7310 Information Technology Responsible Use

As a part of its physical, social, and educational infrastructure, the College acquires, develops, and maintains computers, computer systems, and networks. These computing resources are intended for College-related purposes, including direct and indirect support of the College's instruction, research, and service missions; of College administrative functions; of student and campus life activities; and of the free exchange of ideas among members of the College community and between the College community and the wider local, national, and world communities.

The rights of academic freedom and freedom of expression apply to the use of College computing resources. However, so do the responsibilities and limitations associated with those rights. The use of College computing resources, like the use of any other College-provided resource and like any other College-related activity, is subject to the normal requirements of legal and ethical behavior within the College community. Thus, legitimate use of a computer, computer system, or network does not extend to whatever is technically possible. Users must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

I. Applicability

This policy applies to all users of College computing resources, whether affiliated with the College or not, and to all uses of those resources, whether on campus or from remote locations. Additional policies may apply to specific computers, computer systems, or networks provided or operated by specific units of the College or to uses within specific units. Consult the operators or managers of the specific computer, computer system, or network in which you are interested or the management of the unit for further information.

II. Policy

All users of College computing resources must comply with all federal, Wyoming, and other applicable law; all generally applicable College rules and policies; and all applicable contracts and licenses. Examples include, but are not limited to, the laws of:

- Libel
- Privacy
- Copyright
- Trademark
- Downloading of music
- Child pornography
- The Electronic Communications Privacy Act and
- The Computer Fraud and Abuse Act, which prohibit "hacking", "cracking", and similar activities
- The College's Code of Student Conduct
- The College's Sexual and Other Forms of Harassment Policy
- All applicable software licenses.

Users who engage in electronic communications with persons in other states or countries or on other systems or networks shall be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

Users may only use College computing resources that they are authorized to use and use them only in the manner and to the extent authorized. Users of email or other electronic communications shall not use a false identity or misrepresent themselves to others. Emails may not be sent anonymously. Ability to access computing resources does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.

Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the College. Users who let someone else use their computers, network privileges, and/or password shall be held accountable for any policy violations committed by that other user. The employee shall be subject to the disciplinary actions section of this policy for any such violations.

Users of College computing resources must respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Again, ability to access other persons' accounts does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.

Users of College computing resources must respect the finite capacity of the College computing resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all uses of College computing resources, the College may require users of those resources to limit or refrain from specific uses in accordance with this principle. The reasonableness of any particular use shall be judged in the context of all of the relevant circumstances.

Users of College computing resources must refrain from using those resources for personal commercial purposes, for personal financial or other gain, or to an extent or in ways that interfere with the successful and timely completion of one's job. Personal use of College computing resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other College responsibilities, and is otherwise in compliance with this policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

Users of College computing resources must refrain from stating or implying that they speak on behalf of the College and from using College trademarks and logos without authorization to do so. Affiliation with the College does not, by itself, imply authorization to speak on behalf of the College. Authorization to use College trademarks and logos on College computing resources may be granted only by the Communications and Marketing Office.

III. Enforcement

When a faculty, staff member, or student of the College is found to be in violation of this policy, each individual case shall be handled in accordance with the appropriate policy which covers the terms of employment or enrollment of that person. Violations of this policy may result in disciplinary action up to and including termination or expulsion.

Appeals of any disciplinary action shall again be handled in accordance with the appropriate policy.

If the individual who violated this policy is not an employee or student of the College, all computer and network access privileges shall be terminated. If the person received access to College computers or the College network from an employee of the College, that employee or student may also be sanctioned for the violation.

IV. Security and Privacy

The College employs various measures to protect the security of its computing resources and of their users' accounts. Users shall be aware, however, that the College cannot guarantee such security. Users shall therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly.

Users shall also be aware that their uses of College computing resources are not completely private. The College has access to any information on a College computer or on the College network. Appropriate copyright laws and related College policies shall be honored. Users shall utilize College computing services with this awareness.

While the College does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the College's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendition of service. The College may also specifically monitor the activity and accounts of individual users of College computing resources, including individual login sessions and communications, without notice, when:

A. The user has voluntarily made them accessible to the public, as by posting to Usenet or a web page;
B. It reasonably appears necessary to do so to protect the integrity, security, or functionality of College or other computing resources or to protect the College from liability;
C. There is reasonable cause to believe that the user has violated, or is violating, this policy;
D. An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or
E. It is otherwise required or permitted by law. Any such individual monitoring, other than that specified in "(a)", required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the Chief Information Officer or the Chief Information Officer's designees.

The College, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate College personnel or law enforcement agencies and may use those results in appropriate College disciplinary proceedings.

Adopted 2004
Revised & Adopted 03/11/2013
Revised & Adopted 05/11/2020