Frederick Community College

Technology Use Policy and Procedures	BOT Approved: 10/15/2015 Revised: 4/13/2016 6/30/2016

Table of Contents

I. Philosophy, Purpose, and Scope 1

II. Acceptable Use 1

III. User Responsibilities 2

IV. Password Security 3

V. Email Use 3

VI. Web Policy 4

VII. Social Media 4

VIII. Wireless Network 5

IX. Remote Access 5

X. College-Owned Mobile Devices 5

XI. Computer Classroom/Lab Usage 5

XII. Data Security, Confidentiality, and Access 5

XIII. Disposal of Surplus Computer Equipment 6

XIV. Account Termination 7

XV. Violations 7

Technology Use Policy and Procedures

I. Philosophy, Purpose, and Scope

Frederick Community College ("FCC" or the "College") is committed to creating a teaching and learning environment that is supported through the effective and innovative use of technology. The College has the obligation to protect and guide students, faculty, and staff in the acceptable use of computer systems, networks, and other information technology resources. Access to these resources is a privilege, not a right or guarantee. As such, the College imposes certain responsibilities and obligations on the user. All users are expected to act responsibly, ethically, and legally, and limit their use of these resources to the educational purpose and legitimate business of the College. This Policy and Procedures applies to all information technology systems and services owned by the College and to all users. The College reserves the right to extend, limit, restrict or deny privileges and access to its information technology resources.

Users of information technology resources are expected to access, through any system, only information that relates to the performance of their duties and to exercise good judgment in the use of such information. All members of the College community are bound by all applicable local, state, and federal laws including, but not limited to, those related to copyright, security, privacy including the provisions of FERPA and other statutes regarding electronic media. The College complies with official requests for information made in accordance with the guidelines of the Maryland Public Information Act (MPIA).

The College provides a wide range of computing resources to support the teaching and learning mission of the College. However, the College makes no guarantee that the services provided will be error-free or without defect. The College cannot be responsible for any damage suffered including, but not limited to, loss of data or disruption of service. The College disclaims any responsibility and/or warranties for information and materials residing on non-College systems or available over publicly accessible networks.

II. Acceptable Use

In making technology resources available to all members of the College community, the College affirms its commitment to an open educational environment, conducive to learning, and governed by legal and ethical principles. The College respects individual privacy, civility, and intellectual property rights. Because an electronic environment is easily disrupted and electronic information is readily copied, users of College resources are expected to promote and protect these institutional standards.

The College reserves the right to monitor system resources, including activity and accounts, with or without notice, when:

- It is necessary to protect the integrity, security, or functionality of College technology resources.
- An account or system is engaged in unusual or excessive activity.
- It has good cause to believe that regulations, rules, or laws are being violated.
- In the event of health, safety, or security emergencies.

- When, due to the extended absence of an employee or separation from employment, as verified by the Associate Vice President (AVP) for Human Resources or other authorized College official, it is necessary to retrieve College-related material.

Additionally, the normal operation and maintenance of College computing resources requires the backup of data, the logging of activity, the monitoring of general usage patterns, and other such activities as may be necessary in order to provide desired services. Accordingly, all employees should use College-provided resources for College-related material only. Personal accounts and devices should be used for non-work-related activities.

Certain activities are prohibited per this Policy and Procedures. These include the following:

- Circumvention of any security measure of the College.
- Intentional use, distribution or creation of viruses, worms, or other malicious software.
- Unauthorized copying or distribution of licensed software or copyrighted material.
- Accessing data that is not publicly available, does not belong to the user, and for which the user does not have explicit permission to access.
- Accessing technology resources in a manner designed to circumvent access limitations to public or restricted-access data without permission.
- Use of technology resources for organized political activity.
- Use of technology resources that disables other technology resources, consumes disproportionate technology resources such that other users are denied reasonable access to those resources, or materially increases the costs of technology resources.
- Use of technology resources that violates any local, state, or federal law or regulation, or any other College policy or regulation.
- Use of technology resources that leads to personal gain.

