MCC ACCEPTABLE USE OF TECHNOLOGY POLICY

Category: Technology	**Date Approved:** 1998
Responsible Office: Technology Services	**Date Revised:** Click to enter a date.
Responsible Executive: CFO/VP, Administrative Services	**[To be completed by Administration]**

Summary

MCC computer facilities and systems are intended for appropriate College-related work. MCC computer systems are a public resource and users should have no expectations of privacy while using the resources. Computer systems will be monitored for software not approved by the College.

Policy

POLICY STATEMENT

Individuals using MCC's computing technology, facilities, or equipment are NOT permitted to:

- Copy, download, change, distribute or modify any computer programs in part or whole from a website, textbook, or another individual without the written consent or permission of the owner. This may be considered plagiarism and/or a violation of copyright and patent laws.

- Install non-College-related software or downloads.

- Use MCC facilities and systems for the purpose of advertising or running an organization or business not affiliated with the College.

- Send, view, and/or print lewd or pornographic materials unless directly authorized in writing by the appropriate College officer or their designee.

- Reveal their password to anyone including employees, or let another person use their MCC account. Users are responsible for what is done with their MCC account.

- All data stored on College resources is property of the College, but that does not give any individual permission to access, change, copy, delete, distribute, and/or read electronic data of individual email or personal file storage without the permission of the owner. Shared data locations are meant for collaborative work and as such, changes to files are permitted but limited to the rights afforded by the network administrators. Exceptions to this policy will be allowed for the investigation of potential abuses of College resources by the appropriate College personnel.

- Engage in malicious activity designed to harm computers and networks. Such activity includes but is not limited to: hacking systems; disabling or crashing systems; network sniffing; sending viruses, malware or mass email; creating unnecessary or multiple jobs and processes.

- Bypass accounting or security mechanisms, circumvent data-protection or system consistency schemes, or uncover security loopholes.

- Harass others by sending annoying, obscene, libelous, or threatening messages.

- Aid or abet another person in violating any part of this policy.

- Violate any other state, local or federal laws or regulations pertaining to cyber security.

BACKGROUND

This policy is intended to comply with and augment all local, state, and federal laws. Individuals who violate any part of the policy will be subject to College disciplinary action (in accordance with all applicable collective bargaining agreements), criminal prosecution, or civil action as determined by College and legal authorities. Use of MCC computer systems is a privilege that may be revoked during the investigation of an alleged violation, or a finding of violation of this policy.

APPLICABILITY

This policy applies to all members of the College community with access to the College network resources including but not limited to affiliated organizations, employees, students, volunteers, vendors, and visitors.

DEFINITIONS

Users – Any person who has an MCC Network Account and is permitted to use MCC network resources.

RESPONSIBILITY

Associate Vice President/CIO
Director, Communications and Network Services/CISO

Contact Information

Technology Services

Related Information

The MCC Acceptable Use of Technology Policy is a revision of 6.1 Code of Conduct for Users of College Computer Systems.