Design and Implementation of a Campus Computer Ethics Policy

Michael A. Covington
Artificial Intelligence Center
The University of Georgia
Athens, Georgia 30602-7415

Published in *Internet Research* 5.4 (1995) 31–41.

Abstract

As the set of people using computers becomes larger and less cohesive, it is becoming important to educate users about their ethical responsibilities. Design of an effective campus computer ethics policy requires awareness of numerous cultural, technical, and legal issues. Especially important are the cultural splits between power users and utilitarian users, and between "old world" and "new world" philosophies of computer ethics. This paper discusses those issues and presents the University of Georgia's ethics policy as a model to aid those developing similar policies at other institutions.

Biographical information

Michael A. Covington is Associate Director of the Artificial Intelligence Center at the University of Georgia; was chairman of the task force that developed the University's campus computer ethics policy; and is chairman of the University's computer security and ethics incident handling team. He has a Ph.D. in linguistics from Yale University and has been working with computers for more than 20 years.

Michael A. Covington
Artificial Intelligence Center
The University of Georgia
Athens, GA 30602–7415
+1 706 542-0358
mc@uga.edu

1 Introduction

As the set of people using computers becomes larger and less cohesive, it is becoming more and more important to educate users about their ethical responsibilities. This is particularly the case now that the Internet has made mass communication available to nearly all computer users; conflicts between individuals arise more easily than ever before.

This paper describes how the University of Georgia approached the design of a comprehensive campus computer ethics policy. The policy statement itself is presented herewith as an appendix in the hope that other institutions can use it as a model.[1]

2 The policymaking process

The University of Georgia's computer ethics policy was developed by a task force that met through most of 1994 under my chairmanship. Since computer ethics is primarily a management issue, not a technical issue, the task force included not only computer administrators and users, but also people from Internal Auditing, Student Affairs, Legal Affairs, and even Campus Police. The task force began with a policy statement that had been developed around 1990 by a group of network managers and was already in use in some campus labs.[2]

During the development process, drafts of the policy were circulated to a wide spectrum of administrators and computer users, inviting criticism from all possible sources. This was an essential step because it enabled the task force to answer practically all objections before the finished policy was released.

[1] A much earlier version of this paper was presented at the 1995 University System of Georgia Annual Computing Conference and appears in the proceedings. I am grateful to numerous colleagues who gave me helpful advice about computer ethics over the past several years.

[2] The members of the 1994 task force were myself (from the Artificial Intelligence Center); Doug Mathews and Carolyn Gard (University Computing); David Quarterman (Network Managers' Council); Jim DeHaseth (Chemistry Department); Susan Jones (Legal Affairs); Chuck Horton (Campus Police); Larry Dendy (Public Information); Jack Bennett (Financial Services); and Frank Grindstaff (Internal Auditing). Unfortunately, the names of the earlier 1990 working group were not recorded.

The end product was a comprehensive policy statement (consisting of rules and commentary, and reproduced herewith as an appendix); a one-page summary of the policy statement; and a set of recommendations for implementation. These were sent up through the channels of the University administration and adopted as official policy.

3 Changing issues

The hot issue in computer ethics changes from year to year. In the early 1980s, it was game playing versus serious work; in the mid-1980s, account cracking; and since 1990, the misuse of computers as a means of mass communication. Within that broad category the hottest issue was at first general obnoxiousness and harassment; then indecency and obscenity; and most recently, improper commercialism (junk mail and the like).

Several recent changes have affected the computer ethics scene. On the negative side, the demise of NSFnet and the resulting lack of an enforceable Internet-wide acceptable-use policy has created substantial practical problems. Some people know they're misusing the net, and they don't mind as long as they can get away with it. Indeed, a few commercial sites apparently make their money by tolerating acts of intrusive advertising that wouldn't be tolerated anywhere else.