III. User Responsibilities

Access to technology resources is a privilege to which all College faculty, staff, and students are granted. Users must:

- Protect user identification, password information, and the system from unauthorized use.
- Respect the intellectual property of authors, contributors, and publishers in all media.
- Adhere to the terms of software licenses and other contracts.
- Receive prior authorization to purchase, install, or download of any software applications.
- Adhere to the College procurement system to purchase and lease software and computer applications.

- Adhere to all licensing requirements for the approved software.
- Not copy for personal or professional use College-licensed software, except where allowed by College site licenses.
- Comply with local, federal, and state laws and regulations.
- Comply with laws, licensing, contracts, and College policies and regulations applicable to the appropriate use of technology resources.
- Use good judgment and exercise civility at all times when utilizing technology resources.
- Respect the diverse community utilizing technology in a shared manner.
- Understand the appropriate use of assigned technology resources, including the computer, network address or port, software, and hardware.
- Comply with the College use of email as an official means of communication.
- Never use email as an appropriate tool for confidential communication.
- Not attempt to alter the condition or status of any computing network component in any manner. Gaining unauthorized access to College computing or network resources is prohibited.

IV. Password Security

The College reserves the right to audit user passwords to ensure they meet current password security guidelines. All user accounts will be protected by effective passwords. An effective password is both strong and protected. Strong passwords have at least a specified minimum number of characters, are a combination of alphabetic, numeric and special characters, and are updated on a regular basis. Account holders and system administrators, acting as account/password custodians, will protect the security of those passwords by managing passwords in a responsible fashion.

In addition to following a strong password policy, users are required to safeguard their passwords. Individuals should not write down or store the password on paper or on a computer system where others might acquire it. Passwords should not be shared with other people. Users are also expected to change their password immediately if they know or suspect that it has been compromised.

V. Email Use

College email accounts are intended to serve as an official means of electronic communication. Use of College email accounts is limited to educational purposes and legitimate business of the College. Users must abide by all College policies and procedures and federal, state, and local laws. Users must be aware of the legal risks of using email. If any user sends or forwards emails with libelous, defamatory, offensive, discriminatory, or obscene remarks, the user can be held responsible.

Email is intended for communication between individuals and clearly designated groups of individuals and should not be used for mass broadcasting or the wide distribution of

large attachments. Only authorized users may send email to all faculty and staff. General announcements intended for the College community should be posted on Communication Central. Requests for use of the email system for marketing to prospective or current students must have prior approval by the Chief Technology Officer and Director of Marketing.

The College may send official correspondence to members of its community via email. Students, faculty, and staff are expected to check their College email account regularly. College employees are expected to use their College email account for all College-related communications. If a student elects to forward his/her College email to another email account, the student remains responsible for any material not received because of any defect in the forwarding mechanism or the destination account.

VI. Web Policy

The College web site contains information for and about the College community and is a major means of communication, publication, and collaboration in support of the mission of the College. The College maintains the right to temporarily disable access to any web page under review for possible policy violations as well as web pages containing inaccurate information reflecting upon the integrity of the College.

Users are expected to abide by the following:

- Comply with all laws governing copyright, intellectual property, libel, and privacy.
- Adhere to all policies, rules, and regulations of the College.
- Use of the web for non-College commercial activities is prohibited. For the purposes of this Policy and Procedures, activities such as publishing textbooks and other academic works are considered to be College activities.
- Abide by U.S. and international copyright and licensing laws.

The College Web Team, chaired by the Chief Technology Officer, is responsible for web design and navigation. Information Technology (IT) should be notified via a service request for any updating or changes to web site content. A College web page is considered official when it is published by the College. Official College web pages shall be considered College publications.

This Policy and Procedures applies to all official web pages and associated web-based services developed by or for the College. The College will ensure website accessibility for individuals with disabilities in accordance with the Americans with Disabilities Act.

VII. Social Media

College social media sites and accounts are intended to serve as an official means of electronic communication for the College. Use of College social media accounts is limited to educational purposes and legitimate business of the College. Users must be aware of the legal risks of using social media. If any user posts comments with libelous, defamatory, offensive, discriminatory, or obscene remarks, the user can be held

responsible. Creation or use of social media sites and accounts require approval by the Communications Coordinator.

