MCCC **OMB 946**

USE OF TECHNOLOGY

1. PURPOSE

The purpose of this policy is to outline the College users' rights and responsibilities regarding appropriate use of the College Information Systems. This policy is not intended to cover every situation, but instead to provide general guidelines for all users.

2. DEFINITIONS

Mercer County Community College Information Systems refers to all information technology resources including but not limited to computers, networks, network user accounts, servers, printers, software, phone and voicemail systems, electronic mail, and web pages developed, maintained and/or managed by the College and/or its affiliates.

3. THE POLICY

Mercer County Community College User refers to any College student, faculty, staff, or affiliate using the College Information Systems.

Mercer County Community College IT Administrator refers to any individual with express permission and authority from the College to administer and facilitate access to the College Information Systems.

Mercer County Community College User Account refers to any account assigned by a College IT Administrator to faculty, student, staff, or affiliate. A user who has been assigned a user account has permission to use the College Information Systems within the parameters determined by the IT Administrator, this Appropriate Use policy, and other College policies and regulations.

Restrictions

The College reserves the right to protect its Information Systems and to restrict user access to Information System activities that are related to the College. These systems are primarily intended for the academic, educational, and research purposes of the College. The College reserves the right to define what constitutes unauthorized use.

The College and its users must comply with relevant federal and state laws, including but not limited to, appropriate use, copyright and fair use, and privacy laws.

The Support for Employee-Owned Computers and Equipment

The College will only provide support for College-owned equipment and software.

The College will bear *no* responsibility if the installation or use of any College software on employee-owned computers causes system lockups, crashes, or complete or partial data loss on employee-owned equipment.

Usage
Computers, computer files, internet access, and software furnished to employees at Mercer County Community College are primarily for business purposes and employees are responsible for seeing that these systems are used in a professional, ethical, and lawful manner. Any personal use of these systems may not interfere with the person's job responsibilities and cause any harm or embarrassment to Mercer County Community College.

Employees should not access confidential files, or retrieve any stored confidential communication without authorization.

The College purchases and licenses the use of various computer software for business purposes and does not own the copyright to this software or its related documentation. Unless authorized by the software developer, the College does not have the right to reproduce such software for use on more than one computer. Any employee who circumvents those legal restrictions for access bear legal responsibilities on their own.

Employees may only use software on local area networks or on multiple machines according to the software license agreement. The College prohibits the illegal duplication of software and its related documentation.

Unless permission is granted by the Information Technology Department, employees are not permitted to install or copy software on College equipment. Only software that is licensed to or owned by the College is to be installed on College computers.

Network User Accounts
To utilize the Mercer County Community College network, the College requires all users to log on with the accounts that have been provided to them by the Office of Information Technology. Users are strictly prohibited from sharing user account information with others or using someone else's user account, with or without their permission. Any users suspecting unauthorized use of their accounts are responsible for changing their passwords and/or contacting the Office of Information Technology through the help desk to have their accounts temporarily or permanently disabled.

Appropriate Use of Information Systems
Users are responsible for using the College Information Systems in a professional, ethical, and lawful manner. Usage that conflicts with this policy is prohibited. Such usage may include, but is not limited to the following:

- Supporting commercial interests not related to the work of the College.
- Initiating or propagating electronic chain mail, commercial mailings, or other mass mailings in violation of the CAN-SPAM Act of 2003.
- Intentionally introducing viruses, worms, Trojan horses or other malicious activity.
- Engaging in any activity that interferes with the proper operation of the College Information Systems.
- Installing software on College computers without the authorization of an IT Administrator.
- Tampering or interfering with the intended use of the College Information Systems.
- Engaging in any unauthorized activities that result in monetary charges or non-

monetary harm to the College.

- Engaging in any unauthorized activities that result in monetary or non-monetary gains for individual users.
- Using the College Information Systems to convey fraudulent, defamatory, harassing, obscene, or threatening messages or material and/or any communications prohibited by law.
- Using the College Information Systems to engage in illegal file sharing or any other illegal activities.

Electronic Harassment

The College has set forth explicit policies in the student and faculty/staff handbooks regarding harassment. Harassment within the context of the College Information Systems is prohibited and all incidents will be dealt with according to the relevant College policies and procedures.

Privacy

The College is responsible to ensure its compliance with the Family Educational Rights & Privacy Act (FERPA), the USA Patriot Act of 2001, U.S. Privacy Act, and the Electronic Communications Privacy Act (ECPA). The College takes all necessary and reasonable measures to safeguard the privacy of students' electronic files and communications within the College Information Systems. However, users of these Information Systems should be aware of the inherent limitations of shared information system resources. The College cannot guarantee the privacy or confidentiality of stored information or electronic communications.

As part of the ongoing efforts to ensure compliance and safe guard, at all times, the College has the right to monitor and access a user's communications, files, stored information, and activities using the College Information Systems pursuant to state and federal law and College policies.

If the College monitors or accesses a user's files, communications, or activities using the College Information Systems, it will respect that which is privileged or otherwise protected from disclosure by law.

Sanctions

Violation of these policies may result in the temporary or permanent disabling of the user account, depending on the severity of the offense. Other sanctions, up to and including dismissal and/or termination and prosecution under state and federal law, may apply.

Approved:

<u>Board of Trustees</u>
November 12, 2009

Revised:

<u>Board of Trustees</u>
February 22, 2018