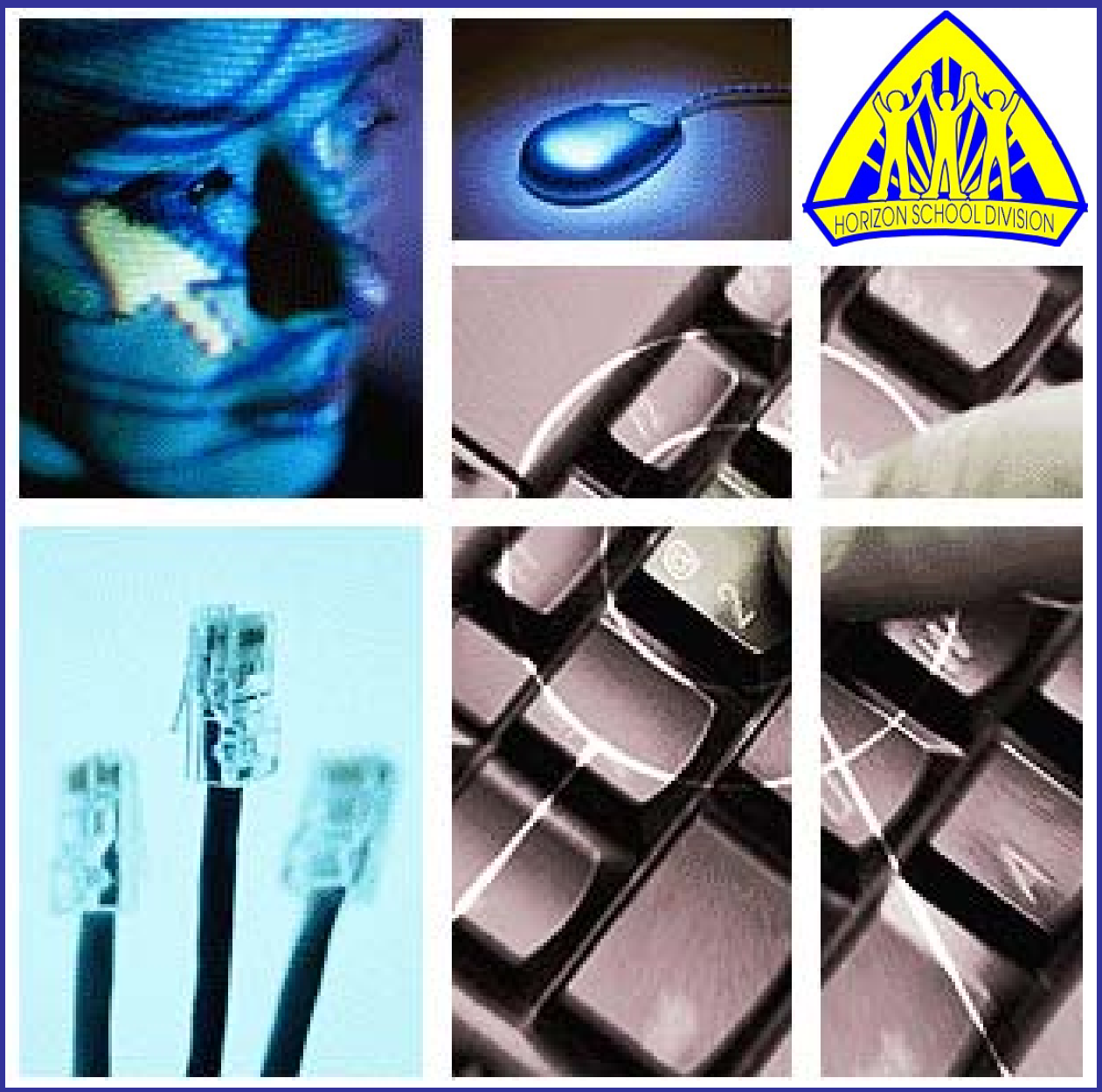
Horizon School Division # 67

CONFIDENTIAL DIGITAL DATA SECURITY GUIDELINES

(ATTACHMENT TO POLICY JB FOIP)



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. This discussion paper addresses, Horizon's privacy obligations regarding the security of confidential data on Horizon's network, and specifically the security of such data 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 confidential student information (e.g. student names, addresses, phone numbers, grades, etc) which have historically been backed up on tape drives, CDs, DVDs, and more recently memory sticks. In some cases these back ups have been misplaced, and/or taken off site. Often once outdated or obsolete the storage devices have been disposed of incorrectly, without ensuring the continued security of the confidential data. Teachers and especially administrators regularly store sensitive 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, PDAs, 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 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 sensitive and confidential information.

DATA STORAGE GUIDLINES

- Confidential **data 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 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.

DATA ACCESS GUIDELINES

- 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.
- Computing devices containing or having access to sensitive and confidential information should be protected with **strong login passwords** (comprised of at least 8 characters with 14 or more being ideal) and utilize further security features such as **password protected screen savers**.

DATA TRANSMISSION GUIDELINES

- 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 or laptop to begin with?).
- Rather than storing and transporting sensitive and confidential 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).
- It is also recommended that the jurisdiction **restrict onsite wireless internet and network access points** within the jurisdiction without technology department approval. Such connections if not secured provide ideal access points for hackers to access network data. If such devices are approved part of the security procedure must include having them deactivated unless specifically utilized (in use).

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** (John Rakai);
- 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.

APPENDUM A – DEFINITIONS

Confidential: The Classification of data of which unauthorized disclosure/use could cause serious damage to an organization or individual. See FOIP definition for further details.

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

Sensitive Information: Information that requires special precautions to protect it from unauthorized access, modification, or deletion. Sensitive information may be either public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness.

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.

APPENDUM B – 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).

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 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. Click **Start**, point to **All Programs**, point to **Accessories**, and then click **Windows 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**.

The folder becomes an encrypted folder. New files that you create in this folder are automatically encrypted. Note that this does not prevent others from viewing the contents of the folder. This prevents others from opening items in the encrypted folder. For example, if another user attempts to open a Microsoft Word document that has been created in the encrypted folder, the following message appears:

Word cannot open the document: *Username* does not have access privileges (*drive*:*filename*.doc)

If another user attempts to copy or move a document from the encrypted folder to another location on the hard disk, the following message appears:

Error Copying File or Folder
Cannot copy *Filename*: Access is denied.
Make sure the disk is not full or write-protected and that the file is not currently in use.

HOW TO SHARE ACCESS TO ENCRYPTED FILES

NOTE: You must be a member of the administrators group or the user that encrypted the file in to add users to it. If you are not authorized to add users to an encrypted file, you receive the following error message:

EFSADU
Error in adding new user(s). Error code 5.

You can retain the security of file encryption while allowing specific users access to your encrypted files. To allow access to your encrypted files:

1. Right-click the encrypted file, and then click **Properties**.
2. Click the **General** tab (if it is not already selected), and then click **Advanced**.
3. Click **Details**, and then click **Add**.
4. Select the user you want to share access to the encrypted file with, and then click **OK**.
5. When you are finished adding users, click **OK** three times.

Note Any user who can decrypt a file can also remove other users if the user who does the decrypting also has write permissions on the file.

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 Sytem** 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.