Policy 7.2 Information Technology: Internet and Network Acceptable Use

TRI-COUNTY 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.

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 restricted to protect systems.

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: 1) illegal peer-to-peer file trafficking by downloading or uploading pirated or illegal material including, but not limited to, software and music files; and 2) 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.

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.

The College does not monitor electronic mail routinely but may do so as the College deems necessary. Students and employees should not have any expectation of privacy regarding their electronic mail addresses provided by 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 site 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 to 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: 3/20/18 Technology Committee; 5/24/18 BOT