TECHNOLOGY RESOURCES – ACCEPTABLE USE

CR
(REGULATION)

NETWORK MISSION

The network, and through the network the Internet, offers an abundance of educational material as well as opportunities for collaboration and the exchange of ideas and information. College of the Mainland recognizes the educational value of the Internet, and strongly encourages the responsible use of the network by all students and employees. Successful operation requires that all users view the network as a shared resource, and work together to maintain its integrity by behaving in a responsible, conscientious manner.

This regulation describes the types of network applications that are contrary to our network mission and which are therefore prohibited. These are guidelines only and are not meant to be an exhaustive list of prohibited activities.

DEFINITION OF USER

A *user* is defined as any person that is not Information Technology Services Personnel that has been assigned a valid network logon by the network administrator. Such logons (or accounts) should be used only by the owner of the account in a legal and ethical fashion.

PRIVACY RIGHTS AND SECURITY

Student and employees data files, email, and electronic storage areas are considered the property of College of the Mainland, subject to College of the Mainland control and inspection. The appropriate Information Technology Services administrator may access all such files and communications to ensure system integrity and that users are complying with the requirements of this regulation and any associated regulations. Students and employees should not expect that information stored on the network will be private.

Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide his or her password to another person. Users will immediately notify the Information Technology Services if they have identified a possible security problem relating to misappropriated passwords.

PROHIBITED USE

A. Illegal or Destructive Activities

Users may not use the network for any purpose that violates the law or threatens the integrity of the network or individual workstations. Prohibited activities include, but are not limited to:

1. Attempting to gain unauthorized access to the network, or go beyond their authorized access. This includes attempting to log on through another person's account, generic account or access another person's files, attempting to obtain passwords, or attempting to remove any existing network security functions. Users will not actively search for security problems, because this will be construed as an illegal attempt to gain access.

2. Intentionally developing or using programs to harass other users or to attempt to violate the security or alter software components of any other network, service or system. Examples of such activities include hacking, cracking into, monitoring or using systems without authorization, scanning ports, conducting denial-of-service attacks and distributing viruses or other harmful software.

3. Attempting to damage hardware, software or data belonging to the college or other users. This includes adding, altering or deleting files or programs on local or network hard drives and removing or damaging equipment such as mice, motherboards, speakers or printers.

4. Fraudulent use of credit card numbers to purchase online merchandise.

5. Distributing or downloading licensed software or installing software such as games or music in violation of software license agreements (piracy). This includes any peer-to-peer file sharing.

B. Inappropriate Material

Users will not use the network to access or distribute material that is obscene, pornographic, indecent or hateful, that advocates illegal acts or that advocates violence or discrimination toward other people. This includes but is not restricted to distribution through email, discussion groups or web pages.

C. Respect for Other Users

Restrictions against inappropriate language or images apply to personal email, discussion group postings and material posted on web pages. Users will not use obscene, profane, vulgar, inflammatory, threatening or disrespectful language. Users will not post false, defamatory, or derogatory information about a person or organization or information that, if acted upon, could cause damage to individuals or property.

Users will not harass other persons through the network. Such harassment includes, but is not limited to, distribution of unsolicited advertising, chain letters, or email spamming (sending an annoying or unnecessary message to a large number of people. Users will not post personal contact information about other people, including address, telephone, home address, work address, etc. Users must not send mail that does not accurately identify the sender, the sender's return email address, and the email address of origin.

D. Resource Limits

No software shall be downloaded from the Internet or email on a workstation without prior permission from Information Technology Services personnel. Software installed by any user other than Information Technology

Services personnel is considered a violation of this regulation. Users have a right to temporary use of disk storage space and are responsible for keeping their disk usage below the maximum size allocated. Extremely large files, if left on the network for an extended period, may be removed at the discretion of the Chief Information Officer.

Users will check their email frequently, delete unwanted messages in a reasonable timeframe, and stay within their email quota. Where applicable, users will comply with state and federal statutes governing public record retention. Users will subscribe only to discussion group mail lists that advance and are relevant to their education or professional/career development.

