H. Councill Trenholm State
Computer Systems Acceptable Use Policy

This policy defines acceptable uses of computer hardware, software, networks, and communication lines, Internet access, and Email transmissions, herein referred to as systems. H. Councill Trenholm State Community College faculty and staff must read this policy before being granted access to the College Systems. Violations of this policy may result in restricted use of Systems and/or disciplinary action.

Systems are provided for business purposes only, and faculty, staff and students are encouraged to utilize this technology as a tool to efficiently perform their job tasks.

Systems are owned by the College and subject to access by the Information Technology division for maintenance, repair, updating, or monitoring. Documents, spreadsheets, database, and Email transmissions on any System may be subject to examination at anytime. Users must comply with all Federal, State, or local laws and regulations, and applicable policies of accessed networks such as the Alabama Research and Education Network.

Statement on Appropriate Use of Information Technology
Facilities and Services

1. Trenholm State Community College is committed to ensuring a working and learning environment in which all persons treat others with humanity and respect.

2. The user bears the primary responsibility for the material that he or she chooses to access, send or display.

3. Instructors teaching programs requiring the placement of equipment on the College network must submit in writing to the President, a request to install equipment on the college network. Request must include the intended use of such equipment and controls to be implemented by the instructor insure their students do not interfere with the administrative network resources. Instructors are solely responsible for the actions of their students in the classroom.

4. The user must use the computing facilities and services in a responsible fashion. This requires that the user:

• Respect the legal protection provided by copyright and license to programs and data.

• Respect the privacy of others by not tampering with their files, passwords, or accounts, or representing others when messaging or conferencing.

• Will not interfere with others access to computing facilities and services

• Use on computer IDs or accounts and communication facilities that the user is duly authorized to use, and use them for the purposes for which they were intended.

Revised – July 6, 2017

• Will not make excessive demands on network resources and capacity, for example by listening to Internet radio/or viewing streaming media not directly related to the business of the College.

• Respect the integrity of computing systems and data; for example, by not intentionally developing programs or making use of already existing programs that harass other users, or infiltrate a computer or computing system, and/or damage or subvert the software components of a computer or computing system, or gain unauthorized access to other facilities accessible via the network, or attempt to reverse engineer or interfere with college administrative or instructional operations.

• Use computing and communication facilities in a manner that is consistent with the ethical principles set forth by the College and with accepted community standards.

• Does not bring or attempt to use software otherwise known as password sniffers within the college network. This software is explicitly illegal within the college network and any use will lead to suspension of computer services and disciplinary actions.

5. Information Services will suspend the computing privileges of anyone contravening these guidelines.

Statement on Email

1. There is no guarantee or expectation of privacy with an email message; email is easily re-distributed, and can (with specialized equipment) be read in transit. With this in mind, users should take care in the phrasing and content of messages they send. Use of online email systems through the college network such as Gmail, Yahoo, and AOL for example are not stored on equipment owned by the State, however content submitted via the web to these providers are subject to monitoring. Therefore no expectation of privacy should be expected when using the college systems to access these external systems.

2. Any unauthorized attempts to read, copy, modify or delete email messages of other users is prohibited. Modification of message headers can be detected and strictly prohibited.

3. Only those who have been permitted to use the email system and have been granted a password may use the system. Unauthorized use is prohibited.

Statement on Use of the Internet

1. Every Internet site visited using the system is capable of identifying the user as a representative of the College. Accordingly, all activity on the Internet must be governed by discretion and good judgment.

Revised – July 6, 2017

2. Use of the college network in an attempt to gain unauthorized access to remote systems is prohibited or any system you are not explicitly authorized is prohibited. Internet bandwidth is available throughout the college in the following capacities:

Wired – 250MB/sec

Wireless – Secured 250MB/sec, Open 160MB/sec

The Digital Millennium Copyright Act (DMCA)
Peer-to-Peer File Sharing Policy

Copying, distributing, and downloading copyrighted materials, including music, videos, and games for which you do not have the owner's (copyright holder's) permission are a violation of federal law. Compliance with federal copyright law is expected of all students, faculty, and staff. If you download and/or distribute unauthorized copies of copyrighted music recordings and movies, you are breaking the law and may be held legally liable for thousands of dollars in damages. Federal law provides severe penalties for the unauthorized reproduction, distribution, or digital transmission of copyrighted materials. The FBI investigates allegations of criminal copyright infringement and violators are prosecuted.

