

**POLICY
BOARD OF TRUSTEES
MAYLAND COMMUNITY COLLEGE**

Title: INFORMATION TECHNOLOGY ACCEPTABLE USE

Type: INSTITUTIONAL

POLICY NO: 3.007

Policy Adopted: April 13, 1998

EFFECTIVE DATE: 11-18-13

**AMENDED DATE: 8-21-00; 8-13-07; 2-18-08; 03-11-13;
11-18-13**

Charles Ronald Kates
Chairman

AUTHORITY: N.C.G.S. 115D-20 (7)/14-453/14-454 (b)

1. Policy Statement

The purpose of this policy is to establish acceptable and unacceptable use of information technology resources at Mayland Community College in conjunction with its established culture of lawful and ethical behavior, trust, openness and integrity.

Recognizing that each individual user is ultimately responsible for his/her own actions, the Board adopts the following policy governing the use of institutional I.T. resources, and establishes conditions relative to their acceptable use for the purpose of allocating resources and avoiding disruption of MCC educational programs and business operations. This policy makes no attempt to articulate all required or prohibited behavior by users of MCC I.T. resources. While ultimate decisions on access shall be made by authorized College personnel, guidelines shall be adopted subject to the limitations of the following sections.

2. Acceptable and Unacceptable Uses

I.T. resources owned and/or operated or services provided or subscribed to by Mayland Community College, hardwired and wireless, are intended for the use of MCC students, faculty, staff and other authorized individuals for purposes directly related to instruction and business operations.

It is not acceptable to utilize or make use of MCC I.T. resources:

- For any purposes prohibited by federal or state law.
- For commercial gain or profit.
- To create or propagate computerized viruses, malware or spyware.
- To access, display, make accessible, play, publish or transmit any annoying (i.e. spamming), discriminatory, indecent, lewd, obscene, pornographic, offensive, racist, sexist, threatening or harassing language and/or materials.
- To transfer copyrighted materials to or from any information resource, except as permitted by law or by written agreement with the owner of the copyright.
- To attempt to obtain unauthorized computer access or privileges, or to attempt to trespass in the files, folders or work of another individual.
- To conduct any activity that could cause a security breach or disrupt service.
- For “snooping”, i.e., obtaining access to the files or electronic mail of others for the purpose of satisfying idle curiosity, with no substantial College business purpose.
- For “spoofing”, i.e., constructing an electronic communication so it appears to be from someone else.
- For “phishing”, i.e., attempting to gain confidential information by using fraudulent emails or other electronic communications.

TITLE: INFORMATION TECHNOLOGY ACCEPTABLE USE

TYPE: INSTITUTIONAL

Due to the possibility of configuration errors, virus infections, etc., personally owned devices such as laptop computers may not be attached to any wired port on the MCC network. Only those devices owned and managed by Mayland Community College will be allowed to connect to the Mayland Community College wired local area network. Further, it is not permissible to deliberately attempt to damage and/or sabotage I.T. resources or to perform port scans.

3. Reservation of Rights and Limits of Liability

Mayland Community College reserves all rights in the use and operation of its I.T. resources, including the right to monitor and inspect electronic files, resources and/or computer support services, or to terminate service at any time and for any reason without notice.

The College makes no guarantees or representations, either explicit or implied, that user files and/or accounts are private or secure.

The College and its representatives are not liable for any damages and/or losses associated with the use of any of its I.T. resources or services.

The College reserves the right to limit the allocation of I.T. resources for users, i.e. bandwidth, access time, disk space, services, etc.

4. Electronic Mail and Voice Messaging

a. Access and Use of Electronic Mail and Voice Messaging:

Only Mayland Community College faculty, staff and students and other persons who have received permission from the appropriate College authority are authorized users of the College's electronic mail and voice messaging systems and resources.

The use of any College resources for electronic mail and voice messaging must be related to College business, including academic pursuits. Incidental and occasional personal use of electronic mail and voice messaging may occur when such use does not generate a direct cost for the College. All uses of electronic mail and voice messaging utilizing Mayland Community College I.T. resources are subject to the provisions of this policy.

b. Monitoring and Disclosure of Electronic Mail and Voice Messages:

Mayland Community College will make reasonable efforts to maintain the integrity and effective operation of its electronic mail and voice messaging systems, but users are advised that those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature and technology of electronic communication, the College can assure neither the privacy of an individual user's use of the college's electronic mail and voice messaging resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored thereby.