Users agree to abide by all relevant policies and procedures, federal, state, and local laws. These include but are not limited to 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.

VIII. Wireless Network

IT governs the deployment, management, network protocols, frequencies, and bandwidth use of the College wireless networks. IT reserves the right to mitigate any unauthorized access point or device in order to maintain the overall integrity of wireless access.

IX. Remote Access

In order to access technology resources hosted at the College from off-campus, use of a virtual private network (VPN) client can be used to make a connection to campus. The VPN provides a secure, encrypted connection over the internet between an individual device and the College network.

When accessing the network, authorized users are responsible for preventing access to any technology resources or data by non-authorized users. Performance of illegal activities through the network by any user is prohibited. The user accepts responsibility and consequences of misuse of remote access.

These rules and requirements are intended to minimize the exposure of the network to potential threats which may result from unauthorized use of College resources.

X. College-Owned Mobile Devices

The College may provide mobile phones or devices for use by approved faculty or staff. Assigned users are held accountable as per the College mobile phone protocol. In addition, users are responsible for any physical damage or loss of the devices. IT is responsible for maintaining the equipment, including antivirus software and security settings.

XI. Computer Classroom/Lab Usage

Computer classroom/labs are for academic use for students currently enrolled in classes at the College. Commercial use is prohibited. Tampering with hardware or software settings on classroom/lab computers is not permitted. Students should not save files on classroom/lab computers.

XII. Data Security, Confidentiality, and Access

College employees are granted access to data and information resources required to carry out the responsibilities of their position. Employees requiring access to restricted data are

assigned specific access codes which they are responsible for protecting from misuse. Any College employee who knowingly damages or misuses computing resources or data will be disciplined. Access capabilities/restrictions apply to all computing resources owned by the College. Safeguards are taken to ensure the security of the resources and to maximize the integrity of the information.

The College will take appropriate measures to protect Personally Identifiable Information (PII) of its students, staff, and faculty to minimize the growing risks of identity theft. Accordingly, a Social Security Number may not be used as a common identifier or used as a database key in any electronic information system. The College will only use personal information to the extent necessary, to enable the College to carry out its purpose in a reasonable manner. The College also has an obligation to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or destruction.

It is the obligation and intent of the College to protect by reasonable security means the PII of its students, staff, and faculty to minimize the growing risks of identity theft or other risks of disclosure. Safeguards are taken to ensure the security of the resources and to maximize the integrity of the information while stored, processed, and transmitted. This applies to all College-owned computing resources, data, and employee activities.

Collecting, accessing, storing, and disseminating PII data is strictly prohibited unless required by the tasks and responsibilities of business processes. The method of transmission must be approved by the College. As a general rule, PII should be stored on secure College servers. Employees who have permission to work with PII data are not permitted to save the data to cloud storage, portable media, or locally on a computer. Employees must not store PII on a non-College device. PII must not be transmitted via email. Employees must limit their storage of PII to that which is appropriate for the job requirements.

XIII. Disposal of Surplus Computer Equipment

Computer equipment that has no further benefit to the College, as determined by the Chief Technology Officer, shall be deemed surplus and shall be appropriately disposed of by one of the following methods:

- Donation to Frederick County Government, Frederick County Public Schools, or another State, County, or Municipal agency.
- Trade-in on newly acquired equipment.
- Disposal as scrap by means of recycling.

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

XIV. Account Termination

In the event of an employee's separation from employment, Human Resources will initiate the deactivation of the employee's account with IT.

XV. Violations

Any individual who becomes aware of an alleged technology resource violation has a responsibility to report it to IT. Employee or student violators of this Policy and Procedures are subject to College disciplinary policies.

Based on the nature of the offense and/or number of violations, employees are subject to appropriate personnel action, up to and including dismissal. Students are subject to disciplinary action in accordance with procedures established under the Code of Student Conduct, up to and including expulsion.

Violations of this Policy and Procedures may be subject to the initiation of legal action by the College.