IT Standard Title:	Transmission and Sharing of Electronic Information
Standard ID:	US-103
Standard Type	User
Classification	Public
Linked to Policy:	6-604 Information Security Policy
Approved by CTO	2022-08-25
Revision Date(s):	2022-08-18 (Initial)
Effective Date:	2022-08-29
Next Review Date:	Annually
Contacts for Procedure Interpretation:	ITS Support Manager, IT Customer Services

1 – Purpose

All Fleming College electronic information that is electronically or physically transmitted is at risk of being intercepted and copied by unauthorized parties. Users of Fleming systems have a responsibility to protect this information, according to its classification level and safeguards described in the College's Information Security Classification Operating Procedure (OP #6-604A).

This document defines standards on how to transmit or share Fleming electronic information in a secure manner.

The Fleming College ITS Service Desk is available to assist users with any questions on how to securely transmit and share electronic information.

The Chief Technology Officer has issued this User Standard under the authority of College Policy 6-604 Electronic Information Security Policy.

2 – Sensitive Information Definition

As defined in the College's Information Security Classification Operating Procedure (OP #6-604A), the term **sensitive information** includes any information that has a classification level of Internal, Confidential or Highly Confidential as shown below.

Sensitivity	Colour	Classification Level
Sensitive	Red	Highly Confidential
Sensitive	Red	Confidential
Sensitive	Yellow	Internal
Non-Sensitive	Green	Public

In some cases the recommended and permitted methods of transmission and sharing will vary based upon the information classification level.

3 – Key Considerations when Transmitting and Sharing Information

Only transmit and share the minimum amount of information required to complete a task, also known as the principle of least privilege. Do not include any information that is not required. Where possible, do not share information that could be used to identify unique individuals. Do not include any confidential Personal Information (PI) unless there is a defined and approved business need to do so. (e.g., do not include Social Insurance Number and Date of Birth unless strictly required).

Sensitive information may be shared with other Fleming employees on a "need to know" basis when their role at Fleming requires them to have access to perform their duties.

Where possible, do not copy, extract, or download sensitive information from Evolve/PeopleSoft, or any other College system. If required to do so, the device used to store the downloaded information must meet the requirements described in the Information Security Classification Operating Procedure (OP 6-604A), Appendix B – Security Protections for Information Classification Levels.

It is also strongly recommended that a Fleming asset computer, laptop, or Fleming Virtual Desktop (VDI), be used by staff when working with sensitive College information. Personal or home computers may not have the appropriate safeguards in place to adequately protect Fleming's electronic information and other home users who share the device may have unauthorized access.

4 – Acceptable Methods of Transmitting and Sharing Fleming Electronic Information

The table below shows, for a given method of transmission, and the information's security classification level, if the method is acceptable, acceptable with appropriate safeguards and precautions, or not permitted.

Method of Transmission /	**per Information Security Classification levels:**			
	Public	**Internal**	**Confidential**	**Highly Confidential**
Fleming Email: Internal (to/from @flemingcollege.ca recipients)	Acceptable	Acceptable	Acceptable, when labelled as "Confidential".	Acceptable when labelled as "Highly Confidential". Strongly recommend the use of email encryption.
Fleming Email: External (to/from all other email domains)		Acceptable. Recommend the use of email encryption when large amounts of data are being	Avoid where possible. Acceptable only when email encryption is used.	Strongly discouraged in all cases. If absolutely required must use email encryption.

		sent.		
Fleming File Sharing & Collaboration Tools: (e.g. OneDrive, Microsoft Teams, SharePoint, Webex, Network shared folder)	Recommended (See further information below)			
Fleming Website(s) or Fleming Provided Website Hosting (e.g. Affinity, GitHub)	Recommended	Permitted with authentication and HTTPS (encryption)	Not Permitted (See Note 1 below)	
Removable Media or Storage Devices (e.g. USB drives, CD/DVD, tapes)	Acceptable	Discouraged, if required must be encrypted.	Not Permitted (See Section 7 below)	
Scan to Email	Acceptable	Acceptable	Strongly discouraged.	
Other Internet Transmissions (e.g. SSH, SCP, FTPS, SFTP)	Permitted with authentication and encryption connections (insecure internet transmissions e.g., telnet, FTP are not permitted.)			
Fax	Acceptable	Only when sending/receiving fax machines are in secure locations.		

Note 1: Not permitted by default and generalized stance unless otherwise authorized in writing for specific cases/instances, by the Data Trustee/OPI and CTO.

Electronic transfer of non-encrypted and personally identifiable information outside of the College via end-user technologies (i.e., e-mail, instant messaging, or SMS text message) is strictly forbidden when the transfer is not performed directly to the information subject.

