

ACCEPTABLE USE OF COMPUTING AND ELECTRONIC RESOURCES POLICY

(Available on-line at http://its.uncg.edu/Policy_Manual/Acceptable_Use/)

(Approved by Chancellor, July 19, 2004)

(Revised March 10, 2009)

I. PURPOSE

The purpose of this policy is to outline the acceptable use of computer and information technology resources provided by The University of North Carolina at Greensboro (hereinafter "the University") to University students, employees, and authorized affiliates. Inappropriate use exposes the University to risks, including breach of personal computer security, exposure of restricted data, compromise of network systems/services, detriments to technology performance, and legal liability. The Information Technology (hereinafter "IT") unit of the Information Technology and Planning division is committed to protecting students, employees, affiliates, and the University from illegal or damaging actions by individuals, either knowingly or unknowingly.

In support of the University's mission, IT provides technology and electronic information systems, including but not limited to computer equipment, software, operating systems, storage media, and network accounts providing electronic mail, web browsing, and file transfer, that are the property of the University. These systems are to be used only for business and academic purposes in serving the interests of the University in the course of normal operations.

II. SCOPE

This policy applies to students living on campus, commuting students and their guests while on the University campus, University employees (including student employees), contractors, consultants, temporaries, and other workers at the University, including all personnel affiliated with third parties. This policy also applies to any member of the University community who accesses the campus network from off-campus locations. It also applies to non-affiliates as defined in the *Security of Networks and Networked Data Policy*.

This policy applies to all equipment that is owned or leased by the University and governs activity on personal machines while on the University campus as well as all communications to and from the University while off campus. The University generally does not monitor material residing on University computers housed within a private domicile or on non-University computers, whether or not such computers are attached or able to connect to campus networks.

III. POLICY

A. General Use and Ownership

It is the responsibility of every University student, employee and affiliate who deals with information and/or information systems to know these guidelines, and to conduct his or her activities accordingly.

Students and employees using personal machines may be subject to restricted network access and may only be permitted access to data that is classified as *public* under the *Data Classification Policy*. Students and employees may not access *restricted* data on personal machines except for purposes and practices authorized by the appropriate *Data Trustee* or *Data Steward* under the *Data Classification Policy*.

Students and employees are permitted to use University-owned machines in computer labs and in public locations after authenticating with the central account database. Any public non-authenticated access will be restricted to limited network resources for specific, defined purposes.

There should be no expectation of privacy in the material sent or received when using the University network, University computer systems, or third-party vendor applications provided by the University (e.g., Google email services). By activating your University computer account, you agree to receive via email University security breach notifications covered by the N.C. Identity Theft Protection Act and other official University communication. For security, legal or policy compliance, quality of service, and network maintenance purposes, authorized individuals within IT may monitor equipment, systems, and network traffic. General content review will not be undertaken, although monitoring of content may occur for the reasons stated above.

All data created or received for work purposes and contained in University electronic files, servers, or e-mail depositories are public records. Public Records are available to the public unless specifically prohibited from general viewing by law or contract. See the *Data Classification Policy*. All public records are to be maintained and disposed of according to state approved records retention and disposition schedules. See *Public Records Law*.

Students and employees are responsible for exercising good judgment regarding the use of technology and information systems. Use of these systems is permitted, with the following restrictions:

- The use is lawful under federal or state law.
- The use complies with applicable University policies and guidelines.
- The use is not prohibited by Board of Governors or University policies, including rules regarding academic integrity, harassment (including sexual harassment), and discrimination on the basis of any federally protected characteristic or sexual orientation.
- The use does not result in commercial gain or private profit (other than allowable under University intellectual property policies) and does not violate the North Carolina Umstead Act. That Act prohibits government agencies from competing with the private commercial activities of North Carolina citizens.
- The use does not violate federal or state laws or University policies on copyright, trademark, or software licensing.
- The use does not intentionally or unintentionally overload University computing equipment or systems, or otherwise harm or negatively impact the system's performance or the support of such systems.
- Communications originating from the user are identified as such and the user assumes responsibility for all communication originating from equipment or accounts assigned to that user. In the case of security breaches related to accounts or equipment belonging to the user, the user acts quickly to report and correct the situation.

- The use does not attempt to circumvent system security or in any way attempt to gain or provide unauthorized system or network access.
- All resources and data accessed are protected by the user according to the standards set forth in the *Security of Networks and Networked Data Policy* and *Data Classification Policy*.
- Reasonable personal use does not state or imply University sponsorship or endorsement and must not interfere with an employee's job performance or activities which directly support the University mission.

