6-10: Acceptable Use of Information Technology

Issued: 01/2007
Revised: 07/2014

TABLE OF CONTENTS

I. PURPOSE

The computing and electronic communications resources at Fort Lewis College (FLC) support the instructional, research, and administrative activities of the College. Users of these facilities may have access to College resources, sensitive data, and external networks. Consequently, it is imperative for all users to behave in a responsible, ethical, and legal manner. This policy presents specific guidelines to appropriate behavior and use of FLC computing resources which are designed to contribute to the security and stability of the network.

II. AUTHORITY

This policy was reviewed and approved by the President"s Cabinet.

III. SCOPE

These guidelines apply to all students, faculty, visiting faculty, staff, guests, and external individuals or organizations that use computing and electronic communications resources, and

computing equipment owned, leased or rented by Fort Lewis College. Computing equipment includes, but is not limited to, dialup modems, terminals and microcomputers in public labs, minicomputers, file servers, telephones, and networking equipment used to link these components together and to the Internet.

IV. ACCEPTABLE USE

Those who make use of the Fort Lewis College computing network are required to behave in a manner consistent with Fort Lewis College's codes of conduct (See Student and Employee Handbooks). As a user of this network, you agree to the following usage guidelines:

1. General

a. Read, understand and adhere to all College Information Technology policies and exercise good judgment in the protection of information resources.

b. Fort Lewis College is not responsible for the content of any material you prepare, receive, transmit, or store. Thus, as a condition of using the College's computer system, you represent that you are in compliance with all federal, state and international copyright and other intellectual property laws, licensing agreements and other federal and state laws, and that you will not use the system to violate any federal, state or local civil or criminal laws. Furthermore, you will indemnify, exonerate and save the College (and its representatives) harmless from any claim, damage or cost related to your use, including any legal fees the College decides it is necessary to incur to defend itself.

c. Because anti-virus programs cannot provide 100% protection from malicious software, you agree to exercise due caution when opening Email, browsing the Internet, downloading files from the Internet, and installing software. You should avoid opening unexpected or suspicious attachments.

d. Immediately report any suspected or known information security compromises, including viruses or malicious code, on a system under your control to Information Technology personnel (as listed at https://www.fortlewis.edu/administrative-offices/information-technology/contact-us) and to cooperate with internal or external investigations if requested.

e. Take advantage of security training opportunities that are offered by the College to maintain awareness of current security issues.

f. Conduct all communications from off campus in a secure manner. Secure access can be achieved by:
1. Dialing in to the campus modem pool
2. Using a Virtual Private Network (VPN) connection
3. Communicating via web pages that utilize protocols such as SSL / TLS to encrypt data during transmission. (e.g. a URL beginning with https:// uses a secure protocol.)

2. Computer Accounts

Computer accounts are granted to Fort Lewis College faculty, staff, and students for bona fide purposes related to their work or studies at the College. You are responsible for all activities, including electronic mail transmissions, performed using any computer account you have been given, whether such activities are performed by you or by another person using your account.

The Office of Information Technology cannot retrieve lost or forgotten passwords. A new password will be issued upon presentation of a valid picture ID to either the Helpdesk or a Lab Coordinator.

a. Make appropriate use of account protection features such as selecting a secure password that is not easily guessed and changing your password at regular intervals.

b. Use only those computer accounts that have been created for your use. The negligence of another user in revealing an account name or password is not considered authorization for use.

c. If you have reason to believe that someone has made unauthorized use of your account, immediately change your password and report the incident to the Office of Information Technology.

d. If you are the head of a department that has been assigned a group account " for example, an email account for an entire office " you are responsible for all use of the account. You agree to notify the Office of Information Technology when a group account is no longer needed.

3. Individually Assigned Computing Resources

a. Physically protect the resources under your control. For example, doors shall be locked to protect equipment when unattended. Particular care is expected when traveling and at home to protect these devices.

b. Make your systems available for anti-virus and operating system updates, patches, and service packs.

c. Be responsible for backing up any data stored on your computer. Backup media containing Confidential or Internal Use Only data must be stored securely, using encryption or password protection on the documents or media.

