COMPUTER USE POLICIES

I. Introduction

North Carolina State University’s (hereinafter "University") computer networks, equipment and resources are owned by the University and are provided primarily to support the academic and administrative functions of the University. The use of this equipment and technologies is governed by federal and state law and University policies and procedures.

II. Regulatory Limitations

A. Accounts are for the exclusive use of the individual to which they were assigned, and users may not allow or facilitate access to University computer accounts, equipment, or restricted files or systems by others. Users may not set up a proxy or anonymous remailer for purposes of allowing access to others.

1. Students and employees of NC State are authorized users unless access privileges have been revoked under University procedures.

2. Guest accounts may be authorized by the Associate Vice Chancellor for Finance and Information Systems or the Vice Provost for Information Technology, or their designees.

B. The University may examine electronic information stored on or passing over University equipment or networks for the following purposes:

1. To insure the security and operating performance of its systems and networks.

2. To enforce University policies or compliance with state or federal law where:
   a. Examination is approved in advance by a dean, vice chancellor, or vice provost, and either
   b. there is a reasonable suspicion that a law or University policy has been violated and examination is appropriate to investigate the apparent violation, or
   c. examination is necessary to comply with a state or federal law.

   Computer users should have no expectation of privacy in the material sent, received, or stored by them on or over the University computing systems or networks when the conditions of subparagraph 1, or 2(a) and 2(b), or 2(a) and 2(c) above have been satisfied.

C. The University reserves the right to limit access when federal or state laws or University policies are violated or where University contractual obligations or University operations may be impeded.

D. The University may authorize confidential passwords or other secure entry identification; however, users should have no expectation of privacy in the material sent or received by them over
the University computing systems or networks. While general content review will not be undertaken, monitoring of this material may occur for the reasons specified above.

E. All material prepared and utilized for purposes of University business and posted to or sent over University computing equipment, systems or networks must be accurate and must correctly identify the sender, unless a University administrator (department head or higher) approves anonymity for a University business purpose.

F. Any traffic on the University’s networks, stripped of information content, may be monitored for operational or research purposes.

G. All material prepared for purpose of University business and posted to or sent over University computing equipment, systems, or networks must be limited to information needed for University business. Personal quotations or other personal statements in signature blocks are not permitted. Supervisors are responsible for enforcement of this provision.

III. Personal Use

Authorized users may access University computing equipment, systems and networks for personal uses if the following conditions are met:

A. The use is lawful under federal and state law.

B. The use does not violate any policy or directive of the Board of Governors, the NC State Board of Trustees, the UNC General Administration, or the NC State administration.

C. The use does not overload the University computing equipment or systems, or otherwise negatively impact the system’s performance.

D. The use does not result in commercial gain or private profit, except as allowed under University intellectual property policies and the external activities for pay policy. However, in no case may University computing resources be used for solicitation of external activity for pay.

E. The use does not violate any University licensing agreements or any law or University policy on copyright and trademark.

F. The use does not state or imply University sponsorship or endorsement.

G. The use does not violate laws or University policies against race, sex, religious, disability, or age discrimination, or harassment.

H. The use does not involve unauthorized passwords or identifying data that attempts to circumvent system security or in any way attempts to gain unauthorized access.

I. The use does not involve sending or soliciting chain letters, nor does it involve sending unsolicited bulk mail messages (e.g., “junk mail,” or “spam,” or “MLM.”).

J. The use does not result in any direct cost to the University.

K. Any creation of a personal World Wide Web page or a personal collection of electronic material that is accessible to others must include a disclaimer that reads as follows:
L. University computers must be registered with NC State in the ncsu.edu domain. It is forbidden to register a non-ncsu.edu domain for any computer which is connected to the NC State network without prior approval of the Associate Vice Chancellor for Finance and Information Systems or the Vice Provost for Information Technology. If such approval is given, it must be made clear that the non-ncsu.edu address is using NC State resources for delivery.