The College will not monitor electronic mail or voice messages as a routine matter but it may do so to the extent permitted by law as the College deems necessary for purposes of maintaining the integrity and effective operation of the College's electronic mail and voice messaging systems. Any user of the College's electronic mail resources who makes use of an encryption device to restrict or inhibit access to his or her electronic mail must provide access to such encrypted communications when requested to do so under appropriate College authority.

TITLE: INFORMATION TECHNOLOGY ACCEPTABLE USE

TYPE: INSTITUTIONAL

To the extent permitted by law, the College reserves the right to access and disclose the contents of faculty, staff, students' and other users' electronic mail and voice messages without the consent of the user. The College will do so when it believes it has a legitimate business need including, but not limited to, those listed below, and only after explicit authorization is obtained from the appropriate College authority:

- in the course of an investigation triggered by indications of misconduct or misuse
- as needed to protect health and safety
- as needed to prevent interference with the academic mission, or
- as needed to locate substantive information required for College business that is not more readily available by some other means

The College will inspect and disclose the contents of electronic mail and voice messages when such action is necessary to respond to legal processes and to fulfill the College's obligations to third parties.

c. Public Inspection and Archiving of Electronic Mail and Voice Messages:

Electronic mail and voice messages of students may constitute "education records" subject to the provisions of the federal statute known as the Family Educational Rights and Privacy Act of 1974 (FERPA). The College may access, inspect, and disclose such records under conditions that are set forth in the statute.

North Carolina law provides that communications of College personnel that are sent by electronic mail and voice messaging may constitute "correspondence" and, therefore, may be considered public records subject to public inspection under North Carolina General Statutes 121 and 132.

Electronic files, including electronic mail and voice messaging, that are considered to be public records are to be retained, archived and/or disposed of in accordance with current guidelines established by the North Carolina Department of Cultural Resources.

5. Administrative Systems

The College accepts its responsibility for good administrative business procedures and record maintenance. All employees have responsibility for system security. Those who use the system are responsible for that portion of data, software, and equipment. Access to the system or any part of the system will be granted on a "need-to-know" basis while in context to the performance of assigned duties. Data retrieved from the system becomes the responsibility of the user. This includes, but is not limited to the following: hardcopy, handwritten, electronic, physical, and acquired knowledge. Each user therefore becomes responsible for securing such information and is responsible for all activities performed under their user account.

6. Violations

Violation of any of the provisions of this policy may result in suspension of information technology resource privileges, disciplinary review, dismissal, termination and/or prosecution in accordance with applicable federal, state or local statutes or ordinances.

Definitions

- a. "Access" means to approach, instruct, communicate with, cause input, cause output, or otherwise make use of any resources of an information system/network or component or service thereof.
- b. "Computer" means an internally programmed, automatic device (either physical or virtual) that performs data processing.
- c. "Computer network" means the interconnection of communication systems with a computer through remote devices, or a complex consisting of two or more interconnected computers or devices.
- d. "Computer program" means an ordered set of data that are coded instructions or statements that, when executed by a computer, cause the computer to process data.

TITLE: INFORMATION TECHNOLOGY ACCEPTABLE USE

TYPE: INSTITUTIONAL

- e. “Computer software” means a set of computer programs, procedures and associated documentation concerned with the operation of a computer or computer system.
- f. “Electronic mail/voice message” means any message in a system that depends on information technology to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, listen, or print for purposes of communication across information systems between or among individuals or groups, that is either explicitly denoted as electronic mail or voice messaging or is implicitly used for such purposes, including services such as electronic bulletin boards, listserves, and newsgroups
- g. “Harass” means to engage persistently in a pattern of unwanted or repeated annoying behavior targeted at one or more particular individuals.
- h. “Indecent” means grossly unseemly or offensive to manners or morals.
- i. “Obscene” means any work or material which, when taken as a whole, would be determined by an average person applying contemporary community standards, to appeal solely to the prurient interests, and which lacks any serious literary, artistic, political or scientific value.
- j. “Property” includes, but is not limited to, financial instruments, information, including electronically processed or produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.
- k. “Pornographic” means erotic or sexually explicit material of any type, including material that depicts children or minors in a sexually explicit manner.
- l. “Resource” includes hardware, software, services, infrastructure and data.
- m. “Snooping” means obtaining access to the files or electronic mail/voice messages of others for the purpose of satisfying idle curiosity, with no substantial College business purpose.
- n. “Spamming” means attempting to deliver unsolicited electronic mail to someone who would not otherwise choose to receive it.
- o. “Spoofing” is the process of deception by which an individual or system alters its identity and/or creates additional identities in order to gain privileged access to information/network resources and/or impersonate a user or user group.
- p. “Phishing” means the practice of using fraudulent emails or other electronic communication in order to obtain confidential information.