UNIVERSITY OF NORTH CAROLINA SCHOOL OF THE ARTS

Technology Use Policy

Policy #508

Source of Authority: N.C.G.S. 116-34(a);
UNC Code § 502(A)

Revision Authority: Chancellor

History: **First Issued:** February 17, 2011

Related Policies: Business Continuity Plan Policy #104;
Code of Conduct & Discipline Policy #802;
E-Mail Policy #502;
Emergency Management Policy #701;
Improper Activities Reporting Policy #114;
IT Account Management Policy #503;
Takedown Notice Policy #507;
Unofficial Websites Policy #509;
Virtual Private Network (VPN) Policy #510

Responsible Offices: Information Technologies Department

Effective Date: February 17, 2011

I. Purpose

UNCSA computing and telecommunicating networks, computer equipment and computing resources are owned by the school and are provided primarily to support the academic and administrative functions of the school. Federal and state laws, and school policies and procedures govern the use of this equipment and technologies. In order to ensure ethical and equitable use of the school's resources, UNCSA has established these policies and procedures for their use.

II. Scope

This policy applies to all UNCSA technology users, including faculty, staff and students.

III. Definitions

A. "**Broadcast**" means transmission of a message to a significant number of computer accounts on a UNCSA server or servers.

B. "**Official UNCSA Website**" means any World Wide Web address that is sponsored or endorsed or created on authority of a UNCSA department or administrative unit. Websites on UNCSA servers are either "UNCSA websites" or unofficial websites.

C. "**Paid Advertising**" means advertising or promotional information provided in exchange for legal consideration, including money or other valuable benefits.

IV. Policy

A. General Policies

1. Access to UNCSA's computing resources are limited to members of the UNCSA community.
2. The use of computers and network resources at UNCSA is a manifestation of assent to using all systems in accordance with the rules described and referred to in this policy. You are responsible for the ways you use these systems and for the safeguarding of your account(s).
3. Use of UNCSA technology resources for direct solicitations or commercial activities for personal financial gain is strictly forbidden.
4. No individual personal rights attach to computers or other devices owned by UNCSA.
5. All information created or received for work purposes and contained in or on school computing equipment files, servers or electronic mail (e-mail) depositories are public records and are available to the public, upon approval by the Chancellor, unless an exception to the law applies.
6. UNCSA computer account holders may not broadcast e-mail messages without prior authorization from the appropriate UNCSA official or policy.
7. Use of UNCSA technological resources to violate authorial integrity, including but not limited to plagiarism, unauthorized access to information, unauthorized exploitation of trade secrets, and violation of intellectual property laws (i.e. copyright, trademark, and patent laws) is prohibited.
8. Use of UNCSA technological resources to gain access to other users' accounts, files, voice mail, or electronic mail, harassing other users in violation of university policies, or otherwise interfering with the work of others is prohibited.
9. Users who access off-campus resources using UNCSA technology must abide by the policies and procedures of the networks and systems accessed.

B. Network Access & Monitoring

1. Computer and network access accounts are for the exclusive use of the individual to which they are assigned. Users may not allow or facilitate access to UNCSA computer accounts, equipment, or restricted files or systems by unauthorized persons. Users may not set up a proxy or anonymous remailer for purposed of allowing unauthorized access to accounts or data of other users.
2. UNCSA may authorize confidential passwords or other secure entry identification; however there is no expectation of privacy in material sent or received by users over the UNCSA computing systems or networks.
3. **Authorized Users**
   a. Students and employees of UNCSA are authorized users of UNCSA technology resources, unless access privileges have been revoked pursuant to UNCSA policy and/or procedures.
   b. Contractors, Non-Agency Staff, and Guest Accounts

i. Department heads may request that the CIO authorize accounts for contractors/non-employees or guests. In such cases the department head is responsible for addressing this policy with the user and for any misuse that may occur.

ii. These accounts must be time limited and pre-expired to that time limit. The department head, in conjunction with Information Technologies ("IT"), will determine the level of access needed.

iii. The department head must notify IT when the account should be deactivated if this occurs before the predetermined expiration date.

4. UNCSA guarantees **no right of confidentially** to users of its technology resources and users should have no expectation of privacy in personal material sent, received, or stored by them on or over the UNCSA computing systems or networks.
5. General content review will not be undertaken; however monitoring of this material may occur as described in this policy.
6. Any traffic on UNCSA's networks may be monitored for operational or research purposes.
7. UNCSA may examine, without notice, any computer that is or has been connected to the UNCSA network and personal electronic information stored on or passing over UNCSA equipment or network, for the following purposes:
   a. to ensure the security and operating performance of UNCSA's systems and networks.
   b. to protect the integrity of the network and technology systems, to comply with state or federal law, or to investigate suspected abuse or violation of UNCSA policies when such examination is requested by the Chancellor, the Chief Academic Officer ("CAO"), the Chief Operating Officer ("COO"), General Counsel, or CIO.
8. For information related to UNCSA business, a supervisor or other UNCSA official may have access for any work-related purpose only after permission is granted by the COO, CAO, or either's designee.
9. All material prepared and utilized for purposes of UNCSA business and posted to or sent over UNCSA computing equipment, systems or networks must correctly identify the sender unless a UNCSA administrator (department head or higher) approves anonymity for a UNCSA business purpose
10. All material prepared for UNCSA purposes and posted to or sent over UNCSA computing equipment, systems, or networks must be limited to information needed for UNCSA business.
11. Filtering software is used in high school residence halls, labs accessible to minor students, and on any state-owned equipment if requested by the department head.