IV. Use of Computing Facilities for Commercial, Advertising, and Broadcast Purposes

A. No paid advertising will be allowed on official University Websites. However, an NC State Website may contain a simple acknowledgment of sponsorship by an outside entity in the following form: "Support for this Website [or university unit] has been provided by ____________.”

1. An “official University Website” is any World Wide Web address that is sponsored or endorsed or created on authority of a University department or administrative unit. Websites on University servers are either “University Websites” or personal websites allowed by the University.

2. “Paid advertising” means advertising or promotional information provided in exchange for legal consideration, including money or other valuable benefits.

B. Personal web pages that are maintained by University computer account holders may not contain paid advertising. This guideline is consistent with the University policy against use of University resources for private gain or commercial purposes.

C. University computer account holders may send advertisements to news groups dedicated to advertising. The ads may not refer readers to a University telephone number. Like other personal use of State computing resources, the ads must be sent on an employee’s own time, not during hours when they are being paid to work.

D. University computer account holders may not “broadcast” E-mail messages without prior approval from a University official with the rank of chancellor, provost, vice chancellor for finance and business, or their designees. “Broadcast” means transmission of a message to a significant number of computer accounts on a University server or servers; the intent is to prevent mass mailings from tying up employee time and computer resources.

E. Registered marks of the University (e.g., an image of a wolf) may be used in the Websites of University computer account holders on the conditions that (a) they are not used for or related to private profit or commercial purposes, and (b) they do not mislead or confuse viewers as to whether the Web page is University-sponsored.

F. The Chancellor or designee may approve specific exceptions to the prohibition on paid advertising.

V. Violation of Policy

A. Any violation of this policy by employees may be “misconduct” under EPA policies (faculty and EPA non-faculty), or “unacceptable personal conduct” under SPA policies. For students, violations...
are misconduct under the applicable student disciplinary code. Violators may be referred to the appropriate disciplinary procedure, and violations of law may also be referred for criminal or civil prosecution. Sanctions may include revocation of access privileges in addition to other sanctions available under the regular disciplinary policies.

B. Apart from referrals to disciplinary procedures, a University system administrator (or designees) may suspend a user’s access privileges or suspend services to a computer for as long as necessary to protect the University’s computing resources, to prevent an ongoing threat of harm to persons or property, or to prevent a threat of interference with normal University functions. As soon as practicable following the suspension of access privileges, the system administrator must take the following actions:

1. The user must be sent written or electronic notice of the suspension of access and the reasons for it, and notice of the time, date, and location at which the suspension may be discussed with the system administrator.

2. The user must be given an opportunity to meet with the system administrator at his or her earliest convenience to discuss the suspension and present any reasons the user has why the suspension should be lifted. The system administrator must reconsider his or her suspension decision in light of the information received at this meeting.

3. Following the meeting, the user must be sent a copy of the system administrator’s decision upon reconsideration, and must be notified that the user may appeal to the system administrator’s immediate supervisor if the user is dissatisfied with the outcome of the meeting.

VI. Application of Public Records Law

All information created or received for University work purposes and contained in University computing equipment files, servers or electronic mail (e-mail) depositories are public records and are available to the public unless an exception to the Public Records law applies.

VII. Additional Rules

Additional rules and regulations on computer use may be adopted by various divisions/departments to meet specific administrative or academic needs. Any adopted requirement must:

A. Comply with applicable federal and state laws;

B. Be consistent with the policies of NC State and the University of North Carolina;

C. Be posted in writing or electronically in a manner that is available to all affected users; and

D. Be filed with the Office of Legal Affairs, the Associate Vice Chancellor for Finance and Information Systems, and the Vice Provost for Information Technology.

Authority: Issued April 9, 1999, by Chancellor Marye Anne Foxe. Changes or exceptions to administrative regulations issued by the Chancellor may only be made by the Chancellor.