4. Shared Computing Resources

Computers located in labs require a logon, and are available to registered students, staff, and faculty of Fort Lewis College. Kiosks located in areas such as building corridors and the Library do not require a logon and may be available to the general public.

a. Observe posted closing times, and to vacate labs at non-posted times when requested to do so. Facilities have varying priorities for use, described fully in the Computer Lab Use and Scheduling Policy. All users should leave prior to the posted beginning of these classes, unless otherwise permitted by the instructor.

b. Comply with guidelines posted in the public computing facilities (e.g. no smoking, eating, drinking, chewing tobacco).

c. Log off from applications, computers, and networks located in computer labs or other public areas when finished. When using on or off campus public facilities such as Internet kiosks where logging off is not allowed, you should always close your Internet browser(s) if possible when finished with your session.

5. Non-College-Owned Devices Attached to the Network

The College computer network is a shared, finite resource installed by the College to promote scholarship and learning. Accidental or intentional disruption of the network will deprive others of access to important College resources. College and internet resource access typically requires computer account authentication.

a. Be responsible for the security of any computer system or network device you attach to the network, and for any intentional or unintentional activities from or to that network connection.

b. Comply with all policies governing the use of network resources, including but not limited to the Student Conduct Code and the Information Technology Security Policy.

c. To avoid network conflicts that arise when duplicate computer names appear on the network, use the name assigned to your Windows computer by the Office of Information Technology. If you are a student and wish to connect your personal computer to the network, set your Computer Name to your Fort Lewis College network account username.

d. Run a legally licensed operating system that is approved by the Office of Information Technology. Contact the Office of Information Technology for a current list of approved operating systems. If not on the approved list, it will be your responsibility to demonstrate that the system is up-to-date with regard to security patches, antivirus software updates, firewall services and other standard security measures.

e. Run a current version of a College-approved antivirus software package. Contact the Office of Information Technology for a current list of approved vendors. Students, Faculty and Staff of Fort Lewis College may obtain antivirus software free of charge that is licensed by the College. Antivirus software must be configured to receive automatic updates of virus definition files on at least a weekly, and preferably a daily basis. Scans should be run at least weekly.

f. Update your computer operating system and application software regularly to maintain the current level of Service Packs, patches, hotfixes, or other software updates related to security and network stability.

g. Make your device available for scanning and update to meet the College"s required security standards, including but not limited to patch levels, service pack versions, definition files, and scan engines.

h. In the event that the Office of Information Technology issues a notice requiring the installation, either immediately or within a designated time period, of a specific security update that is deemed to be critical to the continued security and stability of the network, you agree to apply the update within the time frame specified. Assistance with the installation of such critical updates will be provided if possible. You understand that computers found to be non-compliant may be disconnected from the network if necessary.

i. If a system you attach to the network creates security problems or disrupts others" use of the network, your device will be disconnected until the problems are remedied.

V. UNACCEPTABLE USE

The following activities are strictly prohibited. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use. You may be exempted from these restrictions during the course of your legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

1. General

a. Under no circumstances are you authorized to engage in any activity that is illegal under local, state or federal law while utilizing Fort Lewis College owned or leased resources.

b. State of Colorado Fiscal Rule forbids use of State equipment or resources for private purposes.

c. Examining, copying, modifying or deleting files and/or data belonging to other users without their prior consent. Exception to the 'Examining'□ prohibition is granted when the documents have been published to a public venue such as a website.

d. Using Fort Lewis College computer systems and/or networks to attempt to gain unauthorized access to remote systems.

e. Making any intentional attempts to obtain unauthorized access to or otherwise interfere with the operation of network systems or programs.

f . Willfully introducing computer 'malware'□ (e.g. viruses, worms, spyware or other disruptive/destructive programs) into the College network or into external networks.

g. Intentionally operating any network-intensive application which overloads the network. If you are notified of such an application detected running on a computer under your control that is impeding other users through mass consumption of system resources, you agree to discontinue running the software. If the application presents an imminent hazard to the College network or disrupts the activities of others, the offending computer system or the subnet to which it is attached may be disconnected without prior notice.

h. Performing any unauthorized, deliberate action which damages or disrupts a computing system, alters its normal performance, or causes it to malfunction.

i. Executing port scans, security scans, or any form of network monitoring which will intercept data not intended for you, unless this activity is a part of your normal job duty.

j. Forging or attempting to forge electronic mail messages or header information.

k. Attempting to read, delete, copy, or modify the electronic mail of other users.

l. Sending or attempting to send harassing, obscene, or other threatening e-mail to another user.

m. Making illegal copies of software licensed to the College.

