ROBESON COMMUNITY COLLEGE	INFORMATION TECHNOLOGY TECHNOLOGY SERVICES	POLICY 7.1

I. OVERVIEW

The College's technology systems include technology hardware, electronic mail and other forms of electronic communications, Internet access and use of computing devices. As the owner of property and services, the College has the right to monitor activities and to access information on the College's technology systems stored, sent, created or received by faculty, staff, students or other users. Any individual using the College's technology systems should not expect individual privacy in their use of the technology systems including, but not limited to, the use of the College's electronic mail system.

When using the College's technology systems, all users shall adhere to the College's information technology policies and procedures.

II. PUBLIC AND CONFIDENTIAL RECORDS

Unless otherwise confidential by law, records generated using the College's technology systems are considered public records and must be maintained as public records pursuant to the College's policies and procedures. Student education records and certain personnel information are protected by law and are confidential. For more information concerning student records, see Policy 5.4.3 – Student Records and for information concerning personnel records, see Policy 3.3.1 – Personnel Files.

Employees may not download confidential student and personnel information onto a personally owned electronic device or onto another network unless authorized by the President of the College or Chief Information Officer.

III. EMPLOYEE USE OF TECHNOLOGY SERVICES

Employees using the College's technology hardware, software, or systems should adhere to the following guidelines.

A. Employees shall adhere to Policy 7.2 – Internet and Network Acceptable Use Policy.

B. All computing devices, including portable computing devices such as laptops or tablets, shall

1. Use encryption or other measures to protect confidential information, including personal information, from unauthorized disclosure;

2. Be labeled with tamper-resistant tag, permanently engraved label or ID number, or both identifying the device as the College's property;

3. Be used in compliance with all applicable security requirements for the College's computers; and

4. Include password protection on such devices, if applicable.

C. The College's mobile technology equipment, such as laptops and tablets, may be used at home by College personnel provided:

1. Use of the equipment at home will not interfere with the College's operational needs;

2. Supervisor approval; and

3. Personnel return items to campus upon request for system maintenance, upgrades, inventory, and verification.

D. The College's Information Technology Services Department (ITS) maintains all of the College's technology equipment. ITS does not support the use and setup of the College's technology equipment on Internet, network and computing resources that are not owned and maintained by the College.

E. The College recognizes that employees may occasionally receive personal email on College computers, use College equipment to complete an online course and for other personal reasons. Personal use of College computers and equipment is acceptable provided that employees adhere to the following:

1. Personal use may not interfere with the College's operational needs;

2. Equipment may not be checked out solely for the purpose of personal use;

3. Users understand that data stored on College equipment or sent using College email or other communication methods is not private;

4. Users will adhere to all state and federal laws and the College's policies and procedures;

5. Equipment or information resources are not used for illegal, malicious or obscene purposes;

6. Equipment or information resources are not used to seek or exchange electronic information or software unrelated to one's job duties and responsibilities;

7. The College's data and information are not shared with unauthorized individuals;

8. All software copyright and licensing laws are followed;

9. Not use College passwords for non-college sites (e.g., social networking sites);

10. Not share sensitive College information or student details on social networking sites;

11. Equipment is not used for any political purposes, including nonprofit activities of a political nature;

12. Equipment is not used for private or personal for-profit activities. This includes personal use for marketing or business transactions, advertising of products or services, or any other activity intended to foster personal gain. Employees may not use College equipment or information resources in pursuit of private businesses operated by the employee or in pursuit of work for other agencies, colleges or businesses; and

13. Printers and photocopy machines may not be used for personal use.

Adopted: April 9, 2018

ROBESON COMMUNITY COLLEGE	INFORMATION TECHNOLOGY EMPLOYEE PERSONAL COMPUTER USE	PROCEDURE 7.1.1

Any College employee who wants to use personally owned electronic devices on campus can do so through wireless public access. When using personally owned equipment on the College's technology systems, employees are expected to adhere to all policies and rules regarding such use. The administration may create process and procedures regarding the approval process for an employee's personal electronic device in order to protect the integrity of the College's network and technology systems.

Adopted: April 9, 2018

ROBESON COMMUNITY COLLEGE	INFORMATION TECHNOLOGY INTERNET AND NETWORK ACCEPTABLE USE	POLICY 7.2

I. PURPOSE

The College strives to provide information technology access in an environment in which access is shared equitably among users. This access is intended to be used in support of the College's research, educational and administrative purposes. College owned or operated computer resources are for the use of College employees, students and other authorized individuals. This policy's purpose is to protect the College's technology users and computer resources and to ensure equitable access and proper management of these resources.