On the whole, however, the advent of commercial Internet service providers has made campus ethics policies easier to enforce. The reason is that students and faculty no longer assume that all their Internet access must be provided by the University. Purely recreational access can be obtained elsewhere. This is analogous to the way the advent of personal computers made a moot point of the game playing issue in the early 1980s.

Another welcome cultural development has been the shift from newsgroups and mailing lists toward World Wide Web pages for which particular individuals are accountable. Web page ownership makes users more aware that they have a public image which must be safeguarded. Anonymous sniping and flaming are impossible on the Web; instead, people take pride in delivering useful information to each other.

It is possible, however, that obnoxious Web pages will appear later. The general pattern with any new communication technology is that the first users of it are benevolent and constructive, since they value the technology and want society to accept and preserve it. Once the technology is firmly

established, antisocial uses begin to appear. This happened with television (parts of which are now justly criticized as a moral wasteland) and with newsgroups (which were originally very academic, or at least had a strong commitment to be useful); it will probably find a way to happen on the World Wide Web.

4 Cultural splits

Anyone proposing a computer ethics policy must be aware that users do not all approach computer ethics the same way. The two most important splits are between power users and utilitarian users, and between the "old world" and "new world" approaches to computer ethics.

Some people consider their computer expertise an important superpower; their main specialty may be something else, but the computer is an important part of their life. These are the "power users." Others view the computer only as a tool they use to get their work done; their technical skills may be first-rate, but they consider their main mission to be something other than computing. These I will call utilitarian users.

Power users and utilitarian users often come down on opposite sides of controversies; generally, utilitarians favor restrictions to allocate resources more fairly, while power users oppose restrictions. For instance, there was a minor dispute in a University computer lab a few months ago between power users, who wanted unlimited access to terminals, and utilitarians, who wanted to displace the net-surfing power users in order to get their homework done.

Computer administrators tend to hear only from power users and may get a biased perspective. The needs and desires of utilitarian users were carefully taken into account in developing the Georgia ethics policies.

The second major split divides not users but policymakers and policy advocates. The "new world" view of computer ethics emphasizes the novelty of cyberspace and assumes that pre-existing institutions and policies do not apply there. The "old world" view sees the computer and the network as extensions of previously existing institutions.

These conflicting views lead to radically different ways of constructing a computer ethics policy: either reinvent ethics from scratch, or apply the University's existing policies in a new environment. The Georgia task force chose to do the latter; what they produced is an unabashedly "old

world" approach to computer ethics.

After all, it is not clear that cyberspace is entirely new. Mark Twain wrote a short story in 1878 about the cyberspace of the long-distance telephone.[3] Another kind of cyberspace originated in ancient Greek times with the invention of paper money, enabling people to use gold without knowing where it is stored.

Much of the Internet community favors the "new world" view, which is implicit in some of the publications of the Electronic Frontier Foundation. This probably reflects the general preference of power users to reinvent things from scratch rather than learn existing systems. Utilitarian users tend to prefer, and even assume, the "old world" approach.

5 Countering misconceptions

Most cases of computer misuse arise not from malice, but from serious misunderstandings about what is accepted practice. Accordingly, much of the job of an ethics policy, and of those who enforce it, is to counter misconceptions. This situation may change in the future; already there have been a few instances of naïveté being offered as an excuse for what was actually deliberate maleficence. Even so, the ethics policy must address all common misconceptions, if only to eliminate excuses.

5.1 Misconceptions about limited punishment

The most common misconception is, "All they can do is take away my account" — that is, offenses committed on the computer can only be punished on the computer. This misconception stems from the tradition of letting system administrators act as judge, jury, and executioner rather than referring computer misuse cases to other disciplinary processes.

But taking away an account is no deterrent for someone who expects to lose the account soon anyway, or does not really need it, or is willing to hop from account to account to continue perpetrating mischief. It is important to get it across to users that computational acts can cause non-computational harm and incur non-computational penalties.

[3] "The Loves of Alonzo Fitz Clarence and Rosannah Ethelton," reprinted in numerous anthologies.

