Frederick Community College

Technology Use
Policy and Procedures

BOT Approved:	10/21/2015
Revised:	4/13/2016
Revised:	6/30/2016
BOT Revised:	5/16/2018
Revised:	7/1/2019
Revised:	7/1/2020
Revised:	7/1/2021

Table of Contents

I. Philosophy and Scope ... 1

II. Definitions ... 1

III. Responsible Senior Leader and Responsible Office ... 2

IV. Entities Affected by this Policy and Procedures ... 2

V. Expectations for Technology Use ... 2

VI. Information Technology User Responsibilities ... 3

VII. Password Security ... 3

VIII. Email Use ... 4

IX. Website ... 4

X. Social Media ... 5

XI. Wired/Wireless Network ... 5

XII. Remote Access ... 5

XIII. College-Owned Mobile Phones ... 5

XIV. Classroom Technologies ... 6

XV. Public Access Computers ... 6

XVI. Data Confidentiality, Integrity, and Availability ... 6

XVII. Disposal of Surplus Technology ... 6

XVIII. Account Termination ... 6

XIX. Violations ... 7

XX. Related Policies and Procedures ... 7

Technology Use Policy and Procedures

I. Philosophy and Scope

Frederick Community College ("FCC" or the "College") is committed to creating a teaching and learning environment that supports the effective and innovative use of technology. This Policy and Procedures applies to anyone who uses College information technology (IT) resources and systems. The resources covered by this Policy and Procedures include, but are not limited to, computer hardware and software, mobile communication devices, telephone and data networks, College websites, and electronically stored data.

This Technology Use Policy and Procedures supports an information technology environment that meets the mission of the College in teaching, learning, and administration by promoting:

- Confidentiality, Integrity, reliability, availability, and performance of IT resources
- Assurance that IT resources are used for their intended purposes
- Procedures for addressing policy violations

The College reserves the right to extend, limit, restrict, or deny privileges and access to information technology resources and systems. All information technology users are bound by all applicable local, state, and federal laws. This Policy and Procedures identifies related College policies and procedures that are associated with appropriate use of technology resources and the protection of College data.

The College provides a wide range of IT resources to support the teaching and learning mission and actively protects the information technology environment. The College is not responsible for information and materials residing on non-College systems.

II. Definitions

A. **"Information technology (IT) resources"** refers to resources that include, but are not limited to, telephones, mobile devices, computers, printers, scanners, servers, networking devices, public access computers, and licensed software and services. These resources are often involved in the processing, storage, accessing, and transmission of data owned by, controlled by, or contracted to the College.

B. **"Information technology (IT) users"** refers to anyone accessing College information technology resources.

C. **"Personally Identifiable Information (PII)"** refers to data or information which includes, but is not limited to: an individual's name; the name of the individual's other family members; the address of the individual or individual's family; a personal identifier, such as the individual's social security number, identification number, or biometric record; financial data including student loans, banking information, credit card or credit information; other indirect identifiers, such as the individual's date of birth, place of birth, and mother's maiden name; other information that, alone or in combination is linked to a specific individual that would allow a person, who does not have personal knowledge or the relevant circumstance, to identify the individual with reasonable certainty; or information requested by a person whom the College reasonably believes knows the identity of the individual to whom the record containing PII relates.

D. **"Public access computer"** refers to computers provided for public use.

E. **"College social media account"** refers to accounts on any social media site specifically made to promote the College, or any related organizations, programs, departments, or activities. This policy does not apply to personal social media accounts used by College employees.

F. **"Systems"** refers to software applications, software platforms, computers, and/or devices. (e.g. PeopleSoft, Blackboard, Lumens, Office 365)

III. Responsible Senior Leader and Responsible Office

Chief Information Officer

Information Technology

IV. Entities Affected by this Policy and Procedures

All information technology users

V. Expectations for Technology Use

All IT users must act responsibly, ethically, and legally, and limit their use of IT resources to the educational purpose and legitimate business of the College. IT users are expected to abide by all College Policies and Procedures and the Employee Handbook.

Employees provided with College-owned IT resources may only use them for work-related activities.

The College reserves the right to monitor IT resources including activity and accounts, with or without notice, in order to protect the integrity, security, and functionality of IT resources. Normal operation and maintenance of College IT resources requires backing up data, logging activity, monitoring general usage patterns, and other activities as may be necessary to provide support for College operations.

