

## Student Use of University Computer Systems and Networks

The Student Use of University Computer Systems and Networks is a guideline created by the CSU System and used by all 4 of the campuses within the system. It is implied that all users inherently accept this policy. By accepting this policy, users agree to follow all listed guidelines. Any violation of these guidelines may be subject to disconnection from the network, disciplinary action, and/or legal action by the University and/or local, state, or federal agencies.

University computer systems and networks are provided for student use as a part of the University academic program. Students are encouraged to become proficient in the use of computers as a means of enhancing their educational experience. However, widespread student use also necessitates certain rules of computer conduct. Computer misconduct can result in restrictions on or revocation of computer access privileges.

University computer systems and networks constitute an expensive and valuable resource. The capacity of this resource to fulfill all the legitimate academic and administrative needs of students, faculty, and staff is limited.

Student users have a responsibility to use University computer resources in an efficient, ethical, and lawful manner.

The University has a right and a duty to protect its valuable computer resources and to restrict student access to uses that are strictly related to the students' university related programs as well as reasonably limited in time. The University reserves the right to define what are unauthorized student uses.

The Chief Computer Administrator or designee(s) at each University in the CSU System and at the System Office may monitor student user accounts, files and/or log-in sessions for appropriate management purposes. Such purposes include but are not limited to performing archival and recovery procedures, evaluating system performance, and ensuring system integrity and security.

Upon identifying a violation of the policy which constitutes an immediate, clear danger to the University computer systems or networks the Chief Computer Administrator or designee(s) at each University and in the System Office may immediately limit or suspend a student's access to University computer resources with immediate notification of charges and actions to the appropriate Chief Student Affairs Administrator or designee(s). This emergency suspension of computer use will then follow the student judicial procedures for "Interim Suspension" as provided in the CSU Student Rights and Responsibilities and Judicial Procedures document.

Violations of University computer policy which do not constitute an immediate, clear danger to the University computer systems or networks will be referred to the regular student disciplinary process.

Student computer offenses, which are included as number 25 in the Appendix of Punishable Offenses in the CSU Student Rights and Responsibilities and Judicial Procedures document are as follows:

- Unauthorized use of University computers and/or peripheral systems and networks;
- Unauthorized access to University computer programs or files;
- Unauthorized alteration or duplication of University computer programs or files;
- Any deliberate action to disrupt the operation of University computer systems which serve other members of the University community, including all networks to which University computers are connected;
- Use of University computer systems and networks for committing crimes, violating civil laws, or violating University rules.

UNAUTHORIZED USES for students include but are not limited to the following:

- Computer games which are not assigned course work;
- Development or transmitting of chain letters;
- Entering or transmitting of commercial advertisements or solicitations;
- Entering or transmitting of political campaign material relating to elections to be held outside the University;
- Entering or transmitting of obscene material;
- Sexual harassment or other forms of harassment aimed at others or otherwise threatening others;
- Sharing ones own computer account with others or using another person's accounts;
- Violation of copyright laws or using or copying software in ways that violate the terms of the license;
- Entering or transmitting computer viruses or any form of intentionally destructive programs;
- Intentional disruption of network services;
- Connecting any device to the network without permission;
- Copying, modifying, replacing, or deleting any other user's account or any software used for system management;
- Harming University computer equipment;
- Uses which violate rules developed at each University which are necessitated by facilities limitations or other circumstances unique to each University.