

College of Coastal Georgia Policies On Acceptable Use of Computers

I. Introduction

A. Purpose. Technology resources (hardware and software) provided by College of Coastal Georgia are made available to students, faculty, and staff primarily as tools for enhancing and facilitating teaching, learning, scholarly research, communications, and the operation and administration of the institution. Uses which are not directly related to these purposes shall be considered secondary activities and should such secondary activities in any way interfere with the primary activities, access to institutional technology resources may be terminated immediately. Access to and usage of such resources is a privilege and is not a right. It is therefore deemed appropriate and necessary that certain guidelines for the use of these technology resources be set forth and explained.

B. Scope. These policies are applicable to all campus units as well as all users who operate or use any of the computing systems and networks of the College.

Campus units that manage their own computers or networks may add, with the approval of the Director of Computer Services, individual guidelines which supplement but do not change the intent of these policies.

C. Acceptance of Policies. Users of the College's computing and networking facilities agree by using these facilities they will comply with and be subject to these policies and conditions of use. Changes in policies may occur at any time. Changes will be available on the college's web site.

D. Eligibility for Services. Current or retired College of Coastal Georgia employees and current students are permitted to use these facilities for purposes described in Section I.A. unless prohibited by Section I.F. The facilities available to an individual user are determined by the intended use and the resources available.

User IDs for all students are valid for the academic year in which they are enrolled.

Technology resources are not routinely provided for use by spouses, parents, children, or friends of validated users.

E. Penalties for Misuse of Services. If the College becomes aware of violations of these policies or detects illegal use or practices designed to operate to the detriment of the user community, it will take immediate corrective action. Such action may include suspension of services to the user(s) determined to be at fault, who may also be subject to disciplinary action, up to and including termination for College employees and expulsion for students.

F. College Software Licensing Agreements. The user community must adhere to the licensing agreements that the college has with its vendors.

II. Usage

A. No one shall assist in, encourage, or conceal from authorities any unauthorized use, or attempt at unauthorized use, of any of the College's computers or network facilities.

Comments: The following specific computer crimes are defined by state law (Ga. Code 16-9-90 et seq.):

- * Computer theft (including theft of computer services, intellectual property such as copyrighted material, and any other property);
- * Computer trespass (unauthorized use of computers to delete or alter data or interfere with others' usage);
- * Computer invasion of privacy (unauthorized access to financial or personal data or the like);

* Computer forgery (forgery as defined by other laws, but committed on a computer rather than on paper);

* Misleading transmittal of names or trademarks (falsely identifying yourself or falsely claiming to speak for a person or organization by using their name, trademark, logo, or seal - Ga. Code 16-9-93. 1).

B. No one shall knowingly endanger the security of any College computer or network facility, nor willfully interfere with others' authorized computer usage.

C. No one shall use the College's communication facilities to attempt unauthorized use, nor to interfere with others' legitimate use, of any computer or network facility anywhere.

Comments: State and federal laws forbid malicious disruption of computers. The College does not tolerate individuals who invade others' privacy, steal computer services, or commit misrepresentation or fraud; nor pranksters who attempt to disrupt computers or network facilities for any other purpose.

D. No one shall connect any computer to any College network unless approved by the college's Office of Computer Services.

E. No one shall give any password for any College computer or network facility to any unauthorized person, nor obtain any other person's password by any unauthorized means whatsoever.

Comments: Giving your password to an unauthorized person can be a crime under Georgia law. The criterion is not whether you trust them, but whether the College has authorized them.

You are responsible for choosing a secure password. Do not use names, nicknames, phone numbers, or recognizable words in any language. A good way to make up a secure password is to use the initials of a phrase that includes some numbers as well as letters, such as 57ityMwb - "57 is the year Michael was born."

F. No one shall misrepresent his or her identity or relationship to the College when obtaining or using College computer or network privileges.

Comments: You must not falsify your name, address, email address, or affiliation when sending email or other messages from a College computer. Doing so can be illegal (Ga. Code 16-9-93.1 and other laws against misrepresentation) as well as being an unacceptable use of the College's facilities. Deceptive communication, in which you claim to be some other specific person, is never permitted.

Use prudent caution when sending out any message that appears to be an official communication from the College. If the header identifies your message as coming from an administrative office or from the office of someone other than yourself (e.g., "President's Office"), recipients will presume that you are speaking for that office or person.

G. Without specific authorization, no one shall read, alter, delete or use any other person's computer files, electronic mail or workstation.

H. No one shall copy, install, or use any software or data files in violation of applicable copyrights or license agreements.

Comments: This rule forbids making unauthorized copies, for use elsewhere, of software residing on the College's computers. It also forbids installing or using pirated software on College computers.

I. No one shall create, install, or knowingly distribute a computer virus, "Trojan horse," or other surreptitiously destructive program on any College computer or network facility, regardless of whether any demonstrable harm results.