C. Personal Use

1. Subject to other provisions of this policy, authorized users may access UNCSA computing equipment, systems, and networks for personal uses under the following circumstances:
    a. the use does not overload the UNCSA network computing equipment or systems, or otherwise negatively impact the system's performance;
    b. the use does not state or imply UNCSA sponsorship or endorsement;
    c. 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; AND
    d. the use does not result in any direct cost to the UNCSA.
2. The creation of any personal World Wide Web page or a personal collection of electronic material that is accessible to others, such as a blog, which:
    i. others could reasonably be associate with UNCSA (because of content, domain, etc.) and
    ii. which is not hosted on UNCSA equipment is subject to approval by the CIO. The associated procedures contain a disclaimer which must be included on such pages and materials.
3. **Domain Registration**
    a. UNCSA computers and network devices must be registered with UNCSA in the uncsa.edu domain.
    b. It is forbidden to register a non-uncsa.edu domain for any computer or network device that is connected to the UNCSA network without prior approval of the Chancellor or the CIO.
    c. If approval is given, it must be made clear that the non-uncsa.edu address is using UNCSA resources for delivery.
    d. All routers and switches must be configured to meet UNCSA standards including, but not limited to, turning off of non-required services, and changing passwords and community strings.

D. Commercial, Advertising, and Broadcast Uses

1. No paid advertising will be allowed on official UNCSA Websites.
2. An official UNCSA website may contain a simple acknowledgment of sponsorship by an outside entity in the form proscribed by this policy's procedures.
3. Personal web pages that are maintained by UNCSA computer account holders that could be associated with UNCSA as a result of the material's content or domain or are unofficial websites as defined by the Unofficial Website Policy may not contain paid advertising.

4. UNCSA's intellectual property (e.g., logo and photographs) may be used on the websites of UNCSA 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 sponsored by UNCSA.

E. Division or Department Specific Rules. Additional rules on computer and/or network use may be adopted by various divisions/departments to meet specific administrative or academic needs in compliance with this policy's procedures.

F. Violations of Policy & Remedial Measures

1. Violations of this policy may result in suspension or removal of accounts, University discipline up to and including termination, and civil or criminal liability.
2. A user whose account has been suspended may appeal the CIO's decision upon reconsideration to the Chancellor.

V. Revision History

A. February 17, 2011 – Adopted by Board of Trustees as part of UNCSA Policy Manual

UNIVERSITY OF NORTH CAROLINA SCHOOL OF THE ARTS

Technology Use Procedures

Procedure #508

I. Policy Approved Language

A. Disclaimer Language. "The material located at this site is not endorsed, sponsored or provided by or on behalf of the University of North Carolina School of the Arts."

B. Sponsorship Acknowledgement Language. "Support for this website [or UNCSA unit] has been provided by _____".

II. Investigations of Abuse by Students

A. When a network/computer abuse by a student is reported or found in routine activities, reasonable suspicion must be established before a search of the computer or network account usage.

B. Two UNCSA staff members (one from Student Life and one from Information Technologies) review the information available and make a "good faith judgment call" as to whether a student's computer can be confiscated for investigative purposes.

C. Student Life and Campus Police policies are followed when any confiscation of computers occur.

D. More detailed procedures may be found in the appropriate Student Handbook.

III. Account Suspension

A. These steps must be taken as soon as practical following the suspension of access privileges by the CIO.

B. The user must be sent written and 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 CIO.

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

D. Following the meeting, the user must be sent a copy of the CIO's decision upon reconsideration, and must be notified that the user may appeal to the Chancellor if the user is dissatisfied with the outcome of the meeting.

IV. Authorization Requirements for Contract, Non-Agency Personal, Volunteer, Vendor, & Guest Accounts

A. A written request from the director or manager of the unit;

B. Such authorization will typically be limited to a maximum of 12 months but can be longer as requested by the sponsoring department and approved by the CIO;

C. Signed acceptance by a unit employee or the director/manager accepting responsibility for the actions of the contract, non-agency personnel, volunteers, vendors, or guests; AND

D. The contract, non-agency personnel, volunteers, vendors, or guest's acceptance of University policies and procedures related to accessing University computers, networks, and data.

V. Division or Department Specific Rules

A. Additional rules on computer and/or network use may be adopted by various divisions/departments to meet specific administrative or academic needs in compliance.

B. Any adopted requirements must:

1. comply with all applicable federal and State law;
2. be consistent with UNC and UNCSA policy;
3. be posted, either physically or electronically, in a manner that is available to all affected users; AND
4. be filed with the following:
    a. the Chief Academic Officer
    b. the Chief Operating Officer; AND
    c. the Chief Information Officer.

VI. Officials who may authorize broadcast messages

A. Chancellor;

B. Chief Academic Officer

C. Chief Operating Officer

D. Chief Advancement Officer

E. Director of Human Resources

F. Vice Chancellor of Student Life

G. Chief Information Officer, Chief of Police

H. Associate Vice Chancellor for Facilities Management

I. Film Screening Scheduler

J. Director of the Stevens Center

K. Marketing and Communications Director

L. their designees