What Faculty/Staff Should Know

Most P2P software turns file sharing on by default as soon as the software is installed. This means that others may access materials on their computer without their knowledge, whether they have given permission or not. Downloading copyrighted music or movie files without permission is illegal. It is also illegal to share purchased music or movie files with others, again, whether they are aware that they have done it or not.

If they install P2P software, they should turn the file sharing options off. They should also be made aware that if they are sharing materials inadvertently, they are still liable for violating copyright law.

Distribution of copyrighted material, including music, games, and movies, for which you do not have the owner's permission is a violation of federal law and college policy.1 Popular file-sharing programs, such as KaZaA, LimeWire, Grokster, and Morpheus, commonly share downloaded music, movie and other files from your computer with users worldwide if you do not take specific actions to prevent this.

Copyright holders and their agents frequently scan colleges' networks for copyrighted materials (especially music, games, or movies) that are available to others from computer systems on the college network. The college receives many notices from organizations acting as agents for media companies, alleging copyright infringement by users of the college's computing network.

Alleged Repeat Offenders: The process for faculty/staff alleged "repeat offenders", i.e. for faculty/staff who are the subjects of more than one DMCA notice, is to permanently remove their access to the Internet and other disciplinary actions taken as determined by the individual's supervisor, dean and president as deemed appropriate.

Revised – July 6, 2017

Reporting Alleged Copyright Infringement Policy

Faculty, staff, students and affiliates utilizing college infrastructure must comply with U.S. copyright laws. The college reserves the right to remove or limit access to material posted on college-owned computers if it is alleged that U.S. copyright laws have been violated. If the college determines that U.S. copyright laws have in fact been violated, the infringing material will be permanently removed.

The Information Technology division shall periodically monitor the college network for violations of this policy and report findings to the appropriate Dean.

Statement on Security

1. No user is to give out their user password or other system access passwords to anyone except as approved by the Network.

2. Users of portable hardware or remote access hardware supplied by the College are responsible for ensuring that reasonable measures are taken to prevent the loss or theft of that equipment.

3. A computer must not be left logged onto the Network if a user anticipates being away from their desk for more than 30 minutes, or should be set to use a password protected screensaver.

4. Users shall not circumvent login procedures in order to gain access to the System.

5. Employee and student records are protected under Federal and State laws.

Statement on Software Licensing

1. Trenholm State Community College is taking an active role in the issue of software privacy. Please read and respect all copyright notices on all software that you use. The principles for using and managing software derived from U.S. copyright law and legal agreements in the form of licenses and purchase agreements. That foundation makes the basic policy governing software clear.

2. All faculty, staff, and students of Trenholm State Community College are required and expected to obey the laws and legal agreements governing software use. Failure to do so can lead to monetary damages and/or criminal penalties for the individual violator and the College. Only license software owned by the College will be installed and used on the College computers. Loading of personal software of any kind is prohibited. Some software may be installed for a limited time for evaluation purposes with approval of the software owner. Such evaluation should not exceed 30 days and the software removed if not purchased.

3. The following is a list of software licensed and approved for use on administrative computers:

Revised – July 6, 2017

Microsoft Windows 7 Pro
Microsoft Office 2010/2013/2016
Microsoft Publisher
IBM Client Access
Symantec Endpoint Antivirus
Grade Quick Current Version (where required)
Adobe Acrobat Reader (Free Version)

4. **Other Software**: Although the above list of software is a college wide standard, other software specific to departments may be installed on college computers if approved by the Network Coordinator, including software accompanying book purchases. All software and licenses must be on file in the office of the Network Coordinator and installed by the IT staff. If you are using such software, deliver the software and the license for file as soon as possible.

5. **Software for Student Labs**: Software for student labs varies by department. It is the responsibility of all department heads to ensure that student labs are using only license software and that copyrighted software is not copied and given to students without explicit approval from the software manufacturer. All licenses and software must be placed on file in the office of the Network Coordinator and installed by the IT staff. All lab software installation requests must be made with the Asst Dean of IT 15 days before the software will be required for use in a lab.