II. ACCEPTABLE USE

A. Acceptable Activity

The College's information technology resources are intended for the use of its students, employees and other authorized individuals for purposes related to instruction, learning, research and campus operations. Users are expected to exercise responsible, ethical behavior when using all College computer resources. This policy makes no attempt to articulate all required or prohibited behavior by users of the College's computer resources.

"Authorized Individual" shall mean any person, other than a student or employee, granted permission to access the College's internal network or allowed to use the College's information technology resources. Authorized Individuals are expected to adhere to this and other College policies when accessing the College's network and information technology resources.

B. Unacceptable Activity

Unacceptable activity includes, but is not limited to, the following:

1. Deliberately downloading, uploading, creating or transmitting computer viruses, malware, or other software intended to harm a computer or the College's network;

2. Destroying or modifying directory structures or registries or interfering or tampering with another individual's data or files;

3. Developing programs that infiltrate a computer or computing system, harass other users and/or damage software;

4. Attempting to obtain unauthorized computer access or privileges or attempting to trespass in another individual's work;

5. Using hardware or software sniffers to examine network traffic, except by appropriate College personnel, to diagnose the network for bottlenecks or other problems;

6. Using another person's password or sharing of one's own password (users should not share their password with anyone and those who choose to do so are responsible for the outcomes resulting from the use of their password);

7. Committing any form of vandalism on equipment, communication lines, manuals or software, or attempting to defeat or circumvent any security measures or controls;

8. Consuming food and/or beverages in computer labs, computer classrooms, library or in any other areas, unless otherwise authorized;

9. Wastefully using finite resources such as large amounts of bandwidth including but not limited to, downloading music, television shows, software programs, and/or movies;

10. Connecting personal network devices on the College's wired network. Connecting unsanctioned products (software or hardware) to the College network or installing products for personal use. Special provisions may be made for visiting artists, lecturers, and trainers at the discretion of the Director of Information Technology. Information Technology support staff can offer assistance in gaining network access under these special circumstances, but the College cannot guarantee functionality and assumes no responsibility for configuration of or damage to non-college equipment;

11. Using the College's computer resources and Network to engage in disruptive, threatening, discriminatory or illegal behavior or behavior that violates the Code of Student and/or Employee Conduct;

12. Disclosing confidential student or personnel information to unauthorized third parties;

13. Violating copyright laws and/or fair use provisions through: a) illegal peer-to-peer file trafficking by downloading or uploading pirated or illegal material including, but not limited to, software and music files; and b) reproducing or disseminating Internet materials, except as permitted by law or by written agreement with the owner of the copyright;

14. Other activities that interfere with the effective and efficient operation of the College or its Network or activities that violate the College's Policies and Procedures;

III. RESERVATIONS OF RIGHTS AND LIMITS OF LIABILITY

A. The College reserves all rights in the use and operation of its computer resources, including the right to monitor and inspect computerized files or to terminate service at any time and for any reason without notice;

B. The College makes no guarantees or representations, either explicit or implied, that user files and/or accounts are private and secure. No right of privacy exists in regard to electronic mail or Internet sessions on the College Network or College-owned hardware;

C. The College is not responsible for the accuracy, content or quality of information obtained through or stored on the College Network;

D. The College and its representatives are not liable for any damages and/or losses associated with the use of any of its computer resources or services;

E. The College reserves the right to limit the allocation of computer resources;

F. The College makes efforts to maintain computer resources in good working condition but is not liable for damages incurred by loss of service;

G. College funds may not be used to purchase personal network access or products; and

H. The College shall not be liable legally, financially or otherwise for the actions of anyone using the Internet through the College’s network or College’s computers.

IV. WIRELESS INTERNET ACCESS

The College provides free wireless Internet access. Users of wireless access must abide by the Wireless Internet Access Guidelines and this policy. Connection to the wireless network at any given time is not guaranteed. The College does not accept liability for any personal equipment that is brought to the College and, therefore, may not assist with configuration, installation, trouble-shooting or support of any personal equipment.

V. ELECTRONIC MAIL

The College provides free electronic mail accounts to certain College employees based on job responsibilities, as determined by the employee's appropriate Vice President, and to all students who are enrolled in a curriculum program. The use of College-provided electronic mail accounts must be related to College business, including academic pursuits. Incidental and occasional personal use of these accounts is acceptable when such use does not generate a direct cost to the College or otherwise violate the provisions within this policy.