Users are to utilize the college email only for the purposes related to the college and performance of their jobs. Use of college technology, including email accounts, is limited to purposes related to the college and employees' job performance. Use of college technology for private financial gain, advertising, solicitation, proselytization or fund-raising for any non-college purpose will be considered a violation of this regulation unless approved by the President.

E. Theft of Intellectual Property

Users must respect the legal protection provided by copyright law and license agreements related to content, text, music, computer software and any other protected materials. Users will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user. Users will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user shall follow the expressed requirements. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner. It is the

regulation of College of the Mainland that any illegal peer-to-peer file sharing over the College's network is prohibited. Unauthorized distribution of copyrighted material, such as through peer-to-peer networks, may subject users to civil and criminal penalties. Federal law authorizes a copyright owner to recover civil damages. You can also be prosecuted criminally for copyright infringement.

VIRUS PROTECTION

To maintain a secure and reliable computing environment within our campus, College of the Mainland requires all computers connected to the network to, or that could be connected to the network, have a reliable and updated anti-virus scan program on each computer. This program must be updated and scans performed on a regular basis. Information Technology Services shall maintain network-level anti-virus protection. Any person who knowingly introduces a virus, worm, or Trojan horse programs onto any computer or server is subject to disciplinary action, including restitution and termination.

SECURITY AWARENESS

All students and employees who have access to computers, email, or other forms of electronic data must acknowledge that they have read and agree to comply with all College of the Mainland policies and network security procedures adopted by Information Technology Services.

USERNAME AND PASSWORD

College of the Mainland requires all employees and students be properly identified and authenticated before being allowed to access the college network. Users are responsible for safeguarding their passwords and are responsible for all transactions using their passwords. No individual may assign his or her account or password to any other person. Any person who deliberately makes their account available to an unauthorized user will incur termination of their account. Similarly, any person who fraudulently gains access to another person's password or account may incur disciplinary action.

1. All ITS personel passwords must be changed every 45 days.
2. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days. The recommended change interval is every 60 days.
3. Passwords must not be inserted into email messages or other forms of electronic communication.
4. All user-level and system-level passwords must conform to the guidelines described below.

PASSWORD CONSTRUCTION GUIDELINES

Passwords are used for various purposes at College of the Mainland. Some of the more common uses include: user level accounts, web accounts, email accounts and screen saver protection.

Poor, weak passwords have the following characteristics:

1. The password contains less than eight characters

2. The password is a word found in a dictionary (English or foreign)
3. The password is a common usage word such as:
    a) Names of family, pets, friends, co-workers, fantasy characters, etc.
    b) Computer terms and names, commands, sites, companies, hardware, software.
    c) The words "College of the Mainland", "COM", "mainland" or any derivation.
    d) Birthdays and other personal information such as addresses and phone numbers.
    e) Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    f) Any of the above spelled backwards.
    g) Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Strong passwords have the following characteristics:

1. Contain both upper and lower case characters (e.g., a-z, A-Z)
2. Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
3. Are at least eight alphanumeric characters long.
4. Are not a word in any language, slang, dialect, jargon, etc.
5. Are not based on personal information, names of family, etc.
6. Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords.

PASSWORD PROTECTION STANDARDS

Do not use the same password for College of the

Mainland accounts as for other non-College of the Mainland access (e.g., personal ISP account, option trading, benefits, etc.). Do not share College of the Mainland passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential College of the Mainland information.

Here is a list of "dont's":

1. Don't reveal your password over the phone to ANYONE
2. Don't reveal your password in an email message
3. Don't reveal your password to the boss
4. Don't talk about a password in front of others
5. Don't hint at the format of a password (e.g., "my family name")
6. Don't reveal a password on questionnaires or security forms
7. Don't share a password with family members
8. Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Technology Services (ITS).

Do not use the "Remember Password" feature of applications (e.g., Chrome, Outlook, Firefox, Internet Explorer).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system without encryption.