A more serious misconception, fortunately dying out but still found among the most naive users, is that anyone who cracks an account will be hailed as a technical genius, granted complete amnesty, and perhaps offered a high-paying job. More generally, there are plenty of people who ignore issues of right and wrong when presented with a technical challenge. The appropriate response is to point out that cracking accounts is no different from picking locks — you have to know some out-of-the-way things but you don't have to be a genius — and that the main thing it proves is not skill but untrustworthiness.

5.2 Misconceptions about a separate world

Another class of misconceptions involves the assumption that the computer network is a separate world, rather like a video game, where real-world responsibilities do not apply. People who are under this illusion often use funny made-up names for themselves; they tend to assume that no matter what they say or do, it cannot harm a real human being.

A slight variation on the theme is the assumption that the Internet is, or ought to be, a sanctuary for behaviors that are not tolerated in the rest of the world, ranging from rudeness to drug use, gambling, and pornography. Associated with this is the mistaken belief that laws do not apply to computers unless they explicitly say so.

Even management sometimes acquiesces in the notion that electronic forums are free-for-alls exempt from real-world standards of politeness. But free-for-alls are not really free; anarchy is the tyranny of the strongest or most obnoxious, and any electronic forum that tolerates bullying will be run by bullies. The Internet community is slowly learning this lesson, and standards of politeness are rising.

Still another variation is the assumption that one's postings in an electronic forum will be seen only by a small number of like-minded people. "Don't tell my boss about my cocaine habit" is typical of this kind of net posting, shared only with ten million of one's closest friends. Freshmen think everyone is a freshman, Americans think everyone is an American, and hobbyists think everyone is a hobbyist — a misconception that caused some friction recently when America Online linked up to Usenet.

5.3 Misconceptions about cost

A third class of misconceptions has to do with the cost of computing and who is paying it. Right now, the Internet is plagued with small entrepreneurs who think that they are paying the cost of distributing their net postings and that they should therefore be able to distribute them everywhere, like junk mail.

But the Internet is not a broadcast medium; the costs of transmitting messages are paid by recipients and by sites along the way, not just by the senders. This point deserves repeating often and loudly: *on the Internet, you are always someone's guest.* That's why junk e-mail and spamming are forbidden.

This fact about the Internet may foreshadow a change in the mass media as a whole. One of the peculiarities of the twentieth century is the way people are constantly bombarded with advertising, far from the point of sale. This peculiarity arose because the cost of TV, radio, and newspaper production is borne almost entirely by the sender and can therefore be subsidized by ads. The Internet does not work that way, and neither will cable TV when it matures into something beyond the mere redistribution of broadcasts; in both cases the recipients pay the bills, and advertisements will have to be delivered in the form of information that people will pay to retrieve. There are indications that the advertising industry has realized this and is running scared.

Another misconception is the assumption that computer and network usage cost nothing. Academia has a sacred tradition of concealing costs from end users and even from administrators. To some extent this is desirable, because institutions want to encourage exploration and self-training, and because academic research projects are, by definition, speculative ventures whose success cannot be measured in monetary terms. Besides, much of the Internet access that the University provides for educational purposes is, to the end user, pure recreation.

Difficulties arise when someone claims recreational computing as an inalienable right, or, more commonly, when someone wants to use the University's equipment for commercial purposes. It is important to communicate to users that many legitimate uses of the Internet are not legitimate uses of the University's equipment. There are things the Net permits that the University will not or cannot pay for.

6 Georgia's rule set

The University of Georgia's computer usage rules are presented as an appendix to this paper. Each rule is accompanied by explanatory comments which can be updated without amending the rules.