The College will make reasonable efforts to maintain the integrity and effective operation of its electronic mail systems, but users are advised that those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature and technology of electronic communication, the College cannot assure the privacy of an individual's use of the College's electronic mail resources or the confidentiality of particular messages that may be created, transmitted, received or stored.

College officials do not routinely monitor electronic mail but may do so as the College deems necessary. The College does use software to monitor electronic mail for certain safety protocols. Students and employees should not have any expectation of privacy regarding their electronic mail addresses provided by the College. The electronic mail, sent and received, on a College-provided e-mail account is the exclusive property of the College. Any user of the College's computer resources who makes use of an encryption device shall provide access when requested to do so by the appropriate College authority. The College reserves the right to access and disclose the contents of employees', students' and other users' electronic mail without the consent of the user.
The College will do so when it believes it has a legitimate business or need including, but not limited to, the following:

A. In the course of an investigation triggered by indications of misconduct or misuse;

B. As needed to protect health and safety of students, employees or the community at large;

C. As needed to prevent interference with the College's academic mission;

D. As needed to locate substantive information required for College business that is not more readily available;

E. As needed to respond to legal actions; and

F. As needed to fulfill the College's obligations to third parties.

Electronic mail, including that of students, may constitute "educational records" as defined in the Family Educational Rights and Privacy Act (FERPA). Electronic mail that meets the definition of educational records is subject to the provisions of FERPA. The College may access, inspect and disclose such records under conditions set forth in FERPA.

North Carolina law provides that communications of College personnel that are sent by electronic mail may constitute "correspondence" and, therefore, may be considered public records subject to public inspection under the North Carolina Public Records Act.

Electronic files, including electronic mail, that are considered public records are to be retained, archived and/or disposed of in accordance with current guidelines established by the North Carolina Department of Cultural Resources or otherwise required by College policy 7.2.

VI. PRIVATE EMPLOYEE WEBSITES AND OTHER INTERNET USE

When creating or posting material to a webpage or other Internet sites, including social media, apart from the College's website or approved ancillary external site or page, employees should remember that the content may be viewed by anyone including community members, students and parents. When posting or creating an external website, students, faculty and staff are not permitted to use the College's name in an official capacity or use the College's marks, logos or other intellectual property.

Employees are to maintain an appropriate relationship with students at all times. Having a public personal website or online networking profile or allowing access to a private website or private online networking profile is considered a form of direct communication with students. Any employee found to have created and/or posted content on a website or profile that has a negative impact on the employee's ability to perform his/her job as it relates to working with students and the community or that otherwise disrupts the efficient and effective operation of the College may be subject to disciplinary action up to and including dismissal.

VII. VIOLATIONS

Each individual is ultimately responsible for his/her own actions. For employees, failure to exercise responsible, ethical behavior will result in disciplinary action up to and including dismissal. Students may be sanctioned according to procedures described in the Code of Student Conduct and other users may be barred permanently from using College computers and network access and suspended or expelled.

Certain activities violate Federal and/or State laws governing use of computer systems and may be classified as misdemeanors or felonies. Those convicted could face fines and/or imprisonment.

Adopted: April 9, 2018

ROBESON COMMUNITY COLLEGE	INFORMATION TECHNOLOGY ELECTRONIC RECORDS RETENTION	POLICY 7.3

I. INTRODUCTION

This Policy governs the College's retention of electronic records, including electronic mail (email) and instant messages. The Policy is intended to provide guidance on the need for retention of electronic records and messages sent and received by College employees. The College will retain and destroy electronic records, including email and instant messages, in accordance with this Policy and the approved Record Retention and Disposition Schedule (the Schedule) for community colleges adopted by the North Carolina Department of Cultural Resources and the North Carolina Department of Community Colleges. For the purposes of this Policy, the term "electronic records" is defined to include electronic mail and instant messages.

II. NORTH CAROLINA PUBLIC RECORDS ACT

Electronic records made or received in connection with the transaction of public business are public records pursuant to the North Carolina Public Records Act, as defined by the North Carolina Public Records Act, N.C.G.S. § 132-1 *et seq*. Examples of electronic records that are public records include, but are not limited to: messages that include information about policies or directives, official business correspondence, official reports, or material that has historic or legal value.

Public records, including electronic records, may not be deleted or otherwise disposed of except in accordance with the Schedule. The content of the electronic record determines its retention requirement.

The content of the email, not the method or device in which it was sent, dictates whether the email is a public record. For example, if an employee has work email on his private, personal email account, that email remains a public record. For this purpose, employees are strongly encouraged to use only their work email address for work emails. In the event that an employee, however, does have work emails on their personal email accounts, they are responsible to properly maintain the email and, if necessary for retention purposes, transfer the email to another medium for proper retention.