Individual departments may create additional guidelines concerning use, as long as such guidelines are in accordance with this and other University policies.

B. Security and Proprietary Information

To protect the integrity of the campus network and any data stored there, users must adhere to the *Security of Networks and Networked Data Policy*.

Any information that users consider sensitive or vulnerable and any information that is deemed restricted under federal or state law should be protected. For guidelines on information classification, see the University's *Data Classification Policy*. For guidelines on protecting e-mail and other data, refer to ITS's Help Desk and online resources.

C. Unacceptable Use

Under no circumstances is a student or employee of the University authorized to engage in any activity that is illegal under local, state, federal, or international law, while utilizing University-owned resources.

Employees may be exempted from "unacceptable use" restrictions during the course of their legitimate job responsibilities (e.g., IT systems and networks administration staff may need to disable the network access of a host, if that host is disrupting production services).

The list below provides a framework for activities that fall into the category of unacceptable use. It is not all inclusive, but is intended to give examples of the type of activities that are prohibited.

Prohibited System and Network Activities

The following activities are strictly prohibited, with noted exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the user or device.
- Unauthorized replication or use of copyrighted material, except where such copying qualifies as "Fair Use".
- Exporting software, technical information, encryption software or technology in violation of international or regional export control laws. Legal counsel and appropriate management should be consulted prior to export of any material that is in question.

- Intentionally or recklessly introducing or transmitting destructive or malicious programs such as viruses into the network or networked devices.
- Revealing account passwords to others or allowing use of accounts by others. This includes family and other household members.
- Using a computing asset to actively engage in procuring or transmitting material that is in violation of state/federal law or University policies.
- Originating from any University account or equipment commercial offers of products, items, or services in violation of the Umstead Act.
- Effecting security breaches or disruptions of network communication such as accessing data of which the employee is not an intended recipient, logging into a server or account that the employee is not expressly authorized to access, attempting to intercept others' passwords, or impersonating another user.
- Port scanning or security scanning is strictly prohibited, with one exception. Individual host port/security scanning is allowed only with permission from the administrator of the target host. Authorized IT employees are permitted to port/security scan as part of their normal job duties.
- Executing any form of network monitoring which will intercept data not intended for the employee's host. Authorized IT employees are permitted to monitor network traffic data as part of their normal job duties.
- Circumventing user authentication or security of any host, network, or account.
- Interfering with or denying service to any user.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the network.

Prohibited E-mail and Communications Activities

The following activities are strictly prohibited, with no exceptions:

- Forwarding restricted University e-mail to unauthorized recipients.
- Sending unsolicited mass e-mail messages without proper unit authorization, posting unsolicited and inappropriate list/web/newsgroup messages, including the sending of "spam" (junk e-mail) or other commercial advertising material to individuals.
- Any form of harassment via means such as e-mail, instant messaging, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use/deliberate disguising of the sender or forging of e-mail header information. Alteration of content of an e-mail message originating from another sender with intent to deceive.
- Hosting an e-mail transport/relay service outside of supported and authorized IT systems.
- Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or otherwise misuse e-mail resources.
- Creating or forwarding "chain letters" or "pyramid schemes" prohibited by law.
- Activities in violation of the *E-mail Retention Policy* .

IV. ENFORCEMENT

IT will enforce the *Acceptable Use of Computing and Electronic Resources Policy* and establish standards, procedures, and protocols in support of the policy. Users shall be notified of the *Acceptable Use of Computing and Electronic Resources Policy* upon initial request for University computing accounts.

Violations of this *Acceptable Use of Computing and Electronic Resources Policy* may result in suspension or termination of access to computing accounts, the network and networked resources, and/or other University-owned technology devices. Any violation of this policy by a University student is subject to the Student Code of Conduct in the student handbook. For employees, any violation of this policy is “misconduct” under EPA policies (faculty and EPA non-faculty) and “unacceptable personal conduct” under SPA policies, including any appeal rights stated therein. Violations of law may also be referred for criminal or civil prosecution.

V. REVIEW

The Chancellor has approved the *Acceptable Use of Computing and Electronic Resources Policy* and the Information Security Committee will periodically review the policy as appropriate.

VI. LINKS TO RELATED UNIVERSITY POLICIES

Data Classification Policy

Enterprise Systems Policy

Security of Networks and Networked Data Policy

Standards for Computer and Related Technology (Supported Products List)

E-Mail Retention Policy

Wireless Communications Policy