Computer and Network Use: Remote Access and Labs

All users of North Carolina State University’s computer and network systems must abide by federal and state law and University policies and procedures. The University’s Administrative Regulations – Computer Use issued by the Chancellor and reproduced above, govern all computer use at NC State. The following additional rules govern the computer and network systems supported by campus Information Technology/Computing Services and the College of Engineering.

Use of Remote Access Services

Information Technology provides a limited number of free modem lines and remote access servers for use by the University. The remote access servers are commonly called dialup servers and telnet servers, and include, among others, login.ncsu.edu and ssh.ncsu.edu. The dialup/login machines are to be used for academic work.

Do not play games. Do not use chat programs such as IRC, ICQ, or AIM. Do not use MUDs, MUSHs, or other recreational Bulletin Boards. Do not log into a dialup and then log into other machines.

Running any CPU or memory intensive programs for prolonged periods of time or in the background is prohibited. This includes, but is not limited to setiathome, rc5des clients, and graphical web browsers (such as Netscape). Do not use the dialups as batch or compute servers.

Do not use the dialups as servers to support graphical login sessions. Running a single program back to your display is acceptable, as long as it doesn’t violate the above rules.

Violators of the above mentioned rules will be handled strictly according to the Administrative Computer Usage Regulations and Computer and Network Usage Policy, so heed this message. You could lose your Eos/Unity privileges.

Use of University Computing Labs

1. All those who use University facilities are expected to take proper care of the equipment. Any equipment malfunction should be immediately reported to staff on duty or to the organization responsible for the facility. Users of computing facilities may not move, repair, reconfigure, modify, or attach external devices to the computing systems. No food or drink is permitted in University computing facilities.

2. Recreational use of workstations in University computing labs during periods of light usage is permitted; however, no one may play games or engage in other recreational activities on workstations when others are waiting to use them for academic purposes. It is the responsibility of game players to recognize when resources are needed and to give up their seats to other users. It should not be necessary for someone to ask them to move.

3. Users must realize that they are in an academic facility and refrain from noise, sound effects, violent motion, etc., which may disturb others in the facility.

4. Individual Computing Services (Unity) computing labs and other University–owned computing labs may post additional operational rules and restrictions, which must be filed with the University’s Office of Legal Affairs. Users are responsible for reading and following these rules.

Violations of policy will be treated as academic misconduct, misdemeanor, or felony as appropriate.
**Misdemeanor or felony** violation charges will be prosecuted to the fullest extent of the law and may result in the immediate and permanent loss of privileges. Student disciplinary proceedings may also be initiated against violators.

**Computer and Network Use Regulations and Rules**

See [http://www.ncsu.edu/it/rulesregs/](http://www.ncsu.edu/it/rulesregs/)

**ResNet Terms and Conditions**


**Policies in Eos Public Labs**

No food or drink.
No smoking or chewing tobacco.
No sharing accounts and passwords.
No display of sexually explicit images.
No noise or loud talking.
No recreational use of workstations if lab is busy.
Do not leave workstation unattended.
Do not turn off or unplug workstations.
Always log out before leaving.
Leave workstation area clean.
Take care of equipment and furniture.

Vandalism, theft, harassment, security violations, and misuse of computing resources are grounds for dismissal from the university. Computers are for academic use only. No commercial use of resources is permitted.

**Use of Cell Phones in Eos Public Labs, approved January 31, 2001, by the College of Engineering Computer Committee.**

Owners of cell phones should exercise courtesy to those around them by taking personal calls that are longer than 15 seconds to an area away from computing facilities, preferably outside the building or in lounge areas. Ringers should be set on the lowest setting or on vibrate. Voices should be kept low when speaking so that the labs remain conducive to work and study.

Complete and updated policies on campus computing are available at:

[http://www.ncsu.edu/it/rulesregs/](http://www.ncsu.edu/it/rulesregs/)