Unacceptable use of IT resources or systems includes, but is not limited to, the following examples:

A. Use of IT resources or systems that violates local, state, or federal law or regulation;

B. Use of IT resources or systems that violates College Policies and Procedures;

C. Transmission and/or collection of College data, particularly sensitive data, to unauthorized and/or unapproved parties or systems (see the College Protection of Personally Identifiable Information Policy and Procedures for more information on appropriate use of PII);

D. Unauthorized attempts to alter College data files or systems;

E. Unauthorized access to email, voice mail, data, or systems;

F. Circumvention of any information security measure of the College;

G. Intentional use, distribution, or creation of malware, or other malicious software;

H. Use of any device, system, or method that negatively impacts the availability or integrity of College IT resources;

I. Use of IT resources that disable other IT resources, consume IT resources disproportionately in a way that other users are denied reasonable access, or materially increase the cost of IT resources;

J. Unauthorized installation, copying, or distribution of College-licensed software or copyrighted material (see the College Copyright Policy and Procedures);

K. Use of IT resources for commercial purposes or personal financial gain, with the exception of authorized use of the electronic Community Bulletin Board; and

L. Forwarding all College emails to circumvent the College email system (students excepted).

M. Sensitive PII data may not be stored directly on personal devices (see the College Protection of Personally Identifiable Information Policy and Procedures for more information on appropriate use of PII).

VI. Information Technology User Responsibilities

When using IT resources at the College, IT users are responsible for the following:

A. Protection of individual account passwords, with the exception of accounts created for approved College events (not applicable to public access computers);

B. Compliance with all laws governing copyright, intellectual property, libel, and privacy (see the College Copyright Policy and Procedures);

C. Adherence to the terms of software licenses and other contracts (questions about software license agreements should be directed to the IT Help Desk);

D. Obtaining authorization from the Director of Technical Support Services for any software purchase, download, or installation on College-owned equipment. Authorization is not required for installation of Microsoft Office on a personal device through the Microsoft Campus Agreement;

E. Use of College email by employees and trustees as the official means of electronic communication;

F. Immediate reporting of loss, damage, theft, or misuse of IT Resources to the Director of Technical Support Services; and

G. Logging off or locking devices or systems when not in use.

VII. Password Security

IT users provided with College accounts should protect their passwords at all times.

Sharing passwords is prohibited, with the exception of accounts created for approved College events. The College requires that passwords be changed periodically. IT users are also expected to change their password immediately if they know or suspect that their password has been compromised and to contact the IT Help Desk.

The IT Team will never solicit your password in any electronic communication and or ask you to click a link to keep your account. Any IT user unsure of the authenticity of a message should reach out to the IT Help Desk before opening attachments or websites.

VIII. Email Use

College email accounts serve as the official means of electronic communication. Employees and trustees may only use College email accounts when conducting College business. Employees and trustees may not use College email for personal use.

College IT users must be aware of the legal risks of using email. If any IT user sends or forwards emails with libelous, defamatory, offensive, discriminatory, harassing, or obscene material, the IT user will be held responsible and subject to College disciplinary policies. Sending fraudulent email messages is prohibited.

Employees may not use College email for mass broadcasting or the wide distribution of large attachments. Only the Chief Information Officer or designee may authorize users or systems to send mass distribution emails. Employees should be aware that email messages sent from an FCC email account to an account outside the College are not encrypted. This is of particular importance when sending any email that may contain PII. For information on encrypting email messages contact the IT Help Desk. (See the College Protection of Personally Identifiable Information Policy and Procedures.)

Students, employees, and trustees are expected to check their College email account regularly.

Only students may reroute delivery of College emails to an outside email address. If a student elects to reroute their College email to another email account, the student remains responsible for any material not received because of any problem in the forwarding mechanism or the destination account. Forwarding of all email coming into an employee’s email account is prohibited as it creates additional risk when information is no longer secured and maintained on College-owned or contracted IT resources.

IX. Website

The College website is the most prominent marketing tool for public-facing communications. It contains information for and about the College community and is a mechanism for communication, publication, and collaboration in support of the mission of the College. The College maintains oversight of all website access and content, including all official webpages and associated web-based services developed by or for the College. College website content is recognized as official published work.

