USE OF TECHNOLOGY

1. POLICY STATEMENT

In support of Mercer County Community College Mission, academic instruction, research, and administrative functions, Mercer County Community College encourages the use of, and provides access to, information technologies, systems, email and network resources. Technology use policy is adopted by Mercer County Community College to allow for the proper use and management of all Mercer County Community College computing, systems and network resources. These guidelines pertain to all Mercer County Community College campuses regardless of the networks or systems operated.

The Mercer County Community College grants access to its networks and computer systems subject to certain responsibilities and obligations set forth herein and subject to all local, state, and federal laws. Appropriate use should always be legal, ethical and consistent with the Mercer County Community College mission.

Users must realize that providing access is a privilege provided by the Mercer County Community College and should be treated as such. Enforcement of established rules will help to provide a benefit to all users.

Mercer County Community College views the systems, network and computing resources as shared resources and the use of these as a privilege. The primary purpose of these resources is to allow access to information that will support the Mercer County Community College administration, educational process and Mercer County Community College mission. Thus, network abuse or applications that inhibit or interfere with the use of the network by others are not permitted.

Should it be determined that network traffic being generated from any connection is drastically inhibiting or interfering with the use of the Mercer County Community College systems, network and computing resources by others, Mercer County Community College reserves the right to terminate any user's access without notice.

2. AUTHORIZED USE

An Authorized User is any person who has been granted authority by Mercer County Community College to access its systems, computing and network resources and whose usage complies with this policy. Authority to use a particular Mercer County Community College technology resources should come from the campus unit responsible for operating the resource. Unauthorized use is strictly prohibited.

3. PRIVACY

Users must recognize that there is no guarantee of privacy associated with their use of Mercer County Community College technology resources. The College may find it necessary to view electronic data and it may be required by law to allow third parties to do so (e.g. electronically stored data may become evidence in legal proceedings). It is also possible that messages or data may be inadvertently viewed by others.

Any information traffic sent over Mercer County Community College network and technology resources, whether wire or wireless, becomes Mercer County Community College property. Users cannot have any expectation of privacy concerning this information, its source, or its destination.

4. INDIVIDUAL RESPONSIBILITIES

A. Common Courtesy and Respect for Rights of Others

All users are responsible to respect and value the privacy of others, to behave ethically, and to comply with all legal restrictions regarding the use of electronic data. All users are also responsible to recognize and honor the intellectual property rights of others.

Communications on Mercer County Community College computers (which includes any personal devices registered on the College Network, regardless of ownership) or networks (which includes wired, wireless and remote access via VPN) or approved cloud resources (which includes Teams, Skype and social media) should always be businesslike, courteous and civil. Such systems must not be used for the expression of hostility or bias against individuals or groups, offensive material such as obscenity, vulgarity or profanity, inappropriate jokes or other non-businesslike material. Sexually explicit material, cursing and name-calling are not appropriate communications. Users who engage in such activity will be subject to disciplinary action. For greater clarity, the transmission of inappropriate communications or offensive information at any time via any medium by one member of Mercer County Community College community to another (including communications originating on or received by college and non-College computers) is unacceptable.

No user may, under any circumstances, use Mercer County Community College computers or networks to libel, slander, or harass any other person. The following are examples of Computer Harassment:

1) intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family;
2) intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease;
3) intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease (such as debt collection);
4) intentionally using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another; or

5) intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

B. Content

Users who make use of forums, chat rooms or social networking sites do so voluntarily, with the understanding that they may encounter material they deem offensive. Neither Mercer County Community College nor IT assume any responsibility for material viewed on these network communication utilities.

Furthermore, IT reserves the right to limit access to any content deemed offensive or lacking in educational value

To ensure security and prevent the spread of viruses, users accessing the Internet through our network and computing resources must do so through Mercer County Community College Internet firewall.

C. Copyright Infringement & Peer-To-Peer File Sharing

Under the Digital Millennium Copyright Act and Higher Education Opportunity Act (H.R. 4137), illegal distribution of copyrighted materials and distribution of copyright materials is illegal and may be punishable by law. These materials include, but are not limited to the unauthorized distribution of songs, videos, games, textbooks, or other type of creative content.

In addition to any other charges that might be brought against you, the copyright holder can file suit, which can result in legal fees and damages that must be paid.

Therefore, peer-to-peer file sharing is not allowed and is blocked on Mercer County Community College network using bandwidth shaping technology. Mercer County Community College is legally obligated to assist authorities in identifying individuals who violate copyright law pertaining to peer-to-peer file sharing. It is also in violation of school's policy to use technology designed to circumvent the blocking of this activity.

