated or obsolete storage devices can be disposed of incorrectly, without ensuring destruction of the personal information (this includes photocopiers). Staff may store personal information on personal USB sticks or utilize the synchronization utility on their laptops to transfer data. When these devices are then transported off site, all files are at risk of a privacy breach should the device be lost or stolen.

Computing devices, such as laptops and 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 recent high-profile privacy rulings relating to the inappropriate disclosure by a public body of sensitive and confidential information located in 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. As such, password protection is not adequate. The Horizon Technology Department has made the following recommendations to safeguard privacy of personal information.

DEFINITIONS

Personal Information: recorded information about an identifiable individual that may include but is not limited to: name, age, grade, address, phone number, etc. E.g. include: student records, report cards, attendance reports, health records, photographs, completed forms. As part of the school's focus on digital citizenship, students should be taught to limit, and consider the privacy implications of, sharing their personal information online.

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.

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.

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

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

DATA STORAGE Guidelines

- Personal information **should be retained and removed from schools only when necessary**.
- When retention is required, **data should be 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 (see Appendix B)**. 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/password 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** personal **information** stored **on** mobile computing and storage **devices to a minimum**, based on need;
    - de-identify personal 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**, or utilizing remote access thereby reducing the amount of information on laptops.

DATA ACCESS GUIDELINES

- Network access is controlled through the use of login passwords. Because such passwords provide access to personal information such **passwords should be considered confidential**, even when no personal information is being accessed or transmitted.
- Computing devices may have access to personal information and should be protected with **strong login passwords** and utilize further security features such as auto lock.
- Google Workspace for Education is a learning platform the division has chosen to provide an online environment for students and staff in which to communicate, collaborate and create. Google services used by the division include Gmail, Calendar, Drive, and Classroom. These accounts are different from publicly created Gmail accounts.
- Students should only have access to their digital accounts while they are division students. When students leave the division, they no longer have access to school accounts.

DATA TRANSMISSION GUIDELINES

- Schools should ensure appropriate security protocols are in place whenever personal data is removed or accessed off site. This includes **encryption** of personal information 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 or laptop to begin with?).
- Rather than storing and transporting personal information on portable computing or storage devices, it is recommended that **secure remote access be set up** for those who frequently require access to such information off site, so that the data remains secure on site and only remotely accessed through a virtual private network (VPN).

DATA PROTECTION

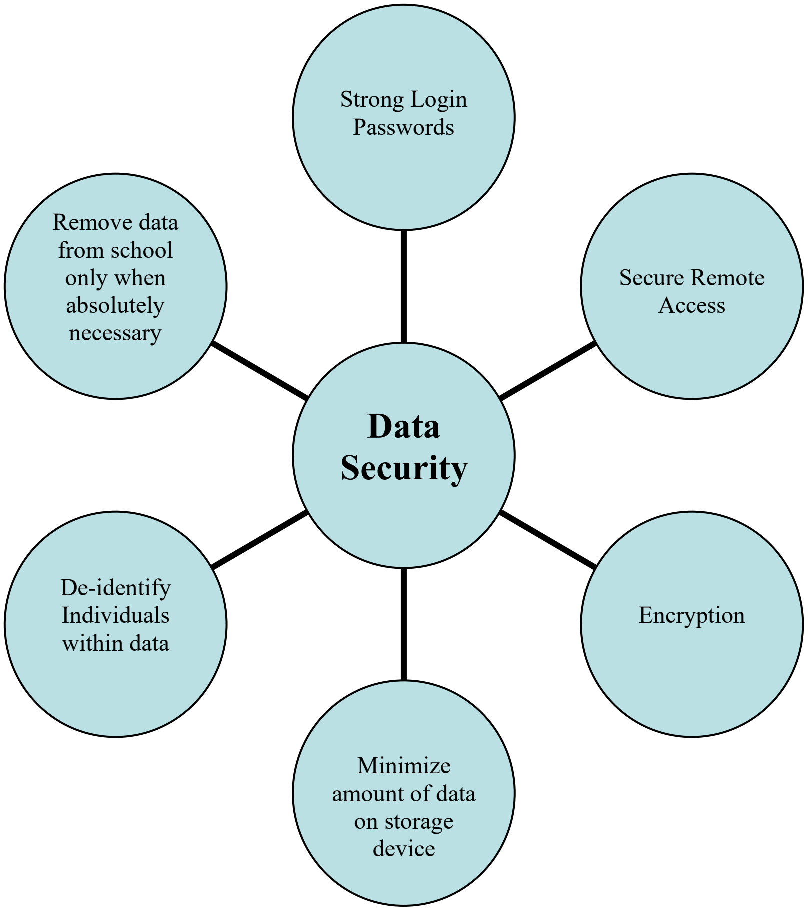
USB sticks can be purchased containing vaults which can store encrypted data).

- HOW FILES ARE ENCRYPTED
  - 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.
  - 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.
- HOW TO ENCRYPT A USB STICK
  - 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.
  - **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.
  1. Click **Start**, point to and click **Control Panel**, point to and click **System**.
  2. On the **Hardware** tab click **Device Manager.**
  3. Locate and click on **Disk Drives** and then locate and right-click on **USB Device** (e.g. Kingston Data Traveler 2.0 USB Device) and then click **Properties**.
  4. On the **Policies** tab, click **Optimize for Performance** and click **OK**.
  5. Close all windows.
  6. Click **Start**, point to and click **My Computer.**
  7. Right-click **USB drive** [e.g. Kingston (E:)] and click on **Format**.
  8. Locate **File System** and change from **FAT to NTFS**, click **OK**
     - You can now create and encrypt folders on the USB device.
     - See “How to encrypt a folder” on previous page for details.

- HOW TO ENCRYPT A FOLDER
  - 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.
  - **NOTE**: You can encrypt files and folders only on volumes that use the NTFS file system.
  1. Open **File Explorer.**
  2. Locate and right-click the folder that you want, and then click **Properties**.
  3. On the **General** tab, click **Advanced**.
  4. Under **Compress or Encrypt attributes**, select the **Encrypt contents to secure data** check box, and then click **OK**.
  5. Click **OK**.

6. 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.**

- PRIVACY BREACH
  - In the event of a privacy breach (lost or stolen device), employees and schools should immediately respond to the breach and:
    - **Evaluate the risks** associated with the breach, including a **determination on whether notification is necessary** to avoid or mitigate harm to a student or staff member;
    - **Investigate the cause** of the breach;
    - **Inform** Horizon's **FOIP coordinator** (Associate Superintendent of Finance and Operations);
    - Develop or **improve** adequate long-term **safeguards** against further breaches. Such alterations and/or additions to the safeguards should be communicated to Horizon's FOIP coordinator.


Strong Login Passwords
Secure Remote Access
Encryption
Minimize amount of data on storage device
De-identify Individuals within data
Remove data from school only when absolutely necessary
Data Security