

PROCEDURES MEMORANDUM

TO: MCC Staff

FROM: Office of the President

SUBJECT: Acceptable Use of Information Technology and Resources

DATE: August 27, 2010

PURPOSE: To establish uniform procedures for use and security of information technology and resources.

SCOPE: This procedure applies to all members of the authorized user-community: all College employees, students, authorized contractors, and members of the Board of Governors.

1. General Principles

- A. The College provides certain information technology resources – such as telephones, pagers, computers, printers, facsimile machines and digital cameras, as well as access to local, national and international sources of information (Internet and College network). That technology is intended for College educational and business use and is designed to assist with effective and efficient learning and communication.
- B. Members of the authorized user-community – all College employees, students, authorized contractors, and Board members – are expected to employ such technology consistently with applicable state and federal laws, the Mission of the College, and other official College documents such as Board of Governors’ Policies and College Procedures Memorandums.

2. User Responsibilities

- A. College information technology resources are intended to be used for College-related business. Modest and prudent personal use is permitted so long as it does not interfere with College operations, conflict or interfere with an employee-user’s performance of duties or responsibilities, interfere with the rights or reasonable expectations of another, or involve additional cost or expense to the College.
- B. Preserving the integrity and security of the College’s information resources must be a user-community effort and requires each member to act responsibly to guard against abuses. Each user must recognize that technology access is a privilege rather than a right of employment or attendance at the College. Ownership of all information and all data stored on College information technology equipment and media is claimed and retained by the College. The College reserves the rights to monitor, copy, use, duplicate, distribute, sell and/or remove information, data and peripheral equipment.

Accordingly, no member of the user-community should have any expectation of privacy in any information or data stored on College information technology equipment or media.

3. College Responsibilities

- A. The College has a responsibility to ensure that public property and public resources are used in a proper manner for proper purposes, as well as a responsibility to ensure that College employees maintain a high level of productivity. Accordingly, College computers, computer systems and computer networks are subject to monitoring by the College at any time without further notice. Use of College computer systems, authorized or unauthorized, constitutes consent to monitoring. Evidence collected or obtained by the College during monitoring may be used for administrative, law enforcement, disciplinary, or other adverse action.
- B. A list of the standard software load, limited support software and examples of unauthorized software is on the College website under IT Services.
- C. System Administrators and providers of College computing and information technology resources have the additional responsibilities of ensuring the integrity and availability of the resources they are managing, as well as of safeguarding the confidentiality and security of the systems from unauthorized access. Persons in these positions are granted significant trust and access on condition that they will use such access appropriately and only for its intended purposes and only when required to maintain the system. Any information not generally accessible that is seen by such persons in carrying out their duties is to be treated in the strictest confidence, unless it relates to or evidences a violation of law or College rules or policy or the security of the system in which case it should be brought to the attention of appropriate staff of the rank of Dean or higher for appropriate action.

4. Standards of Acceptable and Ethical Use

- A. Both the user-community as a whole and each individual user must abide by the following:
 - 1) Use only those computing and information technology resources that the user has been authorized to use. For example, it is a violation:
 - a. to use resources the user has not been specifically authorized to use.
 - b. to use another's account and password or to share one's account or password with another.
 - c. to access files, data or processes without authorization from the Director of IT Network Services and/or MIS.
 - d. to intentionally or knowingly look for or exploit security flaws to gain system or data access.

e. to intentionally or unintentionally share protected College information assets without authorization.

B. Employ computing and information technology resources only for their intended and authorized purposes. For example, it is a violation:

- 1) to send forged e-mail.
- 2) to misuse Internet Relay Chat (IRC) software to allow users to hide or attempt to hide their identities, or to interfere with other systems or users.
- 3) to use electronic resources for harassment or stalking other individuals.
- 4) to send bomb threats or "hoax messages."
- 5) to send chain letters.
- 6) to intercept or monitor any network communications not intended for the employee.
- 7) to use computing or network resources for advertising or other commercial purposes.
- 8) to use information systems or electronic communications for non-College consulting, commercial, or employment purposes.
- 9) to attempt to circumvent security mechanisms.
- 10) to use privileged access for other than official duties.
- 11) to use former privileges after graduation, transfer or termination.

C. Safeguard and protect access to and integrity of computing technology and information assets, and information resources. For example, it is a violation:

- 1) to intentionally or negligently release a virus or worm that damages or harms a system or network.
- 2) to prevent or obstruct others from accessing an authorized service.
- 3) to send email bombs that may cause service problems or disrupt service for other users.
- 4) to deliberately or knowingly degrade performance or deny service, including use or installation of internet file sharing, internet chat/Instant Messaging software and the continuous use of streaming audio or video for personal use (for example, listening to Internet radio).
- 5) to corrupt or misuse information.

