Monroe County Community College
IT Acceptable Use Policy

Policy Type: District Policy

Policy Title: IT Acceptable Use Policy

Who Does the Policy Affect: Administrators, Faculty, Staff, and Students

NETWORK INFORMATION TECHNOLOGY SYSTEMS PURPOSE

MCCC owns and operates a variety of systems (hardware, software, and networks), which are provided to support, improve, and promote education and programs in the College community. The systems are intended to facilitate collaboration and exchange information among faculty, staff, students, and state, national, and international educational entities, as well as to promote access to international information resources. The systems are to be used only for education, research, academic development, and public service.

This document establishes rules and prohibitions that define acceptable use of information technology systems. Unacceptable use is prohibited and is grounds for loss of computing privileges, disciplinary action and/or prosecution under federal, state, and local laws. MCCC reserves the right to access all data and files on college-owned information technology systems at any time.

INFORMATION TECHNOLOGY SYSTEMS USER RESPONSIBILITIES

Information technology systems provide access to resources on and off campus and with other academic and other users worldwide. Such open access is a privilege and requires that individual users act responsibly. MCCC information technology systems may not be used for any purpose which is illegal, unethical or inconsistent with the mission of the College or this policy, or other activities likely to subject the college to liability.

USERS MUST:

- Respect the privacy of other users; for example, users shall not intentionally seek information on, obtain copies of or modify files, other data or passwords belonging to other users or represent themselves as another user unless explicitly authorized to do so by that user;
- Obey all relevant laws, including, without limitation, the Copyright Act;
- Preserve and safeguard the integrity and confidentiality of data created by others;
- Respect the integrity of information technology systems; for example, users shall not intentionally develop programs that harass other users or infiltrate a computer or computing system and/or damage or alter the software and hardware components of a computer or a computing system;
- Follow proper procedures established for all information technology use; and
- Report infractions of this policy.

USERS SHALL NOT:

- Use a disproportionate amount of information systems technology resources for non-educational purposes;
- Use information systems maliciously with or without intent (including, but not limited to, hacking) or in any way which violates applicable laws or regulations;
- Use information systems for commercial or for-profit purposes, political lobbying, religious material or personal advertisement;
- Display or send obscene, sexual, graphic or violent material except for legitimate academic research;
- Use the information technology systems in a way which harasses, threatens, intimidates or defames others; and,

- Gain or enable unauthorized access to resources or data; and,
- Attempt to circumvent or subvert system or network security measures.

SYSTEM MAINTENANCE AND SECURITY

File or account users will be notified of maintenance, in advance, whenever possible. When performing system maintenance, the college strives to ensure the integrity of a user's files. Although reasonable efforts are made, the college cannot and does not guarantee the security of the information technology system. Users should be aware that electronic mail is extremely vulnerable to unauthorized access and modification.

MCCC RIGHT TO INSPECT

MCCC reserves the right to inspect, monitor, and examine any college-owned information technology system, computing resource and/or computer files contained therein at any time. Users should not have an expectation of privacy for information contained on any information technology system.

CONSEQUENCES OF UNACCEPTABLE BEHAVIOR

This acceptable use policy does not attempt to catalog or exhaustively detail all required or proscribed uses or behavior. The Vice President of Finance & Administration may at any time make determinations that particular uses are or are not consistent with the purposes of the MCCC information systems, and may take action accordingly.

Infractions of this policy, which are deemed minor by the college, will typically be handled internally by the appropriate administrator. More serious or repeat violations of this policy shall subject users to the regular disciplinary processes and procedures of the college for students, staff, administrators and faculty. Illegal acts involving the college information systems may also subject violators to prosecution by local, state and/or federal authorities.

EMAIL AND ELECTRONIC COMMUNICATION

Access to MCCC email is a privilege that may be wholly or partially restricted without prior notice and without consent of the user.

An activity that may strain the email or network facilities is a violation of this policy. These activities include, but are not limited to:

- Sending chain letters and widespread dissemination of unsolicited email.
- Modification or forging of email information, including the header, is prohibited.
- Confidentiality of email or other electronic communication cannot be assured; therefore, users should be aware of the risks when sending confidential, personal, financial, or sensitive information.

By opening and using your e-mail account, Authorized Users agree and consent that the College owns, and may access the account for administrative and all other purposes permitted or required by law and/or the College's policies, procedures and ordinances, which may require the College or its e-mail provider (if applicable) to access and disclose to the College any information stored within the account. The College does not centrally retain or archive e-mail sent, processed or received by the College e-mail system. E-mail may be retained, stored or archived by external providers of e-mail services.

OPERATIONAL SECURITY

MCCC may, without advance notice to users, take any action necessary to protect the interests of MCCC to ensure that the IT resources are stable and secure. Any action necessary will be taken, but not limited to monitoring and scanning MCCC resources.

Third-party intrusions, viruses, and physical access can compromise computing and communication security. MCCC takes reasonable precautions to minimize risks. Users must notify and report incidents to the *Security Administrator*.

Known or suspected violations of the Acceptable Use Policy or Social Media Policies should be reported immediately to the *Chief Information Officer*.