D. Responsible Use

All users are responsible for refraining from all acts that waste Mercer County Community College technology and network resources or prevent others from using them. Each user is responsible for the security and integrity of information stored on both his/her Mercer County Community College issued and personal. Computer or portable device, which may include but is not limited to desktops, laptops, tablets, phones cell phones etc. Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with or used by others. All users must maintain confidentiality of student information in compliance with the Family Educational Rights and Privacy Act (FERPA) of 1974.

E. Confidential Data and Personal Computer Security

Mercer County Community College private data must be stored on Mercer County Community College-owned computers or Mercer authorized sites. Personally identifiable information (individual names, phone numbers, addresses, grades, etc...) and other confidential information related to College activities must not be stored on individual faculty or staff personal computers

or other personally owned electronic devices including mass storage hard drives, USB devices, cell phones, or any other device that has storage capabilities. In addition, no personal mass storage device should be connected to the Mercer County Community College Administrative network or administrative devices including PC, workstations, laptops, servers, or other hardware.

F. Permitting Unauthorized Access

All users are prohibited from running or otherwise configuring software or hardware to intentionally allow access by unauthorized users.

G. Use of Privileged Access

Special access to information or other special computing privileges is to be used in the performance of official duties only. Information that is obtained through special privilege is to be treated as private.

H. Termination of Access

Whenever a user ceases being a member of Mercer County Community College community or if such user is assigned a new position and/or responsibilities within Mercer County Community College, such user shall not use facilities, accounts, access codes, privileges, or information for which he/she is not authorized in his/her new position or circumstances. It is the responsibility of the department head to notify the Information Technology Services Department of any change in user responsibility that affects system access. Upon termination, Mercer County Community College owned information on personal devices must be removed by the individual.

Upon separation of employment, the individual's College email, network access and College software systems will be disabled on their last day of work. Approved Emeritus Professors will be issued a new MCCC email account per OMB 978, Emeritus Rank for Faculty Members.

Note – this is related to FERPA where non-employees should not have access to confidential and sensitive information of students and staff.

I. Unauthorized Activities

Users are prohibited from attempting to circumvent or subvert any security measures implemented for the Mercer County Community College computing and network systems. The use of any computer program or device to intercept or decode passwords or similar access control information is prohibited. This section does not prohibit use of security tools by IT system administration personnel.

Deliberate attempts to degrade the performance of a computer system or network or to deprive authorized users of access to or use of such resources are prohibited.

J. Denial of Service Attacks

Denial of service attacks, 'fire bombing', 'Flaming', 'hacking', 'cracking', and any other type of malicious or mischievous intrusion or network attack against any network and computing resource user, any host on Mercer County Community College Network, or any other host on the Internet by any member of Mercer County Community College community will be grounds for immediate removal of said individual from the Mercer County Community College network.

K. Harmful Activities

The following harmful activities are prohibited: creating or propagating viruses; disrupting services; damaging files; intentional destruction of or damage to equipment, software or data belonging to Mercer County Community College and the like.

L. Unauthorized Access

All users are also strictly prohibited from:

1) damaging computer systems;
2) obtaining extra resources without authority;
3) depriving another user of authorized resources;
4) sending frivolous or excessive messages (e.g. chain letters);
5) gaining unauthorized access to Mercer County Community College computing and networking systems;
6) using a password without authority;
7) utilizing potential loopholes in Mercer County Community College computer security systems without authority;
8) using another user's password; and
9) accessing abilities used during a previous position at the Mercer County Community College.

M. Tampering of Equipment or Resources

No computer equipment, including peripherals, networking resources or software applications will be moved from its current location without authorization from IT. This includes the tampering, modification, or additions to network software, hardware or wiring.

N. Use of Licensed Software/Downloading

No software may be installed, copied, or used on Mercer County Community College resources except as permitted by the owner of the software and by law. Software subject to licensing must be properly licensed and all license provisions (installation, use, copying, number of simultaneous users, term of license, etc.) must be strictly adhered to.

Only authorized personnel may install legal software on Mercer County Community College-owned resources. The downloading of software via the Internet is prohibited due to the possibility of legal, or copyright ramifications.