n. Using College-owned computer accounts, computer and communications equipment, software, and networks for commercial purposes. These purposes may include, but are not limited to:
i. Sending Unsolicited Commercial Email (UCE, more commonly known as spam), other 'for profit' messages, or chain letters.
ii. Transmission of commercial or personal advertisements, solicitations, or for extended reproduction of political, ideological or commercial material originated by a person or organization.
iii. The execution of revenue-generating advertising programs.

o. Using software and hardware provided by the College for work outside the teaching, learning, and professional mission of the College. Incidental and occasional personal use not related to College business may be permitted if it does not materially interfere with the availability of services for College purposes and does not result in a direct cost for the College. (For example, receiving an incidental electronic mail message electronically does not create a direct cost; printing a personal electronic mail message does.)

p. Modifying configuration options or installing additional software that may cause increased security vulnerabilities. Installing software or devices to allow remote access to a College-owned computer in such a way that would bypass existing security measures.

q. Encroaching on other's use of shared computing resources. Such encroachment shall include, but is not limited to, creating a disturbance, displaying offensive material on shared equipment, or otherwise interfering with others' use of shared computing resources.

r. Pointing a non-fortlewis.edu domain name at a host within the Fort Lewis College address space, unless that domain is being used by a recognized college organization or affiliate, and the domain registration is handled or approved by the Office of Information Technology.

s. Offering 'server-class' services from your device without prior approval from the Office of Information Technology. Examples of such 'server-class' services include, but are not limited to:

DNS, DHCP, SMTP (e-mail), WINS, File and Print Sharing, WWW (web services such as Microsoft IIS or Apache).

t. Connecting any wireless access devices to the campus network without prior approval from the Office of Information Technology. The Office of Information Technology will collaborate with the person or group affected to ensure that security is maintained and that no interference is introduced into existing systems.

2. Computer Accounts

a. Attempting to decrypt system or user passwords.

b. Attempting to secure a higher level of privilege on network systems, or attempting to subvert the restrictions associated with your use of accounts and/or software.

c. Revealing your account password to others, except for the purpose of technical support by Information Technology personnel. If you must share your password with Information Technology personnel for technical support, you agree to change your password upon resolution of the technical issue. You agree not to store or post your password in any manner, electronic or physical, that would make it easily accessible to unauthorized users.

d. Allowing use of your account by others. This includes family and other household members.

VI. PRIVACY AND CONFIDENTIALITY

1. Information Handling

a. You are responsible for knowing the privacy and confidentiality restrictions associated with any information to which you have access. You agree to safeguard information that is classified Confidential or Internal Use Only, as defined in the Information Technology Security Policy and the Data Classification Guidelines. Such safeguards include but are not limited to:

i. Storage of information:
A. Storing such information in a place that provides a high level of protection against unauthorized access. In general, this means on secure network drives (e.g. 'M:' or 'O:' drives) as provided by the Office of Information Technology.
B. Not taking such information outside of the College unless it can be assured adequate protection. Ensuring that all such data that is taken outside the College is stored in an encrypted format.
C. Logging off or locking devices containing Confidential or Internal Use Only data when left unattended.

ii. Distribution and transmission of information:
A. Not distributing nor making Confidential or Internal Use Only information available to persons who are not authorized to access the information. This applies to originals, copies, and new materials that contain all or part of the information, and to oral communication of

information. When Confidential and Internal use only information is distributed, it shall be distributed in such manner that the future distribution restrictions are clear.

B. Appropriately protecting Confidential or Internal Use Only information that is transmitted electronically, transported physically, or spoken in conversation from unauthorized interception. Encryption shall be used when electronically transmitting Confidential information. In general, electronic mail is not appropriate for transmitting Confidential information. Tamper-resistant packaging shall be used when physically transmitting Confidential information.

iii. Destruction and disposal of information and devices:
A. Disposing of Confidential or Internal Use Only information on paper or other physical media in such a manner as to ensure that it cannot be retrieved and recovered by unauthorized persons. Confidential or Internal Use Only documents must not be placed in recycling bins. Paper shredders are highly recommended.

B. Taking care to ensure that Confidential or Internal Use Only data is rendered unreadable when disposing of computers or removable media.