- 6) to share, alter, delete or destroy – without authorization – information or data created or procured for use by the College in its business or educational activities.
- 7) to install or download any software without appropriate authorization from the Network Server Analysts, or to attempt to do so.

D. Abide by applicable laws and College policies, and respect the copyrights and intellectual property rights of others, including the copyrighted software rights of others.

It is the intent of Metropolitan Community College that this College adhere to the provisions of the United States Copyright Act (Title 17 of the United States Code) and Congressional guidelines. This statement, and the Copyright manual available at the College Library's webpage (<http://www.mccneb.edu/library/facultyservices/copyright.asp?Theme=3>) together form a guide for using materials protected by copyright. The College does not condone the illegal use of reproduction of copyrighted materials in any form. Students, authorized contractors, and employees who willfully disregard the Metropolitan Community College copyright statement, or specific conditions described in the manual, do so at their own risk and assume all liability.

For example, it is a violation:

- 1) to copy or redistribute copyrighted software, without the written authorization of the copyright owner.
- 2) to operate or participate in pyramid schemes.
- 3) to distribute pornography to minors or to acquire pornography for distribution to minors.
- 4) to upload, download, distribute or possess child pornography.
- 5) to access, upload, download, distribute or possess obscene material. Material is "obscene" if its predominant theme is prurient according to the sensibilities of an average person of the community, it depicts sexual conduct in a patently offensive way and, taken as a whole, it lacks serious literary, artistic, political or scientific value.
- 6) to copy or redistribute copyrighted material such as music, movies, and television shows, without the written authorization of the copyright owner. This includes illegally uploading, downloading, reproducing, and distributing copyrighted material via peer to peer (P2P) file sharing tools.

E. Respect the privacy and personal rights of others. For example, it is a violation:

- 1) to tap a phone line or run a network "sniffer" without written authorization from the Director of IT Network Services.

- 2) to access or attempt to access another individual's password or data without explicit authorization from the Director of IT Network Services and/or MIS.
- 3) to access or copy another user's electronic or voicemail, data, programs, or other files without permission from the Executive Vice President or Vice President of Technology and Administrative Services.

F. Abide by applicable laws, contractual agreements, and College policies regarding securing College information assets:

It is the intent of Metropolitan Community College that the College information assets must be available to the College community, protected commensurate with their value, and must be administered in conformance with applicable laws, contractual agreements, and College policies. Reasonable measures shall be taken to protect these assets against accidental or unauthorized access, disclosure, modification, or destruction, as well as to reasonably assure the confidentiality, integrity, availability, and authenticity of information assets. Reasonable measures shall also be taken to reasonably assure availability, integrity, and utility of information systems and the supporting infrastructure.

Students, authorized contractors, and employees who willfully disregard the Metropolitan Community College information security statement above, do so at their own risk.

Examples of applicable laws, contractual agreements, and College policies include:

- 1) Federal Education Rights Privacy Act (FERPA)
- 2) Payment Card Industry Data Security Standards (PCI-DSS)
- 3) Red Flag Rule - Identity Theft Prevention Program PM X-30
- 4) Health Information (HIPPA)
- 5) Gramm-Leach-Bliley ACT
- 6) Nebraska Data-Security Law

5. Failure to Comply

- A. Failure to comply with the foregoing provisions on acceptable use of the College's information resources threatens the atmosphere for the sharing of information and the free exchange of ideas as well as the security of the environment for creating and maintaining information.
- B. A user-community employee or student member who persistently, negligently or deliberately abuses information technology resources is subject to disciplinary action. (Reference Procedures Memorandums V-4, Student Conduct and Discipline and VI-24, Discipline and General Work Expectations for College Staff.) Every member of the College user-community has an obligation to report suspected or known violations. Such reports should be made to the appropriate supervisor, educational or administrative area.

- C. The College may restrict, prohibit or deny the use of all or any part of its information resources in response to violations of property rights or interests, College policies, or state or federal laws. If deemed warranted, the College may also institute and impose any other disciplinary action considered appropriate by the College. (Reference Procedures Memorandums V-3, Grievance Procedures for Alleged Discrimination – Students and VI-4, Grievance Procedures for College Staff.)

Adopted 12/01/02; Revised 9/5/03; 8/23/06 (title changes only); Reviewed but no changes 2/12/08;
Revised 8/27/10