



The University of Georgia

University of Georgia Policies on Use of Computers

Last revised on January 8, 2004

1 Purpose

This document has two purposes: to prohibit certain unacceptable uses of the University of Georgia's computers and network facilities, and to educate users about their responsibilities.

Most of these regulations simply restate obligations that follow from other existing policies or laws (see References and Links below). They fulfill a Board of Regents directive requiring the University to adopt explicit computer security and ethics policies along the lines of those recommended in Internet RFC 2196.

This document is divided into rules and commentary, with the expectation that the commentary can be revised frequently to reflect technical changes and to answer questions that have come up, without materially changing the rules.

2 Penalties

Violations of these policies incur the same types of disciplinary measures as violations of other University policies or state or federal laws, including criminal prosecution in serious cases.

3 Definitions

3.1 *University computers and network facilities* - comprise all computers owned or administered by any part of The University of Georgia or connected to the University's communication facilities, including departmental computers, and also the University's computer network facilities accessed by anyone from anywhere.

3.2 *Authorization* - is permission granted by the appropriate part of the University's governance and/or management structure, depending on the particular computers and/or network facilities involved and the way they are administered.

4 Rules

4.1 No one shall use any University computer or network facility without proper authorization. No one shall assist in, encourage, or conceal from authorities any unauthorized use, or attempt at unauthorized use, of any of the University's computers or network facilities.

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

- 4.3** No one shall use the University's communication facilities to attempt unauthorized use, nor to interfere with others' legitimate use, of any computer or network facility anywhere.
- 4.4** No one shall connect any computer to any of the University's networks unless it meets technical and security standards set by the University administration.
- 4.5** All users shall share computing resources in accordance with policies set for the computers involved, giving priority to more important work and cooperating fully with the other users of the same equipment.
- 4.6** No one without specific authorization shall use any University computer or network facility for non-University business.
- 4.7** No one shall give any password for any University computer or network facility to any unauthorized person, nor obtain any other person's password by any unauthorized means whatsoever. No one except the system administrator in charge of a computer is authorized to issue passwords for that computer.
- 4.8** No one shall misrepresent his or her identity or relationship to the University when obtaining or using University computer or network privileges.
- 4.9** No one without specific authorization shall read, alter, or delete any other person's computer files or electronic mail. This rule applies regardless of whether the operating system of the computer permits these acts.
- 4.10** No one shall copy, install, or use any software or data files in violation of applicable copyrights or license agreements, including but not limited to downloading and/or distribution of music, movies, or any other electronic media via the internet.
- 4.11** No one shall create, install, or knowingly distribute a computer virus, "Trojan horse," or other surreptitiously destructive program on any University computer or network facility, regardless of whether any demonstrable harm results.
- 4.12** No one without proper authorization shall modify or reconfigure the software or hardware of any University computer or network facility.
- 4.13** Users shall not place confidential information in computers without protecting it appropriately. The University cannot guarantee the privacy of computer files, electronic mail, or other information stored or transmitted by computer unless special arrangements are made.

- 4.14** Users shall take full responsibility for messages that they transmit through the University's computers and network facilities. No one shall use the University's computers to transmit fraudulent, defamatory, harassing, obscene, or threatening messages, or any communications prohibited by law.
- 4.15** Those who publish World Wide Web pages or similar information resources on University computers shall take full responsibility for what they publish; shall respect the acceptable-use conditions for the computer on which the material resides; shall obey all applicable laws; and shall not publish commercial advertisements without prior authorization. References and links to commercial sites are permitted, but advertisements, and especially paid advertisements, are not. Users shall not accept payments, discounts, free merchandise or services, or any other remuneration in return for placing anything on their web pages or similar facilities.
- 4.16** Users shall comply with the regulations and policies of newsgroups, mailing lists, and other public forums through which they disseminate messages.
- 4.17** System administrators shall perform their duties fairly, in cooperation with the user community, the appropriate higher-level administrators, University policies, and funding sources. System administrators shall respect the privacy of users as far as possible and shall refer all disciplinary matters to appropriate authorities.
- 4.18** Electronic mail (e-mail) is intended for communication between individuals and clearly identified groups of interested individuals, not for mass broadcasting. No one without prior authorization shall use the University's facilities to distribute the same or substantially the same e-mail message to more than one person without prior evidence that they wish to receive it, nor to distribute chain letters (messages asking the recipient to distribute copies further).

The University reserves the right to discard incoming mass mailings ("spam") without notifying the sender or intended recipient.

For its own protection, the University reserves the right to block all Internet communications from sites that are involved in extensive spamming or other disruptive practices, even though this may leave University Computer users unable to communicate with those sites.

5 References and Links

New state and federal laws concerning computer abuse continue to be passed, and important court decisions occur frequently. For up-to-date guidance about specific questions, consult the Computer Security and Ethics Incident Handling Team. Remember that legal advice circulated on the Internet is unreliable.

Computer crimes defined by Georgia law were mentioned in the comments on rule 1. In addition, there is a specific law against electronic distribution of obscene material to minors (Ga. Code 16-12-100.1).

Federal law (18 USC 1030) provides for fines and imprisonment up to 20 years for unauthorized or fraudulent use of computers that are used by or for the federal government (which includes many of the computers on the net), and for unauthorized disclosure of passwords and similar information when this affects interstate commerce. (Recall that net messages, as well as long-distance phone calls, are interstate commerce and thus fall under this law.)

The Electronic Communications Privacy Act (18 USC 2701-2709) and other wiretap laws prohibit unauthorized interception of electronic communications, including electronic mail.

Pyramid schemes and chain letters that ask for money or anything else of value are illegal under various state and federal laws and postal regulations. The people running these schemes generally claim to have found loopholes in the law, but their claims should not be believed. Even if a pyramid scheme were legal in itself, it would be illegal to use a University computer to participate in it for personal gain.

Computer users must also obey laws against private use of state property, divulging confidential educational records, copyright infringement, fraud, slander, libel, harassment, and obscenity. Laws against obscene or harassing telephone calls apply to computers that are accessed by telephone. The Georgia Open Records Act applies to records stored in computers as well as on paper.

The University must obey the policies of the University System (Board of Regents) and the regulations of the nationwide and worldwide networks to which its computers are connected.