III. ELECTRONIC RECORDS CUSTODIAN

Because electronic messages can be sent and forwarded to multiple people, copies of the messages may exist in the accounts of multiple users. In most cases, the author, or originator, of the electronic message is the legal custodian and is responsible for maintaining the "record" copy. However, cases in which the recipient has altered the

message (made changes, added attachments, etc.), or when the message is coming from outside the college; the recipient is the one responsible for retaining the message.

When the custodian of an electronic message leaves the employment of the College, it is the responsibility of the supervisor to ensure all public records remaining on the computer and in the messaging account are retained or disposed of appropriately.

The College additionally stores all email and instant messages as a fail-safe archive in the event of system failure or unlawful tampering. All messages which are sent or received using the College's email and instant messaging system are copied and retained by this system for (5) five years. This storage mechanism is intended as a safety measure and does not replace the individual employee's legal responsibility for retaining and archiving electronic messages in accordance with the state of North Carolina's record retention laws.

IV. TYPES OF ELECTRONIC MESSAGES

For retention purposes, email messages generally fall into the following two categories:

A. Email of limited or transitory value. For example, a message seeking dates for a meeting has little or no value after the meeting. Retaining such messages serves no purpose and takes up space. Messages of limited or transitory value may be deleted when they no longer serve an administrative purpose.

B. Email containing information having lasting value. Email is sometimes used to transmit records having lasting value. For example, email about interpretations of an agency's policies or regulations may be the only record of that subject matter. Such records should be transferred to another medium and appropriately filed, thus permitting email records to be purged.

V. PROCEDURES FOR COMPLIANCE

While the methods for reviewing, storing or deleting electronic records may vary, compliance with the retention requirements may be accomplished by one of the following:

A. Retention of Hard Copy. Print the record and store the hard copy in the relevant subject matter file as would be done with any other hard-copy communication.

B. Electronic Storage of records and email. Electronically store the record or email in a file, on a disk or a server so that it may be maintained and stored according to its content definition under this Policy.

VI. LITIGATION HOLD

A litigation hold is a directive not to destroy electronic records, including email, which might be relevant to a pending or imminent legal proceeding. The President of the College may establish a committee to oversee and monitor litigation holds; such committee may contain a member of the Technology Department, the College's legal counsel and a member of the Administrative Team. In the case of a litigation hold, the committee shall direct employees and the Technology Department, as necessary, to suspend the normal retention procedure for all related records.

Adopted: April 9, 2018
Legal Reference: N.C.G.S. §§ 121-5; 132-1 *et seq*; Records Retention & Disposition Schedule (July 1, 2016)

ROBESON COMMUNITY COLLEGE	INFORMATION TECHNOLOGY ELECTRONIC SIGNATURES	POLICY 7.4

It is the College's intent to provide efficient services for its employees, students and for the public. The Board of Trustees (Board) encourages College officials and students to use electronic means, especially electronic mail, when conducting College business when those means result in efficient and improved service.

The Board encourages the acceptance of electronic signatures in e-mails from college campus accounts. An electronic signature is defined as any electronic process signifying an approval to terms, and/or ensuring the integrity of the document, presented in electronic format.

Students may use electronic signatures to register, check financial aid awards, pay student bills, obtain unofficial transcripts, update contact information, log into campus computers, complete forms, submission of class work, tests, etc. Employees may use electronic signatures for submitting grades, viewing personal payroll data, logging into campus computers, accessing protected data through the administrative computing system and custom web applications provided by the College, etc.

College user accounts are to be used solely by the student or employee assigned to the account. Users may not allow access to their accounts by other persons, including relatives or friends. All users are responsible for protecting the confidentiality of their account and for adhering to Policy 7.2 – Internet and Network Acceptable Use.

College employees are authorized to use an electronic signature to sign contracts, purchase orders, grant applications and other electronic documents to the same extent the employee is authorized to sign a hard copy of the document.

Adopted: April 9, 2018

ROBESON COMMUNITY COLLEGE	INFORMATION TECHNOLOGY SOCIAL MEDIA	POLICY 7.5

The College recognizes that social media sites are useful technologies in communicating with College constituencies and in enabling transparent communication. All of the College's social media shall follow established procedures and shall be registered with the College's Public Relations Department. College employees shall exercise good, professional judgment when using official College social media sites to ensure that communications are appropriate, professional, maintain the security of the College's network and comply with local, state and federal laws and with the College's technology security procedures. All content generated on a College-operated social media site should support the mission of the College.

