FAYETTEVILLE STATE UNIVERSITY

USE OF COMPUTER RESOURCES

Authority:	Issued by the Chancellor. Changes or exceptions to administrative policies issued by the Chancellor may only be made by the Chancellor.
Category:	University-Wide
Applies to:	●Administrators ●Faculty ●Staff ●Students
History:	Revised – September 17, 2010 Approved – February 2, 2010 First Issued - February 3, 2010
Related Policies:	*Electronic Mail Accounts*
Contact for Info:	Vice Chancellor for Information Technology and Telecommunications (910) 672-1477

I. PURPOSE

This policy governs the use of University computer resources provided by Fayetteville State University ("University") to University students, employees, and other authorized users (i.e., contractors, consultants, temporaries, and any other individuals having authorized access) and applies to all computer and computer communication facilities owned, leased, operated, or contracted by the University. This includes, but is not limited to, word-processing equipment, microcomputers, minicomputers, mainframes, computer networks, computer peripherals, software, cellular devices, e.g., mobile phones, blackberrys, and cellular wifi cards ("computer resources"). The policy extends to any use of University facilities to access computers elsewhere. These computer resources are to be used only for University administrative and academic purposes.

II. AUTHORIZED USE

Use of University computer resources is restricted to authorized users. For the purposes of this policy, an "authorized user" shall be defined as an individual who has been assigned a login ID and password by Information Technology and Telecommunications System (ITTS) staff (on any relevant system). Individual users are responsible for the proper use of their accounts, including the protection of their login IDs and passwords. Users are also responsible for reporting any activities which they believe to be in violation of this policy.

Users should use only those computer resources they have been authorized to use. Such use shall be as follows:

- in a manner consistent with the terms under which the user was granted access to them;
- in a way that respects the rights and privacy of other users;
- so as not to interfere with or violate the normal, appropriate use of the University's computer resources; and

- in a responsible manner.

Any creation of a personal World Wide Web page or a personal collection of electronic material that is available to others must include a disclaimer that states as follows:

The material located at this site is not endorsed, sponsored or provided by or on behalf of Fayetteville State University

III. UNAUTHORIZED USE

A. Unauthorized Activities

Under no circumstances shall a student, employee or other authorized user engage in any of the following activities while using University computer resources. Please note that 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.

- Illegal acts under local, state, federal, or international law;
- Promoting or conducting personal (non-university) enterprises, i.e., private businesses (applies to employees or other authorized user);
- Redistribution, which includes, but is not limited to copying, transmitting, or disclosing data, software or documentation, without proper authorization, of any software licensed or owned by the University, except in the case of software which is clearly marked as being in the public domain.
- Harassment, which includes but may not be limited to interfering with the legitimate work of another user and/or sending abusive or obscene messages;
- Intentionally accessing or disseminating pornography unless (1) such use is specific to work-related functions and has been approved by the user's respective Vice Chancellor or (2) such use is specifically related to an academic discipline or grant/research project.
- Sending either mail or a program which will replicate itself or do damage to another user's account; or
- Tampering with or obstructing the operation of the University's computer systems (for example, attempting to "crash" the system).
- Engaging in copyright infringement or unauthorized distribution of copyrighted material, including downloading or file sharing, in violation of the University's policy on *Unauthorized Distribution of Copyrighted Work Policy*.

B. Use of Computer Resources for Commercial, Advertising, and Broadcast Purposes

1. Website Sponsorship

An *official University website* is any World Wide Web address that is sponsored, 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.

A University 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 _____."* The acknowledgment may include the sponsor's logo only if permission is granted by the sponsor and the use of the logo does not imply commercial endorsement by the University. The Office of Legal Affairs should be consulted prior to the placement of any outside entity's logo on a University website.

2. Paid Advertising

Personal web pages that are maintained by University authorized users may not contain paid advertising. *Paid advertising* means advertising or promotional information provided in exchange for legal consideration, including money or other valuable benefits. . The Chancellor or designee may approve specific exceptions to the prohibition on paid advertising.

3. Use of University Logos and Marks

Marks and/or logos of the University as designated by the University's Office of Legal Affairs may be used on the websites of authorized University users on the condition that the marks are not used for or related to private profit or commercial purposes, and/or do not mislead or confuse viewers as to whether the Web page is University-sponsored.

IV. ACCESSING UNIVERSITY COMPUTER RESOURCES

If the University is informed of inappropriate conduct associated with the use of University computer resources, the University is obligated to investigate and to enforce applicable federal and/or state law and/or policies of the University and the University of North Carolina.

In certain instances, as described below, the University may access a particular University computer resource used by an employee, student or other authorized user. Such instances shall include, but not be limited to:

- troubleshooting hardware and software problems, such as rerouting or disposing of undeliverable mail, if deemed necessary by the Vice Chancellor for Information Technology and Telecommunications ("CIO") or his or her authorized designee;
- preventing or investigating unauthorized access and system misuse*;
- retrieving or reviewing for University purposes University-related information*;
- investigating reports of violation of University policy or local, state, or federal law*;
- investigating reports of employee or student misconduct*;
- complying with legal requests for information (such as subpoenas and public records requests)*; and
- Retrieving information in emergency circumstances where there is a threat to health, safety, or University property involved*.

[*]*The system administrator will need approval from the General Counsel and/or CIO to access a particular user's account for these purposes. The extent of the access will be limited to what is reasonably necessary to acquire the information for a legitimate purpose.*

V. VIOLATIONS

A. Individuals who violate this policy are disciplined as stated below:

1. Faculty and EPA non-faculty who violate this policy shall be deemed to have engaged in misconduct under their respective employment policies.

2. SPA employees who violate this policy shall be deemed to have committed "unacceptable personal conduct" under SPA policies.

3. Students who violate this policy shall be deemed to have committed misconduct under the student disciplinary code.

4. Other authorized users who violate this policy shall have action taken depending on their particular affiliation.

B. Violators may be referred to the appropriate disciplinary process. 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.

C. Apart from referrals for disciplinary action, a University system administrator (or designees) may suspend a user's access privileges for as long as necessary in order to protect the University's computer resources, to prevent an ongoing threat of harm to persons or property, or to prevent a threat of interference with normal University function. A user whose access privileges have been suspended may meet with the system administrator as soon as practicable following the suspension of access privileges to discuss the suspension and any reasons why the suspension should be lifted.

VI. APPLICATION OF PUBLIC RECORDS LAW

All information created or received for work purposes and contained in University computer 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. This information may be purged or destroyed only in accordance with the University records retention schedule and State Division of Archives regulations.