

Executive Summary

Computing is an integral part of the academic, business, and personal experience of University life of college students as we know them today. The on-campus resident student will almost certainly use the campus computing infrastructure while in class and in their residential campus home. The commuting student will also use the facilities while attending class or conducting class related activities. While enjoying the many benefits of the advanced nature of the campus computing facilities and network infrastructure, there comes some basic expectations of use.

This document outlines the basic expectations of Clemson University on how the student will interact with the campus computing systems. Each student is expected to conduct his/her computing needs in a manner that in no way jeopardizes the availability of the campus system or any connected system whether owned by the University or some other entity. The computing resources at Clemson University are the property of Clemson University. Clemson University reserves the right to take all necessary measures either proactively or in reaction to an event or the possibility of an event to protect those computing resources.

Additionally Clemson University strictly prohibits the use of its computing facilities to engage in, participate in, or be party to any illegal activity. The University will monitor its systems in order to protect against such.

Any violation of this policy will result in corresponding disciplinary action by the University. Students suspected to be in violation of this policy will be reported to the appropriate investigative and/or disciplinary unit, including but not limited to, the Office of Community and Ethical Standards or the University Police Department.

All student users of the computing facilities of Clemson University are expected to be familiar with this policy and agree to adhere to it prior to using any computing related facilities. Acceptance will be required before registering any personal computer on the campus network.

Purpose

Clemson University is dedicated to providing a safe, reliable and robust information technology infrastructure for faculty, staff and students. In doing so, there are some general expectations of acceptable use of the computing systems located or connected to Clemson University to ensure that the computing systems maintain their highest level of efficiency and reliability. Many University functions rely heavily on the accessibility of computing systems and the University must take every reasonable action to protect them.

Policy

Use of University computing resources, including network facilities, account numbers, data storage media, printers, plotters, microcomputer systems, and software for

computing activities other than those authorized by the University is strictly prohibited. Unauthorized use of such resources is regarded as a criminal act in the nature of theft and violators are subject to suspension, expulsion, and civil and criminal prosecution.

The following are examples of misuse of computing resources:

1. Unauthorized duplication, distribution or alteration of any licensed software. This includes software licensed by the University and licensed software accessed using the computing networks.
2. Attempting to gain unauthorized access to any computing resource or data, or attempting to disrupt the normal operation of any computing resource or network -- at Clemson or anywhere on the Internet,
3. Attempting to use another student's or employee's computer account or data, without their permission.
4. Using the University electronic mail system to attack other computer systems, falsify the identity of the source of electronic mail messages. Sending harassing, obscene or other threatening electronic mail. Attempting to read, delete, copy or modify the electronic mail of others without their authorization. Sending, without official University authorization, "for-profit" messages, chain letters or other unsolicited "junk" mail.
5. Knowingly infecting any computing resource with a software virus.
6. Tampering with the University computer network or building wiring or installing any type of electronic equipment or software that could be used to capture or change information intended for someone else.
7. Participating in a "denial of service" attack on any other computer, whether on or off campus.
8. Using University computing or network resources for personal gain or illegal activities such as theft, fraud, copyright infringement, piracy (e.g., sound or video recording), unsolicited email solicitations, electronic mail distribution abuse, or distribution of child pornography or obscenities.
9. The installation of network electronic equipment that includes, but is not limited to: routers, remote access devices, modems, wireless access points, or any other devices that allow access to the Clemson Network is prohibited. Wireless access is provided via centrally managed services of CCIT.

Communications

President
Provost
Vice Presidents
Vice Provosts
Deans
Directors/Department Heads
All Faculty, Staff, and Students

General Guidelines

Clemson University computing resources are the property of Clemson University, to be used for University-related business. Students have no expectation of privacy when utilizing University computing resources, even if the use is for personal purposes. The University reserves the right to inspect, without notice, the contents of computer files regardless of medium, the contents of electronic mailboxes and computer conferencing systems, systems output such as printouts, and to monitor network communication when:

1. It is considered reasonably necessary to maintain or protect the integrity, security or functionality of University or other computer resources or to protect the University from liability;
2. There is reasonable cause to believe that the users have violated this policy or otherwise misused computing resources;
3. An account appears to be engaged in unusual or unusually excessive activity;
4. It is otherwise required or permitted by law.

Any suspected violations of this policy or any other misuse of computer resources by students normally should be referred to the Office of Community and Ethical Standards. That office will investigate the allegations and take appropriate disciplinary action. Violations of law related to misuse of computing resources may be referred to the appropriate law enforcement agency.

Notwithstanding the above, Clemson Computing and Information Technology may temporarily suspend, block or restrict access to an account, independent of University disciplinary procedures, when it appears reasonably necessary to do so in order to protect the integrity, security or functionality of University or other computer resources, to protect the University from liability, or where the emotional or physical well-being of any person is immediately threatened. When CCIT unilaterally takes such action, it will immediately notify the account holder of its actions and the reason for them in writing. The account holder may appeal the action taken by CCIT in writing to the Chief Information Officer.

Access will be restored to the account holder whenever the appropriate investigatory unit of the University determines that the protection of the integrity, security or functionality of University or other computing resources has been restored and the safety and well being of all individuals can reasonably be assured, unless access is to remain suspended as a result of formal disciplinary action imposed through the Office of Community and Ethical Standards or as a result of legal action.

Definitions

Student – any person(s) who are currently enrolled or will be enrolled to attend Clemson University for academic related work.

Computing Facilities/Resources – Included but not limited to any dedicated lab or accessible computer hardware/software that is furnished by the University for student

use. This also applies to any wirelessly connectable devices that may connect to the central network.

Infrastructure – Included but not limited to any means of network connectivity, central processing or storage connected either by wired or wireless connections. This includes connection points, wires, and any related computing hardware along or between connection paths.

Denial of Service – The use of a computer in such a manner to attempt to make the receiving computer or component rendered useless. Typically accomplished by but not limited to flooding the network component beyond its capability.

References and Related Documents

Password Security

<http://ccit.clemson.edu/about/policies/password.php>

Office of Community and Ethical Standards

<http://stuaff.clemson.edu/conduct/>