

(published by the Computer Services Division of Libraries and Information Sciences)

These guidelines apply to you whether you are using University computers or are using your personal computer equipment while associated with the University.

Authorized Access

Only authorized users are allowed access to University computing resources.

You are responsible for any activity from your account. Do not let others use your account. Never give your password to anyone else.

Do not leave an active session unattended; always log off when you've completed your work.

Do not represent yourself as anyone else in email correspondence or web documents; do not imply you represent the University.

Privacy

University computing systems maintain strict safeguards to protect your privacy. Your accounts and files, however, can be compromised if you are lax in your gatekeeping!

Choose a password that will be easy for you to remember, but impossible for others to guess (a mix of letters and numbers is best, and steer clear of any word found in the dictionary). For example, the first letter of each word in an easy-to-remember phrase (Jane's going to France next semester -- jg2fns) is a good choice. Change your password regularly!

Be advised that electronic mail should never be considered a completely secure means of communication. If your mail is addressed incorrectly it can end up in the hands of email administrators (best case) or unscrupulous others (worst case). Remember that FORWARD is a built-in function of all electronic mail packages -- anyone can easily forward your message to others. Never send anything via email you would mind seeing on the evening news!

Harassment

It is against the law and University policy to harass someone through email. Harassment is not tolerated in any form. The University gives full support to investigations of messages described as obscene, harassing, and/or threatening. Do not send or forward harassing, fraudulent, obscene, threatening, or defamatory messages or materials to anyone.

Other Legalities

Copyright, obscenity, libel, and other laws governing communication and publication apply to electronic media as well: communications that would be illegal or that would violate University policy in the "off line" world are equally illegal or in violation of University policy when they occur online.

Reasonable Use of Resources

- University resources should be used with discretion and with respect for others. University resources are shared, and should not be monopolized or used for personal gain.
- Commercial use and profit-making ventures are not permitted. Junk mail, spamming, chain letters, and sales pitches are forbidden.
- Copying or distributing proprietary software is forbidden.
- Plagiarism standards also apply to electronic media; do not copy without permission or misrepresent others' ideas, images, or words as your own.
- Respect University equipment and systems.
- Use virus protection software (free copies are available from Computer Services) to protect yourself and others from possible malicious computer viruses.
- When transferring files via electronic mail, limit the size to approximately half-a-megabyte (this is approximately 100 pages of text); larger files can cause traffic problems and may be rejected by

many email systems.

- Obtain other's permission before forwarding mail sent to you in confidence.
- Regularly delete files and email messages you no longer need to save system resources.
- If including email attachments, be sure your recipient can use the file format you send; not all formats are portable.
- Be courteous and careful when sending email. Sign your messages and include a subject. Proof your messages carefully to be sure they are addressed to the appropriate person(s) and are in an appropriate tone. Mail composed in haste can seem terse and offensive; a few moments rereading a message can save you embarrassment and difficulties later.

Reporting Violations

If you suspect your account has been compromised, or you feel you have been violated by others, please keep copies of all relevant electronic documents and contact Computer Services (security@sc.edu or call 777-1800) as quickly as possible. Computer Services will work with appropriate University officials to resolve any reported violations.

Consequences of Computing Abuse

Abuse of University computing systems and inappropriate electronic actions by members of the University community can result in the loss of computing privileges, initiation of legal action by the University, and/or appropriate disciplinary action.

Detailed University Computing Policies

For explicit policies related to computing and student conduct, refer to the computing policies website:
www.sc.edu/csd/policies.html

General Questions about Computing

Information on applying for University internet/email accounts, computer training, and general information on computing at the University are available from Computer Services, (803)777-1800.

General information, specifics for incoming students, and a collection of frequently asked questions are available from the Computer Services website: www.sc.edu/csd