These rules do not impose substantial new restrictions on computer users. Rather, they inform users of responsibilities that they have had all along. For example, Rules 1 to 6 say, in essence, that users need permission to use the University's equipment, and that unauthorized use is prohibited by law. Rules 7 to 13 deal with privacy, confidentiality, copyrights, and tampering. Rules 14 and 15 hold users responsible for their electronic communications and for proper use of electronic forums. Finally, Rule 16 guarantees due process to anyone accused of computer-related misconduct.

The rules do not prescribe any specific penalties for violations. Rather, they stipulate that all cases shall be referred to the appropriate disciplinary authorities, just like offenses not involving computers. After all, the University has long had mechanisms in place to deal with various kinds of misconduct, and there is no reason to handle computer cases differently. A computer security incident handling team (described further below) stands ready to provide technical help to administrators handling such cases.

Contrary to what some users expected, the rules impose no requirement of "political correctness" and no limitation on free speech beyond the limitations already imposed by law and by University policy. If people want to say foolish things on the computer, the University lets them, provided of course they are not terrorizing an individual or misusing an electronic forum. It is not for the University to decide in advance what opinions can be propagated through its equipment.

7 Implementation and results

The first step in implementing Georgia's ethics policy was to publish it both on paper and online. Newspapers reported its adoption and a summary of it was incorporated into the Student Handbook and Employee Handbook. A local newsgroup was set up for discussing it, and a poster was placed in campus computer labs (Figure 1).

