

I. PURPOSE

The purpose of this document is to define the policies and procedures for using the administrative systems, computer resources, and network systems at Caldwell Community College and Technical Institute (CCC&TI).

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.
6. Using another person's username/password or sharing of one's own username/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, 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. The College 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 Student Code 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.

Freedom of expression is a constitutional right afforded to individuals. However, users of college equipment, systems and software are held accountable for their actions and will respect the rights of individuals who may be offended by the services and images retrieved on the Internet. Individuals who feel they have been harassed should report the incident to the Vice President of Technology and Instructional Support Services or the Vice President of Student Services.

Violators of the computer usage policies and procedures previously stated will be subject to one or more of the following sanctions: verbal and/or written warning, temporary or

permanent suspension of computer access privileges, or dismissal from the college as stated in the CCC&TI Student Code of Conduct.

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. 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. 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 all students. The use of College provided electronic mail accounts should be related to academic pursuits.

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 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 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 7.3.

V. ELECTRONIC SIGNATURES

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.

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 all college policies.

VII. PRIVATE 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, students 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, without prior approval of the Vice President of Technology and Instructional Support Services.

Most online social networking sites and resources require an e-mail address and personal profile information. Personal accounts should not be used to officially represent or promote the College, a college organization, department, division, athletic team, group, official business, campus activity or event. When representing the College, or entity of the College, an approved campus representative account must be used. Individuals or groups are not permitted to freely create campus representative accounts on social networking, blog, wiki, or other social media sites. Only college employees specifically authorized by the Marketing and Communications Department may create online accounts and/or post official college (departmental, divisional, athletic, organizational) information, media files, documents, resources, calendars, and events.

VIII. VIOLATIONS

Each individual is ultimately responsible for his/her own actions. Students may be sanctioned according to procedures described in the Student Code of Conduct and 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.