Comments: A virus is a hidden computer program that secretly copies itself onto users' disks, often damaging data. A Trojan horse is a program with a hidden, destructive function, or a program designed to trick users into revealing confidential information such as passwords.

J. Without proper authorization, no one shall modify or reconfigure the software or hardware of any College computer or network facility.

K. Confidential information shall not be placed in computers without protecting it appropriately. The College cannot guarantee the privacy of computer files, electronic mail, or other information stored or transmitted by computer unless special arrangements are made.

Comments: Ordinary electronic mail is not private. Do not use it to transmit computer passwords, credit card numbers, or information that would be damaging if made public. Bear in mind that students' educational records are required by law, and by University System of Georgia policy, to be kept confidential. It may also be necessary to protect confidential information about employees.

The College will normally respect one's privacy but cannot guarantee it absolutely. Because of the nature and technology of electronic communications, the College can assure neither the privacy of an individual user's use of the College's electronic mail resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored thereby.

The Georgia Open Records Act applies to information stored in computers. This act gives citizens the right to obtain copies of most public records, including any record prepared, received, or maintained by the College in the course of its operations. Some kinds of records are exempt from public disclosure, such as student records. Requests for information must be made through proper administrative channels.

System administrators shall respect the privacy of users as far as possible and shall refer all disciplinary matters to appropriate authorities. The Electronic Communications Privacy Act (18 USC 2701-2709) and other wiretap laws prohibit unauthorized interception of electronic communications, including electronic mail.

L. The College's computers, network facilities, and resources for electronic mail are to be used for College business, which may include academic pursuits and fundraising events for College benefit only. An electronic bulletin board can be used to post other community service activities. Incidental and occasional personal use of computer resources may occur when such use does not generate a direct cost for the College. Any such incidental and occasional use of resources is subject to the provisions of this policy. It is always improper to use the College's resources for political campaigns and commercial enterprises.

Comments: As a public institution covered by laws which govern private use of state property, the College can only provide computer services for its own work, not for private use. In this respect the College's computers are different from those owned by private colleges or corporations.

M. Users shall take full responsibility for messages they transmit through the College's computers and network facilities. No one shall use the College's computer resources to transmit fraudulent, defamatory, harassing, obscene, or threatening messages or any communications prohibited by law. In addition, it shall not be an acceptable use of the College's resources to download, view, copy or retrieve materials that may be deemed, by the reasonable person standard, to be pornographic in nature.

Comment: Laws against obscene or harassing telephone calls apply to computers that are accessed by telephone.

N. The use of electronic mail (e-mail) is included in all the foregoing policies regarding computer usage. In addition to the foregoing policies, the use of e-mail shall also be governed by the following:

Inclusion of the work of others into electronic mail communications in violation of copyright laws is not permitted.

Capture or "opening" of electronic mail, except as required in order for authorized employees to diagnose and correct delivery problems, is not permitted.

Use of electronic mail to interfere with the ability of others to conduct College business is not permitted.

Use of electronic mail systems for any purpose restricted or prohibited by laws or regulations is not permitted.

"Spamming," i.e., deliberately flooding a computer with excessive amounts of electronic mail is not permitted.

"Spoofing," i.e., constructing an electronic mail communication so it appears to be from someone else, is not permitted. All users should be aware that there is no guarantee that electronic mail actually came from the person or site indicated in it. Deceptive electronic mail is easy to fake, including the technical information in the header. Doing so is, of course, prohibited and is, in many cases, against the law. "Snooping," i.e., obtaining access to the files or electronic mail of others for the purpose of satisfying idle curiosity, with no substantial College business purpose, is not permitted.

Use of electronic mail for business solicitations, business slamming, chain letters, pyramid schemes, or religious proselytizing is not permitted.

Attempting unauthorized access to electronic mail or attempting to breach any security measures on any electronic mail system, or attempting to intercept any electronic mail transmissions without proper authorization, is not permitted.

Hoaxes, scams, pranks, and con games are common on the Internet. Be on the lookout for misguided "warnings" (about computer viruses, impending legislation, etc.) and false appeals for charity (usually involving dying children). If you get a message that spurs you to take immediate action, it is very likely a hoax, even if the person who passed it along to you was perfectly sincere. Also, genuine appeals that are several years old are still circulating as if they were current.

O. The University System of Georgia provides an extensive collection of Web-based databases under the GALILEO project (www.galileo.peachnet.edu). GALILEO is accessible by anyone at the libraries of public colleges and universities, local public libraries, K-12 schools, and technical institutions in the state of Georgia. Individuals who have the current password may access GALILEO from home. Passwords are available to students and faculty through their college library. GALILEO was established to provide electronic access to library materials, information resources and services, regardless of geographical location or size of institution.