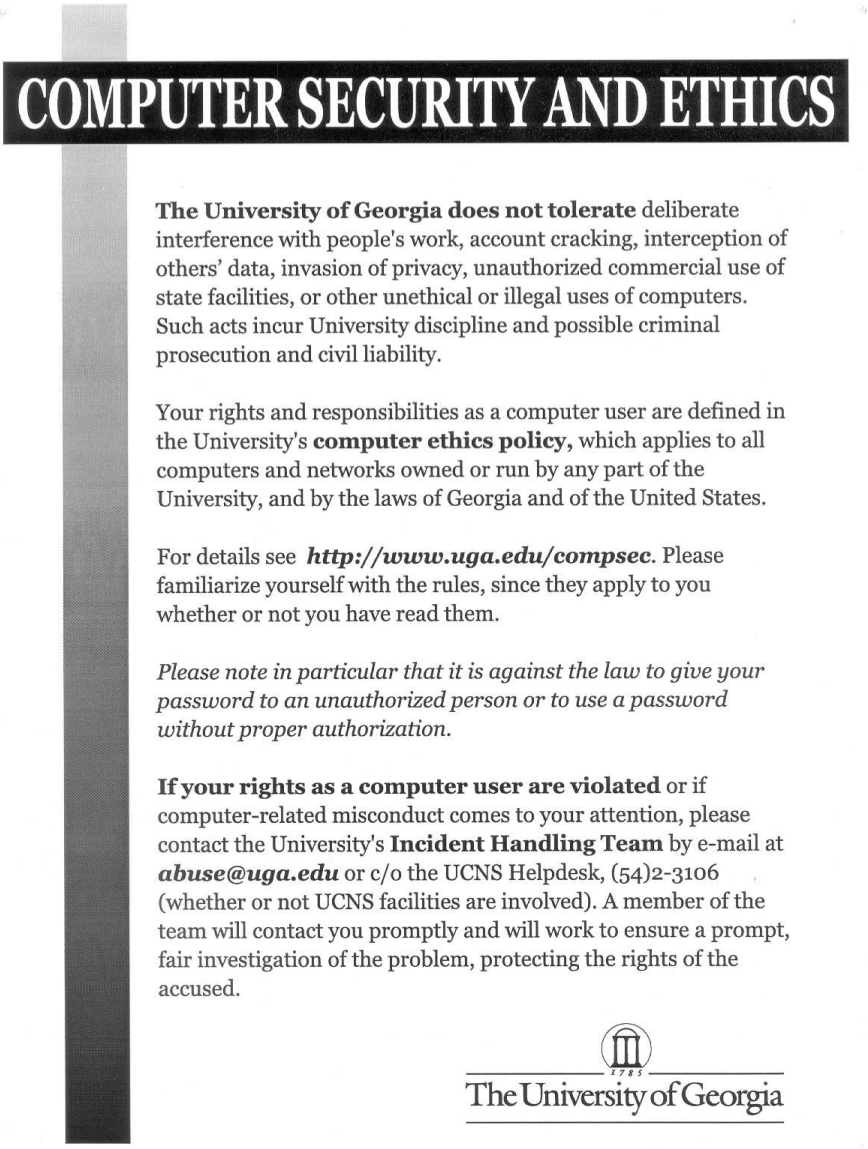

Figure 1: Poster placed in campus computer labs.

Besides adopting the rules, the University has set up a continuing task force to keep them updated and an incident handling team to deal with specific cases. The incident handling team is important for two reasons. First, it gives users somebody to complain to when things go wrong; and second, it protects accused individuals from unfair treatment by administrators who do not understand the situation.

The incident handling team is not a judicial body; rather, its purpose is to advise the other administrators and officials (ranging from employees' supervisors to police) which might be involved in handling an incident. Many incidents of prohibited behavior arise from misconceptions which can be countered simply by giving information and advice to the people involved. The members of the incident handling team are in the best position to give this advice. Further, University policy requires that the team be called in whenever disciplinary action is taken for computer-related misconduct, to ensure that the team is utilized when needed and that the team is aware of recurrent or ongoing problems.

The mere knowledge that there *is* a computer ethics policy has had a beneficial effect on the user community. It would be desirable for all users to actually *read* the rules, but that is probably unachievable. At the very least, users realize that they are accountable for what they do, and that if they need a ruling on a specific question, there is a written policy that will give an answer.

Far from objecting to the explicit rules, the community seems to have welcomed them. Indeed, the University of Georgia appears to have become an unusually well-behaved campus, and there have been no really serious incidents of computer misuse at the University since the rules were adopted. People seem to have a clearer understanding of their rights and responsibilities. The wild debates about freedom of speech that have characterized the local newsgroups two or three years ago have died down.

Indeed, the computer ethics policy provides an opportunity for members of the University community to learn something about the nature of ethics itself. The crucial point is that it's not enough to mean well; one has to learn how things work and actually follow the rules. There are two reasons for this. First, good intentions are no good without the ability to foresee accurately the effects of one's actions. Second, in any complex social system, any act is likely to have unforeseeable and unintended

consequences which must be contained to avoid harming others.[4] These principles hold not only for computing, but also for other areas of life.

Appendix: University of Georgia policies on use of computers

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 "Relevant Laws," 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 1244.

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.

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.

Definitions:

- **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.
- **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.

Rules:

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.**

   Comment: Computers and networks are just like any other University facilities — they are to be used only by people who have permission.

   Using a computer without permission is theft of services and is illegal under state and federal laws. In addition, the following specific computer crimes are defined by state law (Ga. Code 16-9-90 et seq.):

[4] On this point see Sir Karl Popper, "Towards a Rational Theory of Tradition," in his *Conjectures and Refutations* (New York: Harper and Row, 1963), 120–135.

- *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);
- *Computer password disclosure* (unauthorized disclosure of a password resulting in damages exceeding $500 — in practice, this includes any disclosure that requires a system security audit afterward).

Maximum penalties are a $5,000 fine and 1 year of imprisonment for password disclosure, and a $50,000 fine and 15 years of imprisonment for the other computer crimes, plus civil liability.

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

   Comment: Many of the other regulations given here deal with specific acts of this kind. You should not assume that other malicious acts or deliberate security violations are permissible merely because there is no specific rule against them.

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.**

   Comments: State and federal laws forbid malicious disruption of computers. The University of Georgia 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.