Marketing is responsible for the website user experience. Any changes or modifications to website content require the submission of a Marketing Request Form and approval by the appropriate area supervisor. The College will ensure website accessibility for individuals with disabilities in accordance with the Americans with Disabilities Act.

X. Social Media

College social media sites and accounts serve as an additional means of electronic communication for the College. Use of College social media accounts is limited to authorized users for approved College business. Users must be aware of the legal risks of using social media. If any user posts comments with libelous, defamatory, offensive, discriminatory, harassing, or obscene remarks, the user will be held responsible. Creation or use of College social media sites and accounts requires approval by the Communications Coordinator. All College policies and procedures related to harassment, plagiarism, commercial use, security, unethical conduct, and laws prohibiting theft, copyright and licensing infringement, unlawful intrusions, and data privacy laws should be followed when using social media accounts. Student and employee personal social media accounts are not subject to this Policy and Procedures. Students' personal electronic accounts are addressed under the Student Personal Electronic Account Privacy Policy.

XI. Wired/Wireless Network

IT is responsible for the deployment, management, network protocols, frequencies, and bandwidth use of College networks. Installation of unauthorized network equipment is prohibited. Within all networks at the College, IT reserves the right to mitigate any unauthorized wireless access point or device in order to maintain the overall integrity of College networks. Unauthorized collection of data from College networks is prohibited. The Chief Information Officer or designee will review requests for authorization for these activities.

XII. Remote Access

Supervisors may request remote access to College IT resources for employees by contacting IT (e.g. internal file share, remote desktop). Senior Leaders review and approve remote access requests. When accessing the network, authorized users are responsible for preventing access to any technology resources or data by unauthorized users. The user accepts responsibility and consequences of misuse of remote access. Remote Access is not required for Office 365.

XIII. College-Owned Mobile Phones

The College may provide mobile phones for employees. Assigned employees are held accountable as per the College mobile phone protocol. See the Employee Handbook for more information. IT users must contact the IT Help Desk immediately if they believe a device is lost or stolen. IT is responsible for maintaining College-owned devices including updates and security settings.

XIV. Classroom Technologies

Computer classroom/labs are used by students currently enrolled in classes at the College or for approved College events. Employees and students are required to use their login credentials when using classroom/lab computers, with the exception of public access computers. Tampering with any technology in classroom/lab environments is prohibited. Students and employees should not store files on classroom/lab computers. Supported College systems should be used for this purpose (e.g. Office 365, OneDrive, Blackboard).

XV. Public Access Computers

Public access computers are available throughout the main campus and Monroe Center. Public access computers do not require login credentials.

XVI. Data Confidentiality, Integrity, and Availability

The College is committed to protecting data on any IT resource or system. The College is also committed to protecting the PII of all students, employees, and any other individual whose PII is collected by the College in carrying out its mission. For more information on PII, including guidance on PII use, see the College Protection of Personally Identifiable Information Policy and Procedures.

XVII. Disposal of Surplus Technology

IT resources that have no further benefit to the College, as determined by the Chief Information Officer, will be deemed surplus and appropriately disposed of by one of the following methods:

A. Donation to Frederick County Government, Frederick County Public Schools, or another State, County, or Municipal agency;

B. Trade-in on newly acquired equipment; or

Disposal as scrap by means of recycling or data destruction services. All hardware storage containing College data must have data securely erased or destroyed before disposal.

Computers with software purchased under the Maryland Education Enterprise Consortium (MEEC) licensing agreement will follow the rules set forth in the MEEC contract. Equipment or software purchased with grant funds will follow disposal guidelines as set forth by the grant.

XVIII. Account Termination

In the event of an employee's separation from employment, supervisors will follow the Exit Process for Separating Employees found in the Employee Handbook. Human Resources will initiate the request to IT for deactivation of the employee's accounts.

XIX. Violations

Any individual who becomes aware of an alleged technology resource violation has a responsibility to report it to IT by contacting the Chief Information Officer or the IT Security Officer. IT Users who violate this Technology Use Policy and Procedures are subject to College disciplinary policies.

XX. Related Policies and Procedures

Code of Student Conduct

Copyright

Employee Misconduct

Protection of Personally Identifiable Information

Student Personal Electronic Account Privacy