O. Personal Business, Political Campaigning, and Commercial Advertising

Mercer County Community College computing and network systems are a College-owned resource and business tool to be used only by authorized persons for Mercer County Community College business and academic purposes. Except as may be authorized by Mercer County Community College, users should not use Mercer County Community College computing facilities, services, and networks for:

1) compensated outside work;
2) the benefit of organizations not related to Mercer County Community College, except in connection with scholarly pursuits (such as faculty publishing activities);
3) political campaigning;
4) commercial or personal advertising; and/or
5) the personal gain or benefit of the user.

5. SECURITY

A. System Administration Access

Certain system administrators of Mercer County Community College systems will be granted authority to access files for the maintenance of the systems, and storage or backup of information.

B. Mercer County Community College Access

Mercer County Community College may access usage data, such as network session connection times and end-points, CPU and disk utilization, security audit trails, network loading, etc. Such activity may be performed within the reasonable discretion of IT management, subject to Mercer County Community College approval.

C. Availability

IT will make every effort to insure the operation of Mercer County Community College network and the integrity of the data it contains. In order to perform needed repairs or system upgrades IT may, from time to time, limit network access and/or computing resources for regular or unexpected system maintenance. IT will make every effort to give notice of these times in advance, but makes no guarantees.

D. Departmental Responsibilities

Each Mercer County Community College department has the responsibility of:

1) enforcing this policy;
2) providing for security in such department areas;
3) encouraging users to save all files to a network drive (network drives are backed up every day where local drives are not and external media tend to be less reliable); and
4) notification of personnel changes.

E. Wireless Access Points

The Information Technologies department provides wireless service for use by Mercer County Community College faculty, students, and staff. Wireless access is also available to the public at large for limited internet access only. Since wireless is provided centrally by IT, the installation of private wireless access points (APs) and other devices used to boost wireless signal coverage is not allowed on campus. These devices can and do interfere with Mercer County Community College centrally provided wireless network system. The IT department will take steps to shut down any personal network access devices used.

F. Virus Protection and Device Security

All Mercer County Community College computers, including file servers, utilize virus detection software. All personnel devices such as desktops, laptops or any other device that may compromise the security of Mercer County Community College network is required to utilize a fully functioning and updated virus detection software application. In addition, all personal devices must be fully updated with the most recent vendor supplied security patches.

G. Remote Access

All remote access to Mercer County Community College (MCCC) applications, systems and hardware shall be authorized and approved in advance, and any access not explicitly authorized and approved is prohibited. Remote access to specific applications, systems, components and technology infrastructure shall only be granted to users with a legitimate business or academic need for such access. The level of access granted and privileges assigned shall be limited to the minimum required to perform assigned duties.

Employees and third parties authorized to utilize remote connections shall ensure that unauthorized users are not allowed access to the MCCC internal network utilizing these connections. All individuals and machines, while accessing the network, including college - owned and personal equipment, are an extension of MCCC's network.

All devices, including personally-owned computers, that are connected to the network via remote access technologies must use the most up-to-date anti-virus software, and be up-to-date on available patches. Security patches for installed operating systems (with auto-update enabled), web browsers, and common applications shall be applied. A firewall must be enabled on each applicable device.

Remote access to data or services may not be used to copy private or personal information such as that residing on a privately owned computer, to company file shares, or other company-owned information systems.

Remote access to data or services may not be used to store College information on a personal system, file share or other non-College owned system without prior approval from management.

6. PROCEDURES AND SANCTIONS

A. Responding to Security and Abuse Incidents

All users and departmental units have the responsibility to report any discovered unauthorized access attempts or other improper usage of Mercer County Community College computers, networks, or other information processing equipment. If a security or abuse problem with any Mercer County Community College computer or network facility is observed by or reported to a user, such user shall immediately report the same to such user's department head and/or the Chief Information Officer.

B. Range of Disciplinary Sanctions

Persons in violation of this policy are subject to a full range of sanctions, including, but not limited to, the loss of computer or network access privileges, disciplinary action, and dismissal from the Mercer County Community College. Some violations may constitute criminal offenses, as defined by local, state, and federal laws and Mercer County Community College may prosecute any such violations to the full extent of the law.

C. Employees on Family Medical Leave Act (FMLA), Workman's Compensation (WC) and other leaves are limited to incidental work and will continue to have access to email and the network; however access to College software systems will be limited to "read only access". Exceptions can be approved by the Human Resources Department for intermittent FMLA or restricted WC work duties pertinent to the individual cases.

7. AMENDMENTS

Mercer County Community College reserves the right to amend or revise the policies herein as needed. Users will be provided with copies of these amendments whenever possible.

Board of Trustees
November 12, 2009

Revised:
February 22, 2018
March 18, 2021