   Also, you should be aware that *ability* to use a remote computer does not constitute *permission.* Some computer services *are* open to the public, and clearly identify themselves as such; examples are anonymous FTP sites and Gopher servers. But the mere lack of security measures does not mean that a computer is open to anyone who wishes to use it. The same goes for unauthorized use of communication paths, such as remote dialout modems and the like.

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.**

   Comments: The applicable requirements depend on what kind of connection is being made. For example, dialing up with an ordinary asynchronous modem does not require any special authorization, but connecting to the campus–wide Ethernet cable does, because one improperly configured machine on a network can cause widespread disruption.

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.**

   Comments: If you need an unusual amount of disk space, CPU time, or other resources, check with the administrators in charge of the computer rather than risk disrupting others' work. When resources are tight, work that is necessary to the University's mission (instruction, research, and service) must take priority over computing that is done to pursue personal interests or self–training on side topics. Also, no matter how important your work may be, you are only entitled to one person's fair share of the machine unless additional resources are available and appropriate permission has been granted.

   Priorities for any particular machine are set by the administrators in charge of it in consultation with the user community.

   Obtaining extra computer resources through any form of deception (e.g., secretly opening multiple accounts, misrepresenting the nature of your work, or the like) is strictly prohibited.

6. **No one without specific authorization shall use any University computer or network facility for non–University business.**

   Comments: By law, the University can only provide computer services for its own work, not for private use. In this respect the University's computers are different from those owned by private colleges or corporations. If you need unlimited access to computer networks for private purposes, you can subscribe to a private service such as America Online or CompuServe.

   The University's mission can be understood broadly as including education, self–training, and discussion on a wide range of subjects, not just those immediately necessary for a person's job or courses.

   The University grants the use of its facilities to numerous organizations whose activities contribute to its mission, such as student organizations, professional societies, and the Campaign for Charities. But it is improper to use the University's computers for political campaigns, fund–raising, commercial enterprises, mass mailings, or other outside activities that have not been granted the use of the University's facilities.

   Various policies permit members of the University community to earn outside income by writing books and articles related to their academic work, and to use University resources for this purpose, including computers. Most faculty are also permitted to use University facilities for outside consulting jobs provided the University is reimbursed for costs incurred. Check with your supervisor to find out how these policies apply to you.

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.**

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 *University* has authorized them.

A password is like the key to a building — you are responsible for what happens to it while it's in your care. If you give it away, you are endangering the entire machine, not just your own files. In fact, there are computer criminals who would like to have your password so they can make it look as though you, not they, are committing their crimes.

You are responsible for choosing a secure password. *Don't use names, nicknames, phone numbers, or recognizable words in any language,* because some people guess passwords by automatically trying every word in a large dictionary.

A good way to make up a secure password is to use the initials of a phrase, and include some numbers as well as letters. For example, `57ityMwb` is a good password, and it's easy to remember because it stands for " '57 is the year Michael was born."

Your password is secret. System administrators will not normally ask you for it. The computer will never ask you to type it unless you are logging in or changing your password. Beware of computer programs that ask you to "log in again" or type your password at any other time; they are likely to be tricks. (There are rare exceptions on some computers; check with your system manager. If anything that you don't understand ever happens after you type your password, then change your password immediately.)

If you need to work with someone else on a project, don't share a password; instead, arrange to share file space. Learn how to use file permissions, groups, and other security features of the system you are using.

8. **No one shall misrepresent his or her identity or relationship to the University for the purpose of obtaining or using computer or network privileges.**

   Comments: Naturally, you must not claim to be someone else, nor claim to have a different relationship to the University than you actually do, when obtaining a computer account or access to a lab.

   All access to the Internet through the University's facilities is restricted to people who are identified to the University, even if the purpose is to use a computer elsewhere.

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.**

   Comments: Don't even TRY to guess or steal other people's passwords, or read their files, even if the computer permits this. Doing so would be like rummaging through someone else's desk. Even if you can pick the lock, and even if there is no lock at all, you have no right to intrude.

10. **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 University's computers. It also forbids installing or using pirated software on University computers.

