



UNC Computer, Internet & Electronic Communication Procedures

General

What does this procedure govern?

This procedure explains the acceptable use of University of Northern Colorado's computing and communication resources, including computers, networks, electronic mail, electronic information sources, voice mail, telephone services and other communication resources. Acceptable use is based on common sense, common decency and civility applied to the electronic communications environment.

How can resources be used?

Who can use the computing and communication resources?

What are the penalties for abuse or violation?

What if I suspect my resources have been compromised?

What other applicable administrative policies and procedures and student code of conduct are applicable to University system users?

Required Procedures & Prohibited Usage

Required Procedures

By acquiring an account or utilizing University electronic resources you assume the responsibility to:

1. Comply with these procedures, state, federal laws and UNC regulations and policies
2. Respect the rights and privacy of others, including intellectual property and personal property rights
3. Refrain from activities that may damage or obstruct the network and electronic resources and information
4. Avoid restricted areas and not compromise the integrity of electronic resources
5. Secure your passwords and make them difficult to obtain or guess
6. Be honest and accurate in personal and computer identification
7. Agree to cooperate and comply with UNC's requests for access to and copies of email messages or data when access or disclosure is authorized by this procedure or required or allowed by law or other applicable procedures, regulations and policies.

Prohibited Usage

Unacceptable uses that are prohibited include, but are not limited to the following:

1. Use of computer resources or electronic information for any purpose that may violate federal or state laws
2. Any person who knowingly uses any computer, computer system, computer network or any part thereof for the purpose of devising or executing any scheme or artifice to defraud; obtain money, property, or service by means of false or fraudulent pretenses, representations, or promises; using the property or services of another without authorization; or committing theft
3. Any person who knowingly and without authorization uses, alters, damages or destroys any computer, computer system, computer network or any computer software, program documentation, or data contained in such computer, computer system, or computer network
4. Use of resources for personal or private business or commercial activities, fund raising or advertising on behalf of non-UNC organizations
5. Misrepresentation or forging your identity or the source of any electronic communication
6. Unlawful communications, including threats of violence, obscenity, child pornography and harassing communications
7. Unauthorized acquisition, attempts to acquire, and use of passwords of others. Unauthorized use and attempts to use the computer accounts of others.
8. Assuming someone else's identity or altering the content of a message originating from another person or computer with intent to deceive

9. Interference with or disruption of the computer, telephone or network accounts, services or equipment of others is prohibited. The intentional propagation of computer "worms", "viruses", activities that place undue stress on resources such as ending chain letters, "spam" or widespread dissemination of unsolicited email and letter bombs or the resending of the same email repeatedly to one or more recipients
10. Reselling of UNC resources
11. Unauthorized use of University logos and other protected trademarks and logos
12. Any alteration of source or destination addresses including uniform resource locators (URLs) or other actions that mask the University identity
13. Unauthorized anonymous and pseudonymous communications
14. Unauthorized modification of or deletion of another person's files, account or posting; altering or attempting to alter files or systems without authorization
15. Use of computer resources or electronic information without authorization or beyond one's level of authorization
16. Interception or attempted interception of communications by parties not authorized or intended to receive them
17. Making resources available to individuals not affiliated with UNC without prior administrative approval
18. Revealing passwords or otherwise permitting the use by other (by intent or negligence) of personal accounts for computer and network access without authorization
19. Intentionally or recklessly compromising the privacy or security of University electronic information
20. Infringing upon the copyright, trademark, patent or other intellectual property rights of others in computer programs or electronic information (including plagiarism and unauthorized use of reproduction) is prohibited. The unauthorized storing, copying or use of audio files, images, graphics, computer software, data sets, bibliographic records and other protected property is prohibited except as permitted by law
21. Failure to comply with requests from appropriate UNC officials to discontinue activities that threaten the operation or integrity of computers, systems or networks, or otherwise violate this procedure
22. Unauthorized scanning of networks or computers for security vulnerabilities.
23. Altering or attempting to alter any computing or network components (such as routers, switches, and hubs) without approval or beyond one's level of authorization
24. Negligent or intentional conduct leading to disruption and or damage of electronic networks or information systems

Privacy & Security

Web Procedures

Purpose

The University of Northern Colorado recognizes the importance of the World Wide Web ("Web") in meeting the needs of many audiences, including prospective students. The Web is a valuable tool for areas of instruction, research and information sharing and is a critical component of the university's image. The university encourages faculty, staff and students to publish information in support of the mission of the university, recognizing that all users at the university are accountable to the taxpayers of the State of Colorado and the Web resources must be used in an ethical, courteous, legal and efficient manner.

University Web Pages

Responsibilities

1. Users must comply with all federal and state laws, contracts, software licenses and university policies, regulations and procedures, including but not limited to those related to personal conduct. The regulations of the Family Educational Rights and Privacy Act apply to all student information published on the web.
2. All users must comply with UNC Web Publication Guidelines.
3. Individual departments are responsible for quality of their own Web pages. Each office or group should designate a faculty or staff person responsible for accuracy, quality and currency of its Web pages.
4. The Office of Web Communications is responsible for design, content creation and maintenance of all university top level pages, such as the home and user pages,, as well as the development of Web procedures and publication guidelines. Web Communications is also responsible for coordination of university Web efforts and serves as a resource to the campus for information and assistance.
5. The university does not monitor official Web pages but will respond to issues or concerns of which it is made aware as they arise. Web Communications may review and request changes to any official university page(s) as appropriate.

Use of Resources

Advertising

Enforcement

Page Last Updated: [Oct 15, 2019](#) | Contact for this Page: [Sonya DeWitt \(mailto:sonya.dewitt@unco.edu\)](mailto:sonya.dewitt@unco.edu)
[Privacy Policy \(/general-counsel/privacy.aspx\)](#) | [Affirmative Action/Equal Employment Opportunity/Title IX Policy & Coordinator \(/sexual-misconduct/index.aspx\)](#)