5 – Email Encryption

Email is a ubiquitous tool for sending messages and attachments, but it does have some security pitfalls. Emails sent outside of the organization, (to non "@flemingcollege.ca" addresses), is comparable to sending a postcard in the mail, the contents of the message can be seen by those handling the message while in transit. It is also very easy to accidentally forward emails to unintended recipients. Once an email is sent, access to the information within cannot be revoked.

Because of these inherent security risks, the use of email ranges from recommended to strongly discouraged based on the information classification level, with requirements that email encryption is used in specific circumstances as per the table above.

There are two methods of email encryption available to Fleming users:

1) **Office 365 Message Encryption (OME)** is a service built into Fleming's Microsoft 365 email system. It allows any Fleming email user to easily send an encrypted email message to any recipient. This method protects the email attachments and body, but not the subject of the email itself. Refer to these instructions for usage details:

   Office 365 Message Encryption (OME) | Information Technology Services

(flemingcollege.ca)

2) **Encrypt the email attachment(s) using file-based encryption.**

   See Fleming IT Standard – Encryption Requirements (US-102), section 4 – File-Level Encryption Requirements, for recommended tools and instructions on how to encrypt files to be sent as an email attachment. Important notes when using this method:

   a) This method protects only the email attachments and not the body or subject of the email itself.
   b) **Key Exchange:** You will also have to securely exchange an encryption key/password with the recipient(s). Do not put the encryption key/password in the same email or email thread as the encrypted attachment. The best practice is to share the key "out-of-band" using a different form of communication such as secure chat.
   c) **Key Storage:** Encryption passwords/keys should be stored in a password manager/vault to retain a record for future use, such as anytime you need to re-open the encrypted file. See Fleming IT Standard – Password and Passphrase Requirements (US-101), section 11 – Password Manager Applications for recommended password manager/vault applications. If the individual is receiving encrypted files regularly, it is acceptable to use the same password/passphrase for all of the encrypted files, as long as it is changed at least once per year.

6 – Using Fleming File Sharing & Collaboration Tools

The following file sharing and collaboration tools can be used to securely share files and folder access. File-based encryption is not required as a means of transport when using these methods as the individual access is defined, revokable, and inherently secure as a method of transport.

Software Tool	Resources & Notes
OneDrive	Sharing Files and Folders in Office 365 | Information Technology Services (flemingcollege.ca) Sharing using the default "People you specify" option to explicitly define access to only the named users or groups. Sharing using OneDrive will grant ongoing access to the source files and/or folders until removed. Users with access can see future changes and co-edit documents if Edit access was granted.
Microsoft Teams	Share files in Teams (microsoft.com) Within the Teams application, right-click on a team name and select **Manage Team** to view the team Owners, Members, and Guests. These individuals will have access to some or all of the information, files, and folders within the Microsoft Teams space. Review the team membership with the team owner before sharing any sensitive information. Sharing using a Microsoft Team space provides ongoing access to the source files and/or folders until removed. Users with access will be able to see future changes and co-edit documents if Edit access was granted.

SharePoint	The information you store on a SharePoint site is usually available to everyone with permission to the site. The Site Owner(s) can add or delete users. Review the site audience with the site owner before using it to share any sensitive information. You can also share specific files or folders with people who don't otherwise have access to the site. When you share files and/or folders, you can decide whether to let people edit or just view them. Share SharePoint files or folders (microsoft.com) Sharing using these methods provides ongoing access to the source files and/or folders until removed. Users with access will be able to see future changes and co-edit documents if Edit access was provided. Creating a new SharePoint site requires some technical expertise. Please contact the Fleming ITS Service Desk before creating a SharePoint site. Fleming College strongly recommends that most end-users create a Microsoft Team site unless they have a specific requirement for a SharePoint "classic" site.
Microsoft Team (Chat)	Share files in Teams (microsoft.com) Within a one-to-one or group chat, use the attachment button to upload a local file into the discussion thread. Uploading a file transmits a copy of the file. You can also share links to files located in OneDrive, Microsoft Teams, or SharePoint, in which case the team or site permissions will also need to be granted for the recipient to be able to use the link.
Webex (Chat)	Within a one-to-one or group chat, use the attachment button to upload a local file into the discussion thread. Uploading a file transmits a copy of the file.
Network shared folder	Fleming uses a common S:\ drive (shared data) available to on-campus domain joined PCs and VDI desktops. Top-level folders are typically created for various departments, schools, committees, and other teams upon request to ITS Support. The folder's owner can grant and modify access as needed. Review the folder permissions with the folder owner before using it to share any sensitive information. To view a folder's permissions: **right-click** on the folder, select **Properties** and select the **Security** tab. Here you can see a list of all name user and groups who have access to the folder. When working remotely from the College or on WiFi, access to S:\ and H:\ drives is available using MyWorkDrive.