The price of a piece of software isn't just the cost of the disk — it's also one user's share of the cost of developing and supporting it. It's wrong to use software without paying your fair share.

Not only that, but the University benefits from the generosity and good will of many software vendors; any sign of software piracy would bring this generosity to a halt and result in higher prices for everybody.

As if that weren't enough, unauthorized copying is usually a violation of federal copyright law.

Some educational software licenses forbid the use of the software for commercial purposes. Some software is "site licensed" and can be used on any University computer. (The terms of various site licenses differ.) Some software is genuinely free; the author allows everyone to use it free of charge. Before copying software, BE SURE what you are doing is legal, and consult people who have full information; don't just give yourself the benefit of the doubt.

License checks: If strangers show up at your computer site saying they are there to check software licenses, you should immediately contact Legal Affairs and your administrative superiors. After hours, contact Campus Police. Software licenses do not normally authorize these surprise inspections, and there is a substantial risk that the "inspectors" are not legitimate.

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.**

    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. Even when the harm done by programs of these types is not readily evident, they confuse beginning computer users, degrade CPU performance, and waste the time of system managers who must remove them.

12. **No one without proper authorization shall modify or reconfigure the software or hardware of any University computer or network facility.**

    Comments: Do not modify the hardware, operating system, or application software of a University computer unless you have been given permission to do so by the department or other administrative unit that is in charge of the machine. The other users with whom you share the machine, and the technicians on whom you rely for support, are expecting to find it set up exactly the way they left it.

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.**

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 U.Ga. policy, to be kept confidential. It is also necessary to protect confidential information about employees, such as performance evaluations. This applies not only to networked computers, but also to computers, tapes, or disks that could be stolen; an increasing number of computer thieves are after data rather than equipment.

The University will normally respect your privacy but cannot guarantee it absolutely. There are many ways a normally private file can end up being read by others. If a disk is damaged, a system administrator may have to read all the damaged files and try to reconstruct them. If email is mis–addressed, it may go to one or more "postmasters" who will read it and try to correct the address. For your own protection, system administrators will often look at unusual activity to make sure your account hasn't fallen victim to a "cracker."

The Georgia Open Records Act applies to information stored in computers. This act gives citizens the right to obtain copies of public records, including any record prepared, received, or maintained by the University in the course of its operations. Some kinds of records are exempt; among these are student records (including tests and homework), medical records, confidential hiring evaluations, trade secrets (which probably includes unpublished research), and material whose disclosure would violate copyright. Moreover, the Open Records Act is not a license to snoop; requests for information must be made through proper administrative channels.

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.**

    Comments: You have exactly the same responsibilities on the computer network as when using other forms of communication. You must obey laws against fraud, defamation, harassment, obscenity, solicitation of illegal acts, threatening or inciting violence, and the like. Bear in mind that uninvited amorous or sexual messages are likely to be construed as harassment. If you are bothered by uninvited email, ask the sender to stop, and then, if necessary, consult a system administrator.

    Use of the computers to circulate chain letters and pyramid schemes is not permitted. If someone says, "Forward a copy of this to everyone you know on the Internet," *don't.* Such messages often contain misunderstood or outdated information, or even outright hoaxes. Even when the information is legitimate, chain forwarding is a needlessly expensive way to distribute it.

    Send electronic mail only to people you actually wish to contact — not to randomly chosen individuals who just happen to be on the same campus. (Well–known people do not like to serve as secretaries for their entire institutions.) If you do not have the email address of the person you want to reach, use ordinary mail or the telephone.

Never participate in schemes to deliberately flood a computer with excessive amounts of email. "Mail bombing" can incapacitate a whole computer or even a whole subnetwork, not just the intended victim.

Never falsify your name or status when using privileges such as electronic mail and newsgroups. On some computers, *anonymous* communication (concealing your name) is sometimes permitted. *Deceptive* communication, in which your messages appear to come from another specific person, is never allowed.

