

## Table of Contents

<b>I.</b>	<b>Philosophy and Scope</b> .....	1
<b>II.</b>	<b>Definitions</b> .....	1
<b>III.</b>	<b>Expectations for Technology Use</b> .....	2
<b>IV.</b>	<b>Information Technology User Responsibilities</b> .....	3
<b>V.</b>	<b>Password Security</b> .....	3
<b>VI.</b>	<b>Email Use</b> .....	4
<b>VII.</b>	<b>Website</b> .....	4
<b>VIII.</b>	<b>Social Media</b> .....	4
<b>IX.</b>	<b>Wired/Wireless Network</b> .....	5
<b>X.</b>	<b>Remote Access</b> .....	5
<b>XI.</b>	<b>College-Owned Mobile Devices</b> .....	5
<b>XII.</b>	<b>Classroom Technologies</b> .....	5
<b>XIII.</b>	<b>Public Access Computers</b> .....	5
<b>XIV.</b>	<b>Data Integrity, Confidentiality, and Access</b> .....	6
<b>XV.</b>	<b>Disposal of Surplus Technology</b> .....	6
<b>XVI.</b>	<b>Account Termination</b> .....	6
<b>XVII.</b>	<b>Violations</b> .....	6

# 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. 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:

- integrity, reliability, availability, and performance of IT resources
- assurance that IT resources are used for their intended purposes
- procedures for addressing policy violations

Access to IT resources is a privilege, not a right or guarantee. The College reserves the right to extend, limit, restrict, or deny privileges and access to information technology resources. 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 or available over publicly accessible networks.

## 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. 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

## **Technology Use Policy and Procedures**

---

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 that do not require an FCC computer account to 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.

### **III. 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](#).

Employees provided with College-owned IT resources are expected to use the resources 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 includes, but is not limited to, the following examples:

- A. Use of IT resources that violates local, state, or federal law or regulation;
- B. Use of IT resources that violates [College Policies and Procedures](#);
- C. Transmission and/or collection of College data, particularly sensitive PII, to unauthorized and/or unapproved parties (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, or other communications intended for others;
- F. Circumvention of any information security measure of the College;
- G. Intentional use, distribution, or creation of viruses, worms, 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 copying or distribution of College-licensed software or copyrighted material (see the College [Copyright Policy and Procedures](#));

## **Technology Use Policy and Procedures**

---

- K. Access of data that is not publicly available, does not belong to the user, and for which the user does not have explicit permission to access;
- L. Circumvention of access limitations to IT resources ;
- M. Use of IT resources for commercial purposes or personal financial gain, with the exception of authorized use of the electronic Community Bulletin Board; and
- N. Rerouting the delivery of College emails to circumvent the College email system (students excepted).

### **IV. 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 department);
- D. Prior authorization from the Manager of User Services by contacting the IT Help Desk 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. Prior authorization from the Manager of User Services by contacting the IT Help Desk for any installation of College-owned software on personal devices;
- F. Good judgment and civility when using College IT resources; and
- G. Use of College email by employees and trustees as the official means of communication.

### **V. 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. For passwords related to services rather than individuals, contact the IT Help Desk for guidance and resources.

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.

# Technology Use Policy and Procedures

---

## VI. 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 may authorize the use of 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. (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 are allowed to reroute delivery of College emails to an outside email address. If a student elects to reroute his/her 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. Rerouting of College email by employees creates additional risk as the information is no longer secured and maintained on College owned or contracted IT resources.

## VII. 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.

## VIII. 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

## **Technology Use Policy and Procedures**

---

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](#).

### **IX. Wired/Wireless Network**

IT is responsible for the deployment, management, network protocols, frequencies, and bandwidth use of College networks. Within all networks at the College, IT reserves the right to mitigate any unauthorized 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 provides authorization for these activities.

### **X. Remote Access**

Supervisors may request remote access to College IT resources for employees by contacting IT. When accessing the network, authorized users are responsible for preventing access to any technology resources or data by non-authorized users. The user accepts responsibility and consequences of misuse of remote access.

### **XI. College-Owned Mobile Devices**

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

### **XII. Classroom Technologies**

Computer classroom/labs are for academic use by students currently enrolled in classes at the College or for approved College events. Employees are required to use their login credentials when using classroom/lab computers. Effective spring 2019, all students will be required to log in to classroom/lab computers, with the exception of public access computers. Tampering with any technology in classroom/lab environments is prohibited. Students should not store files on classroom/lab computers and are encouraged to store files within their Office 365 – OneDrive environment or other storage option.

### **XIII. Public Access Computers**

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

# **Technology Use Policy and Procedures**

---

## **XIV. Data Integrity, Confidentiality, and Access**

The College is committed to protecting the PII of all students, staff members, 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](#).

Supervisors approve access levels for their employees by submitting an IT support ticket. Employees using classroom/lab computers should save files to their network drives.

## **XV. Disposal of Surplus Technology**

Computer equipment that has 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
- C. Disposal as scrap by means of recycling.

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.

## **XVI. Account Termination**

In the event of an employee's separation from employment, supervisors will notify Human Resources who will initiate the request to IT for deactivation of the employee's accounts.

## **XVII. 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. [Employee](#) or [student](#) violators of this Technology Use Policy and Procedures are subject to College disciplinary policies.