FLEMING

IT Standard Title:	Bring Your Own Device (BYOD)
Standard ID:	US-107
Standard Type	User
Classification	Public
Linked to Policy:	6-604 Information Security Policy
Approved by CTO	2023-10-03
Revision Date(s):	2022-10-03 (Initial)
Effective Date:	2023-10-03
Next Review Date:	Annually
Contacts for Procedure Interpretation:	ITS Support Director, ITS

1 – Purpose

Fleming students and staff often study and work using personal computing devices belonging to the individual, not the college. This practice is commonly known as Bring Your Own Device (BYOD).

This standard defines the responsibilities and expectations of Fleming users when studying or working from a personal BYOD device, both on and off campus.

Fleming's electronic information is generally more at risk of being compromised, corrupted, or lost when accessed using a BYOD due to:

- the vulnerability of laptops or other mobile devices to theft or loss;
- the risk of unauthorized persons accessing the device; and
- unintentional storage or retention of information on BYOD devices without the user being aware (e.g. file downloads, browser cache, etc.)

Fleming College students and staff have different levels of access to college information and services. This document will differentiate between the two groups as needed when describing the various secure access methods and practices.

The Fleming College ITS Service Desk is available to assist users with questions related to configuring BYOD devices according to this standard and any system or application settings required to access Fleming's IT resources.

The Chief Information Officer has issued this User Standard under the authority of the college's IT Policy Framework 6-600.

2 – BYOD System Requirements

The system requirements below provide a general-purpose **minimum** recommendation for computer hardware and software required to access and utilize the college's IT resources. Some academic programs may have other more specialized requirements. Consult the academic program guide for these requirements where they exist.

Operating System	Windows 10 or 11 (64-bit) macOS 10.15 (*)
Processor (CPU)	Intel: Core i5 @ 1.6 GHz or greater AMD: Ryzen 5 @ 1.6 GHz or greater Apple Silicon: Any M series CPU
Memory (RAM)	8 GB minimum, (16 GB recommended)
Hard Drive (Storage)	128 GB of available space, (SSD recommended)
Display Resolution	Capable of High Definition Plus (HD+), 1600 x 900 pixels
External Display Output	Support for an external display connection via an HDMI port.
Network	Wireless (WiFi) adapter that supports wireless N.
Headset	Wired or wireless headset with microphone (or working laptop microphone and speakers).
Webcam	A webcam is required.
Internet Connectivity	Reliable access to Internet with at least 5 Mbps (upload and download) throughput speeds.
Virus Protection	An up-to-date antivirus client is required. Windows Defender is included with Windows 10 & 11 at no additional cost.

(*) Windows operating system is preferred as some academic software is not available for macOS.

Note: Chromebooks are not recommended as many of the college's software applications are not available for this platform.

3 – User BYOD Responsibilities

a) Be responsible for the security, care and repair of your device and peripherals.
b) Password protect your personal user account on your BYOD device with a strong password known only to you. Do not share BYOD passwords or login accounts. See IT User Standard US-101 – Password and Passphrase Protection for additional password guidance.
c) Enable hard drive encryption on your BYOD device, such as BitLocker for Windows or macOS drive encryption.
d) Enable the local firewall on your Windows or macOS device.
e) Keep your software up to date. The best way to achieve this is by enabling automatic updates for your operating system, virus protection and installed applications.

This responsibility is also described in the college's Appropriate Use Policy (AUP) #6-601 §5.8.f.

4 – Students - Secure Access Methods & Practices

Fleming students are strongly encouraged to have their own personal computer, or reliable access to one, for the duration of their academic studies. For some programs of study, this is a stated requirement. To protect a student's personal privacy and the confidentiality of their

Fleming account and related resources, we recommend students observe the following secure access methods and practices below:

a) Use a personal device that meets the **BYOD System Requirements** above. Other than on-campus college PCs, do not use any shared or public access computer terminals to access Fleming resources.
b) Use college web applications with built-in cloud storage where available. For example, Outlook Web Access and Microsoft Office Online. Using web applications avoids the need to download potentially sensitive/private information onto your device.
c) Use the college-provided OneDrive service to store and/or backup your college data.
d) To access files located on network drives such as H: or S: from a BYOD device, use the college's MyWorkDrive service.
e) Use the college's Virtual Desktop Interface (VDI) if is it offered as part of your academic program.

