Information Systems Code of Conduct

FT_IT_UT_40

Responsible Officer
Rick Snider
Responsible Office
IT
Approving Body
Board of Trustees
Approval Date
2019-11
Last Revision
2019-10
Re-evaluation Date
2021
Departmental Impact
All departments

Policy Statement

Individuals using CU’s technology must adhere to specific guidelines (listed below) for the safety of the institution.

Policy Procedures

- Your account and network connection are for your individual use. A computer account is to be used only by the person to whom it has been issued. You are responsible for all actions originating through your account or network connection. You must not impersonate others, misrepresent yourself, or conceal your identity in electronic messages and actions.
- Unless information is specifically made public or accessible to you, you should assume anything on the network is private. Just because you may have the ability, through a loophole, someone's carelessness, etc. to access files, directories, or information that does not belong to you, you do not have the right to do so. Any attempt to circumvent computer, network or file security, or to take advantage of security lapses is prohibited.
- Disruptive and/or invasive actions using computer systems and networks are strictly prohibited. Examples of this include, but are not limited to: viruses, threatening or harassing messages, "spamming," packet sniffing, self-perpetuating programs, excessive volume of file transfers, network traffic or printing and other programs, files, hardware, software or actions that deliberately or unintentionally degrade or disrupt system or network performance, compromise or circumvent system or network security, or interfere with the work of others. Due to its adverse impact on our systems and networks, the sending of chain letters and similar "pass-along" email messages is explicitly prohibited.
- The Technology Department will make reasonable efforts to have its computer systems and networks available at all times. However, as part of regular maintenance and other planned and unplanned activities, systems and networks may be unavailable at any particular time. CU reserves the right to restrict or terminate access to its computer and network resources as necessary. CU computer systems, facilities, and network resources are for noncommercial individual use related to the educational mission of the college by its faculty, staff, and students, and for approved CU business activities. CU reserves the right to limit or terminate access to computing, networking and other technology facilities as necessary.
- The Technology Department will take reasonable efforts to ensure that your user files and email messages remain private, and does not routinely monitor the contents of user files or messages. However, given the nature of computers and electronic communications, we cannot guarantee the absolute privacy of your files and information. You must take reasonable precautions and understand that there is a risk that in some circumstances others can, either intentionally or unintentionally, gain access to files and messages. Where it appears that the integrity, security, or functionality of the college's computer or network resources are at risk or in instances of abuse of CU policies, codes, or local, state or federal laws, or when someone's well being is in jeopardy, CU reserves the right to take whatever actions it deems necessary (including, but not limited to, monitoring activity and viewing files) to investigate and resolve the situation. CU will treat personal files and communications as confidential, and will only examine or disclose their contents when authorized by the owner or when directed by a member of the Cabinet or by the CIO. Such actions will be taken when there is evidence or reasonable information that inappropriate use of resources is taking place.