RESPONSIBLE USE OF ELECTRONIC RESOURCES

07.100

Authority:	Board of Trustees
History:	Approved by Board of Trustees August 3, 2007; revised July 18, 2007; reformatted May 25, 2005; approved by Board of Trustees October 28, 2004; revised October 23, 2003; effective January 18, 2002; replaced policy ITS 1.00
Source of Authority:	Consolidated University of North Carolina Netstudy – Security Subcommittee Baseline Recommendations (Feb. 16, 2003); International Standard ISO17799
Related Links:	Administrative Provisions
Responsible Office:	Information Technology Systems Division

I. Introduction/Purpose

This document provides guidelines for the responsible and appropriate use of the university's electronic computing and communication resources and services. Requiring the responsible use of university electronic resources is necessary to:

A. Ensure business continuity capability (administrative as well as teaching and learning) in an effective and efficient manner without interruption of service.

B. Ensure proper stewardship of university resources and that resources are not utilized for personal gain.

C. Ensure optimum security and integrity of systems and data.

D. Ensure the protection of personal identity of faculty, staff and students.

E. Ensure that resources of the university are not utilized to cause harm to any entity or individual.

F. Ensure 100% legality in every aspect of the use of electronic resources at the university.

II. Scope/Coverage

This policy applies to every user of the university's electronic resources including faculty, staff, students and visitors. Electronic resources include but are not limited to microcomputers, servers, telecommunications equipment, AV and multimedia equipment, the campus network infrastructure, the campus gateway to the Internet whether accessed from a university or privately owned device, PDA's, etc.

III. Policy Statement

A. The electronic resources of the university are powerful tools, shared among all members of the campus community, designed to support the teaching, learning, instructional, research, administrative, service, and other activities of the university and are intended to be used in useful and productive ways. Individuals using these resources are expected to do so wisely and carefully, with respect and consideration of the rights, needs and privacy of others. Electronic resources and the data they support are used by and accessible to a large number of authorized users. However, since these are typically networked resources they are also subject to unauthorized intrusion, access and attack. It is essential, therefore, that all users understand and follow guidelines concerning authorized and responsible use. These guidelines are designed to preserve and protect users, their data and other assets, the university, and the electronic computing and communication systems themselves, and are set forth below.

B. The University of North Carolina Wilmington regards e-mail as an official method of communication with student, staff and faculty. Further, Outlook and OWA are viewed as the current official e-mail clients, and ITSD is charged with maintaining these clients and recommending future modifications or changes of clients to the Cabinet. The UNCW e-mail address is the official address for faculty, staff and student electronic communications. Faculty, staff and students assume full responsibility for the decision to forward e-mail and any failure to receive e-mail communications due to an alternative e-mail service does not necessarily constitute a defense for failure to respond. While e-mail is an official method of communication, it is not the only official method of communication and does not exclude alternate methods such as written or oral communications. All members of the university community must maintain good e-mail management habits and adhere to the standards of responsible use.

C. Electronic computing and communication technologies increase the risks of actions, deliberate or not, that are harmful in various ways, including:

1. interference with the rights of others;

2. violation of the law;

3. interference with the mission of the university; or

4. endangering the integrity of the university's computer and communication networks.

D. Users must act prudently and responsibly to both preserve the freedom to acquire and share information and to sustain the security and integrity of individuals within the community. Access to electronic resources at the university is a privilege, not a right, and must be treated as such by all users of these resources. Every user is responsible for the integrity of these information resources. All users must respect the rights of other computer users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements related to electronic resources.

E. Users must also understand the ramifications of illegal use, exchange, or display of

copyrighted, deceptive, defamatory, or obscene materials on a Web page or through other electronic communication channels. It is the policy of university to promptly process and investigate notices of alleged copyright infringement and take appropriate actions under the Digital Millennium Copyright Act, Title 17, United States Code, Section 512 ("DMCA").

F. All users shall act in accordance with this policy and all relevant university policies, rules and regulation, including adherence to all relevant local, state and federal laws and regulations.

G. Accepting any account and/or using university electronic resources shall constitute an agreement on behalf of the user or other individual accessing such information systems to abide and be bound by the provisions of this policy and the principles and guidelines contained herein.