5 – Staff - Secure Access Methods & Practices

Fleming employees are generally provided with access to one or more of the following IT resources as part of their employment at the college:

- Access to an on-campus staff desktop computer (dedicated or shared).
- Assigned a college-provided laptop by the ITS Department.
- Assigned a college-provided smartphone by the ITS Department

Staff that have been assigned a college-provided laptop, (generally, this only applies to some full-time college staff), should use the laptop as their primary computing device both on and off campus. Laptops and smartphones provided the by ITS Department are pre-configured to meet the college's security requirement for mobile devices.

Staff may also choose to work from a BYOD device provided they adhere to the following secure access methods and practices:

a) Use a personal device that meets the **BYOD System Requirements** above. Other than on-campus college PCs, the use of shared or public access computer terminals to access Fleming resources is strictly prohibited.
b) Ensure that no other persons, (e.g. members of your household), have "local administrator" privileges on your BYOD device. This access could be used to compromise the confidentiality of your BYOD device login and local files.
c) Do not store any sensitive college information on your BYOD device.
d) Use college web applications with built-in cloud storage where available. For example, Outlook Web Access and Microsoft Office Online. Using web applications avoids the need to download potentially sensitive/private information onto your device.
e) To access files located on network drives such as H: or S: from a BYOD device, use the college's MyWorkDrive service.
f) Use the college's Virtual Desktop Interface (VDI) as a secure method of accessing sensitive college information from your BYOD device.
g) In some limited circumstances when required, staff are provided with Remote Desktop access to their on-campus staff desktop computer using a secure Virtual Private Network (VPN) connection.

6 – Physical Security

Reasonable measures should be taken to prevent or reduce the possibility of loss or theft of your personal property, especially valuable BYOD devices. Do not leave devices unattended in a public place, especially well-travelled areas. Keep devices secured when working from home and ensure sensitive college information cannot be accessed by other members of your household.

7 – Network Access

Only use trusted wireless (Wi-Fi) and wired networks when accessing college resources from your BYOD device. These include:

a) On-campus Wi-Fi services provided by the ITS Department;
b) Your personal and secure home network;
c) When travelling, only use wireless services provided by known and trusted entities such as your hotel operator, conference hosts, other higher education institutions or government services. Ask the host which wireless network name (SSID) is available for guest use and instructions to connect. Do not assume based on the wireless network name alone.

Staff who have been issued a college mobile phone should utilize the device's Wi-Fi mobile hotspot feature when travelling within Canada.

Access to some college IT resources is only available to remote users who first connect to the college's VPN service.

8 – Using Fleming File Sharing & Collaboration Tools

Consult the IT User Standard US-103 – Transmission and Sharing of Electronic Information for more information on approved and secure methods of file sharing and collaboration from your BYOD device.

9 – Email Access

Fleming strongly recommends using the Microsoft Outlook mobile app to access Fleming email from a smartphone or tablet device

Employees of the college are not permitted to use their home/personal email accounts to conduct college business. This is to protect home/personal resources from potential exposure to freedom of information requests.

10 – Telephone Services

Employees of the college are not permitted to use any home/personal communication resources, such as a home phone number, to communicate with students or suppliers. Staff who need to use telephony services to conduct college business should use one of the following college-provided IT services:

a) A college phone extension. Extensions can be remotely accessed from BYOD or college devices by using the Webex Calls within the Webex desktop application;

b) A Microsoft Teams Phone; or

c) A college mobile phone.

For all other voice, video or text chat with internal Fleming contacts, Microsoft Teams is the recommended application. Microsoft Teams can be installed on BYOD laptops and smartphones.

10 – Removable Media

The use of removable or portable media (USB sticks or drives) is strongly discouraged due to the likelihood of being lost or stolen.

To protect sensitive college information removable media may only be used for Internal college information if absolutely necessary and the removable media device must be encrypted. For Confidential and higher sensitivity information, the use of removable media is not permitted.

11 – Printing

Fleming College users can print from their BYOD devices using our Mobility Print service.

12 – Related Documents

- College Policy – Information Technology (IT) Appropriate Use Policy (AUP) (6-601)
- 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)

- Information Sensitivity Labels | Information Technology Services (flemingcollege.ca)
- Virtual Desktop (VDI) | Information Technology Services (flemingcollege.ca)
- MyWorkDrive | Information Technology Services (flemingcollege.ca)
- Network cyber security: An introduction - Get Cyber Safe
- Turn Microsoft Defender Firewall on or off - Microsoft Support
- Change Firewall settings on Mac - Apple Support (CA)
- Mobility Print | Information Technology Services (flemingcollege.ca)

13 – History of Amendments & Reviews

N/A