It is considered good practice to use your real name, rather than a nickname or pseudonym, in the headers of all outgoing communications. Use of nicknames is often interpreted as a sign of immaturity or an indication that you are not taking full responsibility for what you are sending out.

Fake electronic mail: 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.

15. **Users shall comply with the regulations and policies of newsgroups, mailing lists, and other public forums through which they disseminate messages.**

    Comments: When participating in Usenet newsgroups and similar forums, you must respect their policies and practices, for two reasons:

    - To join these networks, the University has to agree to abide by their policies. Misuse would endanger the University's eligibility to participate.
    - Most of the cost of transmitting any message in a discussion is borne by the sites that receive it, not the site that sends it out. Thus, you are the guest of the whole network community, and it is important to abide by the policies and practices of the entire network.

    The most ironclad rule is to *respect the announced subject of each forum and not to post anything off-topic.* Other things that are generally unwelcome include:

    - Advertisements (except that many forums permit announcements that are directly relevant to their subject areas);
    - Multiple postings of the same material (a general–interest message should go in one general–interest forum, not several specialized ones);
    - Survey questionnaires and other mass solicitations;
    - Questions that are easily answered by looking in dictionaries, encyclopedias, or readily available software manuals;
    - Requests for help with homework;
    - Uninformative criticisms of other people's postings (unwelcome material posted by others should be ignored, not discussed);
    - Postings that are misspelled, obscurely worded, or TYPED IN ALL CAPITALS LIKE THIS;

- Postings that say "Test message, please ignore" (try out your software when you actually have something to say, or use a test newsgroup).

Before posting anything, make sure that you know how to cancel it in case you subsequently discover that it is redundant or misinformed. Also, before posting in any Usenet newsgroup, read the appropriate guidelines for new Usenet users, and read some of the messages that are already there so you can be sure you have not misjudged the newsgroup's subject or purpose.

Always assume that everyone in the entire world can read what you are posting, that permanent copies will be kept at several sites, and that you will be expected to take full responsibility for everything you say. Do not post anything that you would not want to see quoted in a major newspaper.

Remember that newsgroups are not confined to the United States and are certainly not confined to students. You will sometimes see postings from other countries in their native languages, and you will often see postings from senior professionals in their fields.

16. **System administrators shall perform their duties fairly, in cooperation with the user community, the appropriate higher–level adminstrators, 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.**

    Comments: The first responsibility of any computer or network administrator is to serve the user community. But regardless of what the users want, system administrators are not free to violate copyrights, software licenses, other legal restrictions, or obligations undertaken by the University in order to obtain funding.

    Although computer users' privacy is never perfect, system administrators are expected to respect this privacy as far as possible and refrain from unnecessary snooping. Administrators who must read users' files for administrative reasons must be prepared to justify their actions to higher administrators and to the user community.

    System administrators should not normally interfere with users' electronic communication, especially in any way that could be interpreted as favoring one side of a controversy or suppressing an unpopular opinion or topic. As far as possible, decisions affecting access to online information services should be made in full consultation with the user community, taking into account the cost of the computer resources involved.

    The system administrator is not the judge, jury, and executioner in cases of computer misuse. Rather than penalizing users directly for their misdeeds, the system administrator is expected to refer all cases to appropriate authorities who can protect the rights of the accused. If you are accused of any violation that justifies disciplinary action, you have a right to a fair hearing just as if your alleged misdeeds had not involved computers.

    It is important to distinguish actions taken to *punish a person* from actions taken to *protect a system.* If your account appears to have been misused or broken into,

your system administrator will inactivate it and contact you or wait to hear from you. This is done to stop the misuse and does not presume that you are the guilty person; you can expect to have your privileges reinstated right away, with new passwords, as soon as you identify yourself and indicate willingness to follow the rules. Thus, you can resume using the computer while investigation of the incident continues.

Relevant laws:

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.

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.