IV. Enforcement

A. The university reserves the right to place restrictions on the use of its electronic resources in response to complaints that present evidence of violations of university policies, rules, regulations or codes, or local, state or federal laws and regulations. Actions that violate these policies can result in immediate disabling, suspension, and/or revocation of the account owner's privileges pending review for further action. Such unauthorized or illegitimate use of electronic resources including computer accounts, resources or facilities may constitute misconduct and accordingly violators are subject to appropriate disciplinary, criminal and/or legal action by the university and/or the State. If evidence is established, the university authorities responsible for overseeing these policies and codes will be consulted on the appropriateness of specific actions.

B. Individuals who have concerns about the conduct of a member of the university community or the propriety of a given situation or activity should notify their department chair, dean, director, or an administrator in their supervisory chain at a level sufficient to allow objectivity in evaluating the subject of concern. If action is deemed warranted by this official, the matter shall be referred to the appropriate vice chancellor or senior officer. Prior to taking action, the vice chancellor or senior officer responsible for the situation or activity at issue shall consult with the vice chancellor for ITSD, who shall, as appropriate, consult with the university's general counsel. The responsible official shall then respond to university community members who express concerns about such activities or incidents, and shall inform the chancellor regarding their response.

C. When concern about a given situation or activity involves an imminent threat to individuals, systems, or facilities, users should immediately communicate the concern directly to the Office of the Vice Chancellor Information Technology Systems and to University Police.

V. Review and Disclaimer

A. This is not a comprehensive document covering all aspects of responsible use. It is not possible to anticipate all the conditions and circumstances associated with the use of

these resources. The guidelines within this document and the specific policies they reference seek to link established codes of conduct for the use of electronic resources by members of the university community.

B. This is a dynamic document that is continuously reviewed by the Information Technology Systems Division and all other interested parties whose input is solicited and taken seriously. Modifications are reviewed (at a minimum) by the senior officers, the IT security officer, university counsel, and the Faculty Senate IT sub committee.

VI. Links to Related University Policies and Procedures

The university has instituted policies dealing with specific actions in a number of areas. These are listed below. As a matter of principle, users should act prudently and responsibly in the use of electronic resources, and are prohibited from engaging in activities including but not limited to those generally described in the following categories:

A. Harassing or threatening a specific individual(s), (see Harassment, Threats, Stalking, and Similar Threats);

B. Impeding, interfering with, impairing, or otherwise causing harm to the activities of others (see Interfering with the Rights and Activities of Others and E-mail Abuse);

C. Downloading, or posting to university computers, or transporting across university networks, material that is illegal, proprietary, in violation of other university policies and procedures, regulations or contractual agreements, or is otherwise damaging to the institution;

D. Illegal P2P or Peer-to-Peer file sharing. This includes illegal file sharing that takes place with or without a "sharing" agent or software;

E. Using university or campus logos, word marks, service marks, or other symbols of the university or campus on non-UNCW-hosted personal or professional home pages;

F. Creating pages which contain direct links to pages that violate this policy (in this case, users may be requested to deactivate links to materials that violate this policy);

G. Damaging, abusing, or in other ways destroying or interfering with the successful operation of electronic resources (see Abusing, Damaging, or Destroying Electronic Resources and Viruses and Hoaxes);

H. Accessing or attempting to access, use, or modify resources or data for which authorization has not been granted (see User Accounts and Authorized Access; Security; Confidentiality; and Privacy);

I. Engaging in activities that are illegal under federal, state, local and other applicable laws.

An outline of the administrative provisions follows:

1. ITS 07.100.01 - User Accounts and Authorized Access
2. ITS 07.100.02 - Security
3. ITS 07.100.03 - Confidentiality
4. ITS 07.100.04 – Privacy
5. ITS 07.100.05 – Employees' Incidental Personal Use of Electronic Resources
6. ITS 07.100.06 - Interfering with the Rights and Activities of Others
7. ITS 07.100.07 - Harassment, Threats, Stalking, and Similar Activities
8. ITS 07.100.08 - Abusing, Damaging, or Destroying Electronic Resources
9. ITS 07.100.09 - Email Abuse
10. ITS 07.100.10 - Viruses and Hoaxes
11. Addressing Concerns

Protection of copyrighted material has a direct correlation with responsible use of electronic resources. For additional information refer to http://www.northcarolina.edu/content.php/legal/copyright/index.htm

For additional information with regard to the Responsible Management of Information Technology Resources refer to http://www.uncw.edu/policies/07-200-respmngmtresources.htm