
TOPIC:
Computer Usage - Procedures

Policy Number:
C21

Purpose

Cloud County Community College owns and operates a variety of computing systems which are provided for the use of CCCC students, faculty and staff in support of the programs of the College and are to be used for education, research, academic development and public service only. Commercial uses are specifically excluded. All students, faculty and staff are responsible for seeing that these computing systems and equipment are used in an effective, efficient, ethical, and lawful manner.

Unacceptable use of the system is prohibited and is grounds for loss of privileges, as well as discipline up to and including termination.

User Agreement

All users of CCCC computing systems must read, understand, and comply with the procedures outlined in this document. By using any of these systems, users agree that they will comply with these procedures.

Rights

These computer systems, equipment, and accounts are owned and operated by CCCC. CCCC reserves all rights, including the right to terminate without notice, to the computing resources which it owns and operates. These procedures shall not be construed as a waiver of any rights of CCCC, nor shall they conflict with applicable acts of law. Users have rights that may be protected by Federal, State, and local laws.

Privileges

Access and privileges on CCCC computing systems are assigned and managed by the network administrators of the systems. Eligible individuals may become authorized users of a system and be granted appropriate access and privileges by following the approval steps prescribed by CCCC.

Users may not, under any circumstances, transfer or confer these privileges to other individuals. Any account assigned to an individual shall not be used by others. The authorized user is responsible for the proper use of the system, including password protection.

TOPIC:
Computer Usage - Procedures

Policy Number:
C21

Responsibilities

Users are responsible for maintaining the following:

- *An environment conducive to learning:* The user who uses the computing systems at CCCC to harass, discriminate, make defamatory remarks, or otherwise violate Cloud County Community College policies and procedures, shall bear full responsibility for his or her actions. Further, by using these systems, users agree that individuals who transmit such remarks are solely responsible for their actions. Users agree that CCCC's role in managing these systems is only as an information carrier. Any violation of this procedure shall not be considered an endorsement by CCCC.

Many of the CCCC computing systems provide access to outside networks, both public and private, which furnish electronic mail, information services, bulletin boards, conferences, etc. Users are advised that they may encounter material which may be considered offensive or objectionable in nature or content. Users are further advised that CCCC does not assume responsibility for the contents of any of these outside networks.

The user agrees to comply with the acceptable use guidelines for whichever outside networks or services they may access through CCCC systems.

Further, the user agrees to follow proper etiquette on outside networks. The user agrees never to attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading (except for those outside services which may conceal identities as part of the service).

The user agrees that, if they violate CCCC's policies, procedures, or state and federal laws and transmit, or cause to be transmitted, a message that is inconsistent with an environment conducive to learning or with a misleading origination, the person who performed the transmission will be solely accountable for the message, not CCCC.

- *An environment free of illegal or malicious acts:* The user agrees never to use a system to perform an illegal or malicious act. Any attempt to increase the level of access to which he/she is authorized, or any attempt to deprive other authorized users of resources or access to any CCCC computer system shall be regarded as malicious and may be treated as an illegal act.
- *A secure environment:* Any user who finds a possible security lapse on any system is obliged to report it to the system administrators.

Knowledge of passwords or of loopholes in computer security systems shall not be used to damage computing resources, obtain extra resources, take resources

Adopted: 5/29/12	Revised 7/21/20	Revised/Reviewed	Revised/Reviewed	Revised/Reviewed
---------------------	--------------------	------------------	------------------	------------------

TOPIC:	Policy Number:
Computer Usage - Procedures	C21

from another user, gain unauthorized access to resources or otherwise make use of computing resources for which proper authorization has not been given.

Accounts

The individual is responsible for the proper use of their account.

Confidentiality

Programs and files are confidential unless they have been made available, with written permission, to other authorized individuals. CCCC reserves the right to access all information on CCCC computers. Employees have no expectation of privacy as to information and materials on CCCC's information system and the college may review and has access to all information placed on college information systems and equipment. File owners will be notified of file maintenance, in advance, if such notice is practical. If procedure violations are discovered, they will be reported immediately to the appropriate systems administrator and any violations are subject to discipline up to and including termination.

Electronic communications facilities (such as e-mail) are for college related activities only. Discriminatory, Fraudulent, harassing, or obscene messages and/or materials are not to be sent or stored. Violation of these procedures will result in discipline up to and including termination.

System Performance

No one should deliberately attempt to degrade the performance of a computer system or to deprive authorized personnel of resources or access to any college computer system.

Unauthorized Access

Loopholes in computer security systems or knowledge of special passwords should not be used to damage the computer system, obtain extra resources, take resources from another user, gain access to systems, or use systems for which proper authorization has not been given.

Copyright

Computer software protected by copyright is not to be copied from, into or by using campus computing systems and equipment, except as permitted by law or by the contract with the owner of the copyright. This means that such computer and microcomputer software may only be copied to make back-up copies, if permitted by the copyright owner. The number of copies and distribution of copies may not be done in

Adopted:	Revised	Revised/Reviewed	Revised/Reviewed	Revised/Reviewed
5/29/12	7/21/20			

TOPIC:	Policy Number:
Computer Usage - Procedures	C21

such a way that the number of simultaneous users exceeds the number of original copies purchased.

Violations

An individual's computer use privileges may be suspended immediately upon the discovery of a possible violation of the procedures. Such suspected violations will be confidentially reported to the appropriate system administrator.

Violations of these procedures will result in discipline up to and including termination. In such a review, the full range of disciplinary sanctions is available including the loss of computer use privileges, dismissal from the College and legal action. Violations may also constitute a criminal offense which will be reported to law enforcement.

Additional Guidelines

System administrators will establish more detailed guidelines, as needed, for specific computer systems and networks. These guidelines will cover such issues as allowable connect time and disk space, handling of unretrievable mail, responsibility for account approval and other items related to administering the system.

Systems Usage

Two accounts on this system have the ability to read your mail: your own account and the system administrator account. Employees have no expectation of privacy in their email or other accounts. There is no guarantee that your accounts or your electronic mail is private. The systems are not secure, nor are they connected to a secure network.