7 – Removable Media

Storing sensitive information on portable/removable media is not permitted, should be avoided where possible, and is only to be used when a defined legitimate business need to do so exists. If the use of removable media is necessary, device/media-level encryption is required as stated in the table above.

Due to the elevated risk of loss, theft, and inappropriate disclosure, the following safeguards must be implemented to secure removable media when not in use:

- Physical removable media must be stored in a secure & locked location, such as a room accessible only by staff with a key or access card.
- Physical removable media must be stored in a secure & locked container, such as a safe, file cabinet, or lockable desk drawer.

Transportation of Personal Information using removable media to other organizations, or third parties is not permitted and should be avoided where possible. If absolutely required, device encryption and a chain of custody log must be created, stored, maintained, and updated.

8 – Personal (Non-Fleming) Accounts

Fleming staff are not permitted to use personal (non-Fleming) accounts, not provided or authorized by Fleming College, to transmit or store college information that has a sensitivity classification level of Internal, Confidential, or Highly Confidential.

9 – Automatically Forwarding Fleming Email

Students: Students may forward their @flemingcollege.ca email address to any other external personal email address at their discretion.

Staff: Automatically forwarding or redirecting Fleming email accounts to non-Fleming accounts (”auto-forwarding”) is only acceptable for Fleming faculty and staff members who have appointments at other institutions and have difficulty managing multiple work email accounts. Under these circumstances, it is acceptable to auto-forward the Fleming email account to the email account at the other institution, provided that:

a) The other institution is a public sector institution located in Canada;
b) The other institution’s email system is at least as secure as Fleming’s email system; and
c) The staff or faculty member ensures that copies of emails of business value are returned to the Fleming email system so that they are managed as Fleming information records.

10 –Transmissions and Data Sharing with Third Parties

The term third parties includes but is not limited to any external organizations, partners, vendors, or service providers.

Before any Confidential, Highly Confidential is shared with third parties, users must ensure the recipient is compliant with the College’s Electronic Information Security Policy (#6-604), related operating procedures, and IT Standards. Contact the College’s IT Security team to determine compliance and if a Higher Education Community Vendor Assessment (HECVAT) is required.

Before any Personal Information (PI) is shared with third parties, users must ensure the recipient is compliant with the College’s Access to Information and Protection of Privacy Policy (#1-111). Contact the College’s Privacy Officer to review compliance and determine if a Privacy Impact Assessment (PIA) and/or HECVAT is required.

Before any Personal Health Information (PHI) is shared with third parties, users must ensure the

recipient is compliant with the College's Information Practices Related to Personal Health Information Policy (#1-112) and related operating procedures. Contact the College's Privacy Officer to review compliance and determine if a Privacy Impact Assessment (PIA) and/or HECVAT is required.

11 – Receiving Information from Third Parties

Individuals who are not Fleming employees, such as students, sometimes use insecure methods, such as personal email accounts, to transmit their information to Fleming College. While it is acceptable to receive information in this way, we should encourage these individuals to take measures to minimize their risk of interception by unauthorized parties, such as encrypting files.

Case Study: Receiving Emails from Students
Students sometimes send emails to their instructors containing personal information about themselves. It is acceptable for instructors to receive and respond to these emails, as long as they only do so using their Fleming email account. If the student wants to send or receive some sensitive information, such as a medical note, the instructor should encourage the use of encryption to ensure it is secure.

12 – Related Documents

- College Policy - Electronic Information Security Policy (6-604)
    - College Operating Procedure - Information Security Classification Operating Procedure (OP 6-604A)

- IT Standard - Password and Passphrase Protection (US-101)
- IT Standard - Encryption Requirements (US-102)

- Information Sensitivity Labels | Information Technology Services (flemingcollege.ca)
- Office 365 Message Encryption (OME) | Information Technology Services (flemingcollege.ca)
- Virtual Desktop (VDI) | Information Technology Services (flemingcollege.ca)
- MyWorkDrive | Information Technology Services (flemingcollege.ca)

- Advanced Encryption Standard (AES) | NIST
- FIPS 140-2, Security Requirements for Cryptographic Modules | CSRC (nist.gov)

- Educause - Higher Education Community Vendor Assessment Toolkit (HEVCAT) https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit

13 – History of Amendments & Reviews

N/A