If an account or password is suspected to have been compromised, report the incident to ITS and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by ITS or its delegates. If a password is guessed or cracked during one of these

	scans, the user will be required to change it.
NETWORK SECURITY	Any and all actions that jeopardize the integrity and stability of the network by violating the network security standards outlined in the Acceptable Use Policy or other college regulation is subject to disciplinary action commensurate to the level of risk or damage incurred.
ACCESS	Employees and students who are given authorization may connect to the college network, for college activities through a wired or wireless connection after demonstrating compliance with security procedures established by the Information Technology Services.
REMOTE ACCESS	This regulation refers to connection to the college computing network from outside of the College of the Mainland network, such as from an employee's home. The computer systems, networks and data repositories of the college's network are critical resources and must be protected against unauthorized access, malicious access, and disruption of service. Authorized users of the college's computer systems, networks and data repositories may be permitted to remotely connect to those systems, networks and data repositories for the conduct of college related business only through secure, authenticated and carefully managed access methods.
TECHNOLOGY HARDWARE AND SOFTWARE PROCUREMENT	To maintain high levels of reliability, cost effectiveness, and interoperability of the communications and data technology within the college, College of the Mainland requires all technology purchases, with the exception of toner/ink cartridges, be approved by Information Technology Services.
COLLEAGUE/WEBADVISOR	College of the Mainland maintains a database system for a wide variety of information management purposes. Much of the information is personal information on students, faculty, employees, alumnae and friends of the college. College of the Mainland considers the security of this information to be one of the college's most serious

responsibilities, and accordingly, access to these databases is limited to persons who have a legitimate need to use the information to advance the academic and administrative goals of the college.

Persons who are given passwords and have legitimate access to the information on Colleague/WebAdvisor have a strict responsibility to ensure that this information is used appropriately, and that the privacy of persons identified through this information is strictly protected. This responsibility extends both to information available on computer screens as well as information available in print media, including all printouts, manual dossiers, correspondence files, directories, and similar forms of information banks.

TELEPHONE SYSTEM AND VOICE-MAIL

College of the Mainland provides telephone and voice mail access to full-time employees. Employees receive phone numbers and voice mailboxes when they begin employment at College of the Mainland. The same policies and expectations that govern e-mail also govern voice mail and telephone usage.

Any use of College of the Mainland telephones for any fraudulent or illegal purpose will incur severe penalties, including the possible involvement of law enforcement authorities as well as disciplinary action by College of the Mainland.

Telephone misconduct includes misuse of telephone credit cards, misuse of college long-distance access codes, theft of telephone instruments, and any related misconduct.

BLOGS, ONLINE JOURNALS AND SOCIAL NETWORKING SITES

College of the Mainland recognizes the broad array of communications and networking tools available in the online environment. College of the Mainland is not responsible for any blogs, online journals, social networking sites or other communications and information tools except those that the college chooses to maintain

officially on its website or in other locations.

College of the Mainland has no official relationship, nor does College of the Mainland approve, of any communications or references that occur on other websites, blogs, social networking sites or other Internet locations, and College of the Mainland accepts no responsibility for materials that appear or communications or representations that occur on such external websites, including but not limited to facebook.com, twitter, instagram, craigslist.com and similar sites.

VIOLATIONS

In the event there is an allegation that a student or employee has violated the Acceptable-Use Regulation, the student or employee will be provided with notice of the alleged violation and an opportunity to present an explanation before an administrator. Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student or employee in gaining the self-discipline necessary to behave appropriately on a computer network. The Chief Information Officer has authority to disable any account where there is a violation of this regulation.

The college may at its sole discretion determine whether a use of the network is a violation of this regulation. Violations of this regulation may result in a demand for immediate removal of offending material, blocked access, suspension or termination of the users account, or other action appropriate to the violation. The college reserves the right to act without notice when necessary, as determined by the administration. The college may involve, and will cooperate with, law enforcement officials if criminal activity is suspected. Violators may also be subject to civil or criminal liability under applicable law.