College employees whose responsibility it is to operate a social media account on behalf of the College shall be responsible for monitoring discussions and content added by third-parties, including comments. The College's Public Relations Department has the right to remove any post or comment on any social media account operated by the College.

Social media accounts controlled by the College are subject to records retention regulations.

Adopted: April 9, 2018

ROBESON COMMUNITY COLLEGE	INFORMATION TECHNOLOGY PEER-TO-PEER FILE SHARING	POLICY 7.6

I. PURPOSE

The Digital Millennium Copyright Act of 1998 (DMCA) legally protects a copyright holder from the unauthorized use of his or her digital content. Unauthorized use means violating the user agreement or terms of use for the digital content. Illegally sharing and/or reproducing copyrighted materials such as music, videos, documents, software and photos is considered copyright infringement. The Higher Education Opportunity Act (HEOA) includes a provision directly related to DMCA.

HEOA holds higher education institutions accountable for student illegal peer-to-peer (P2P) file sharing occurring on College networks. Illegal P2P file sharing is downloading, also known as copying and/or saving, copyrighted material to a hard drive or any other storage device and/or sharing or making it available to other people without the consent of the copyright holder.

P2P applications are used to legitimately share digital content. However, P2P applications can expose the College to legal liabilities when illegal file sharing occurs. P2P applications can also present a security risk because a downloaded file may actually contain a virus or a malicious program that could target and infect other machines on the network, impact the performance of the network and compromise sensitive/confidential information.

The purpose of this policy is to inform the College community on preventive measures that will help avoid legal liability and security risks resulting from illegal file sharing. This policy applies to any individual using the College's computer network.

II. POLICY

Individuals using the College's computer network will be held accountable for adhering to the following terms and conditions:

A. Read the user agreement or terms of use for the following digital content in order to make sure you do not use nor share digital material illegally: documents, videos, and games located on the Internet; social networking sites (i.e. YouTube); purchased digital content (i.e., music, software); and peer-to-peer file sharing applications;

B. Delete unauthorized copyrighted material from your electronic device (i.e. computer, iPod);

C. Use a legal alternative to unauthorized downloading. The College does not endorse a particular product or service nor is it responsible for any cost or any technology related issues resulting from the use of the legitimate sources;

D. Disable the file sharing feature for P2P software if you do not have permission to share the digital material (i.e., documents, movies, games, etc.) legally; contact the software vendor for technical support;

E. Follow the P2P vendor's best practices for securing the computer used for P2P activity (i.e., anti-virus software, a vendor supported operating system, personal firewall, current version of P2P application, etc.); the Federal Trade Commission also has P2P best practices; and

F. For College-owned assets, P2P software can only be used to promote the College's mission, academic and business needs. Where applicable, P2P software is not allowed on machines that process and/or store confidential/sensitive data. The personal use of P2P applications on College-owned assets for recreational and leisure purposes is prohibited.

III. ENFORCEMENT

Enforcement of this Policy shall include:

A. Disclosure to students and employees on an annual basis;

B. Monitoring network traffic and limiting network bandwidth; and

C. Implementing other technology-based deterrents as needed.

In addition to employment and student discipline issued by the College in accordance with applicable policies and procedures (up to and including dismissal/suspension), individuals cited for unauthorized use may be subjected to civil and/or criminal damages such as monetary damages and potential prison time. According to the US Copyright Office, monetary damages can range from $200 to $150,000 for each act. Criminal prosecutions may result in a fine of up to $250,000 and a prison term of up to five (5) years for each act.

Adopted: April 9, 2018

ROBESON COMMUNITY COLLEGE	INFORMATION TECHNOLOGY DIGITAL TECHNOLOGY ACCESSIBILITY	POLICY 7.7

The College is committed to taking reasonable measures to support the accessibility of its audio, visual, telecommunications and web-based technologies (Digital Technology) for use by students, employees and/or the general public. Students who seek an accommodation for Digital Technology should contact Student Services. Other individuals who seek accommodations should contact the College's Information Technology Services office.

Undue burden and non-availability may qualify as an exemption from this policy when compliance is not technically possible or is unreasonably burdensome in that it would require extraordinary measures due to the nature of the request or would fundamentally alter the purpose of the Digital Technology.

When conducting core academic and business activities using web content, the College shall make a good faith effort to align the web content with the guidelines of the most current version of Web Content Accessibility Guidelines 2.0 Level AA (WCAG 2.0 AA).

Adopted: April 9, 2018

Legal Reference: Americans with Disabilities Act of 1990, as amended.