2. Electronic Communications and Data

a. The College does not routinely intercept or monitor electronic mail, other electronic communications, or other data stored in electronic format. Capture and/or "reading" of electronic communications and/or other data stored in electronic format by technical staff or others is expressly prohibited, except under the following circumstances:

i. To resolve technical or delivery problems.
ii. To prevent illegal, unauthorized, or inappropriate use.
iii. To meet externally imposed legal requirements.
iv. In the course of an investigation triggered by indications of misconduct.
v. To protect health and safety.
vi. To prevent interference with the mission of the College.
vii. To locate information required for College business that is not more readily available elsewhere.

b. However, employees should not have an expectation of privacy in anything that they create, send, or receive on the College e-mail, network, Internet or computer systems. Such systems are provided to facilitate College business and all transactions and data on the systems are consider to be business related. In accordance with the Colorado Open Records Act (CORA) (CRS 24-72-201 et seq.) all information and e-mail correspondence on state employees" computers are public records, open for public inspection by any person at reasonable times (unless a specific CORA exception applies).

c. You agree that electronic mail, other electronic communications, or other data stored in electronic format on College business or with the use of College resources may be made available for review by any authorized College official for purposes related to College business.

d. The Family Educational Rights and Privacy Act of 1974 (FERPA) gives students the right to inspect and review their educational records and provides them with some protection against the release of information. Electronic correspondence could become a student record under FERPA, and thus be available to disclosure under that Act.

e. Confidentiality regarding student records is protected under the Family Educational Rights and Privacy Act of 1974 (FERPA). All use of electronic mail, including use for sensitive or confidential information, will be consistent with FERPA.

3. Confidential Data

You agree to comply with:

a. The Family Educational Rights and Privacy Act (FERPA) of 1974 (Buckley Amendment), as amended. If your account gives you access to student data, you must comply with all FERPA regulations regarding disclosure of student information. To find out specifically what information you may or may not give out and to whom, visit the FERPA website maintained by the Records office or contact that office via phone or e-mail. When you are in doubt as to whether or not you are permitted to release some information, do not release the information until you know for sure.

b. The laws of the State of Colorado, the United States and other regulatory agencies. This includes all applicable federal and state laws which govern the privacy and confidentiality of data, including but not limited to the Electronic Communications Privacy Act of 1986, Health Insurance Information Portability and Accountability Act (HIPAA), Foreign Corruptions Practice Act, Gramm-Leach-Bliley Act, and the Computer Fraud and Abuse Act.

c. All College policies and handbooks.

VII. CONSEQUENCES OF POLICY VIOLATIONS

1. Malicious, destructive or illegal conduct or failure to comply with this policy may result in disconnection from the network, loss of lab privileges, legal action, or other disciplinary action, subject to normal College procedures as described in the appropriate student, faculty or employee handbooks and documents. Illegal activities may be reported to the appropriate civil authorities for prosecution. The College will fully comply with the authorities to provide any information necessary for the litigation process.

2. The Office of Information Technology may revoke accounts at any time if computing privileges are abused. This revocation may be temporary, if such action is deemed necessary for the successful management and operation of the facilities, or permanent through the normal College disciplinary process.

3. You are responsible for any damages resulting from your failure to comply with these guidelines. Such damages include the cost of College staff time spent recovering from any unauthorized activity.

4. Faculty and staff will be referred to their dean or department head for appropriate action. Students will be subject to normal College disciplinary procedures as outlined in the student handbook.

5. Copyright violation procedures:
Storing or transmitting content in violation of federal, state and international copyright and other intellectual property laws and agreements and other federal and state laws will result in the following disciplinary action:

a. Faculty and staff will be referred to their dean or department head for appropriate action.

b. Students in the Residence Hall network will be subject to the following rules:

i. 1st Offense:
A. Port will turned off until workstation is compliant
B. Student informed of offense and compliance requirements
C. Computer is inspected for compliance ~ port turned on
D. User is referred to Judicial Affairs
E. Documentation of student incidents is shared with student and parents as allowed by FERPA and other applicable law

ii. 2nd Offense:
A. Port will be turned off for an indefinite period of time
B. Student informed of offense and compliance requirements
C. Computer is inspected for compliance ~ port turned on after punitive period
D. User is referred to Judicial Affairs
E. Documentation of student incidents is shared with student and parents as allowed by FERPA and other applicable law

iii. 3rd Offense:
A. Port will be turned off for remainder of semester
B. Student informed of offense and compliance requirements
C. Computer is inspected for compliance ~ port turned on the first day of the following semester
D. User is referred to Judicial Affairs
E. Documentation of student incidents is shared with student and parents as allowed by FERPA and other applicable law