Proposed UNCW Policy Update
07.100.00
RESPONSIBLE USE OF INFORMATION TECHNOLOGY RESOURCES

Summary:

The 07.100.00 policy has been updated to reflect requirements of the new UNC System Office Policy Manual, chapter 1400 “Information Technology” requirement for reporting to the UNCW Board of Trustees. In addition updates to department names, titles, and definitions were made to make the policy current with university organization and IT terminology.

Key changes in addition to the above:

- Header - Source of Authority updated to be new UNC System Office polices
- Section II - Added definition of “Information technology resources” based on UNC System Office policies
- Section III - Moved section concerning email as an official method of communication to 07.100.09
- Section III - UNCW Board of Trustees charges CIO to maintain polices in accordance with UNC System Office Policy Manual
- Section III – CIO will provide regular updates to the Board of Trustees ARC Committee
- Section IV – Added paragraph for gender-based discrimination, harassment or sexual misconduct
- Removed redundant section “Links to Related University Policies and Procedures”
- All – updated department names and titles

Final version:
Attended

Redline version:
Attended
RESPONSIBLE USE OF INFORMATION TECHNOLOGY RESOURCES
07.100.00

Authority: Board of Trustees

History: Approved by the Board of Trustees July xx, 2018; Approved by the 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


Responsible Office: Information Technology Services

I. Introduction/Purpose

The 07.100 series of policies outlines responsibilities and the appropriate use of the university’s information technology resources and services. Requiring the responsible use of university information technology 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 ensure 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 students, faculty and staff.

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

F. Ensure legality in every aspect of the use of information technology resources at the university.

II. Scope

The 07.100 series of policies applies to every user of the university’s information technology resources including, but not limited to, students, faculty, staff, and visitors.

“Information technology resources” means information owned or possessed by the university, or related to business of the university, regardless of form or location, and the hardware and software resources used to electronically store, process or transmit that information owned, leased or used
by the university and its partners.

III. Policy

B. General Statement
The information technology resources of the university are powerful tools, shared among all members of the campus community and designed to support the teaching, learning, instructional, research, administrative, service and other activities of the university. They 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. Information technology 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 policies concerning authorized and responsible use. These policies are designed to preserve and protect users, data, other assets, the university, and the information technology resources and communication systems.

The UNCW Board of Trustees charges the UNCW CIO to maintain UNCW ITS policies in accordance with requirements set forth in the UNC System Office Policy Manual, chapter 1400 “Information Technology.”

The UNCW CIO will provide, on a regular basis at scheduled meetings, an IT Governance update to the UNCW Board of Trustees Audit, Risk & Compliance Committee.

C. 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 information technology 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 technology 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.

D. Users must also understand the ramifications of illegal use, exchange or display of copyrighted, deceptive, defamatory or obscene materials through electronic communication channels. It is the policy of the 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").

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

F. Accepting any account and/or using university information technology resources shall constitute an agreement on behalf of the individual accessing such information systems to abide and be bound by UNCW policies.

IV. Enforcement / Addressing Concerns
A. The university reserves the right to place restrictions on the use of its information technology resources in response to 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 information technology resources including computer accounts, resources or facilities may subject the violators 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 of concern shall consult with the CIO, who shall, as appropriate, consult with the university's general counsel.

C. When concern about a given situation or activity involves an imminent threat to individuals, systems or facilities, users are to immediately communicate the concern directly to the University Police.

D. Concerns involving gender-based discrimination, harassment or sexual misconduct must be reported in accordance with Policy 02.205 Unlawful Discrimination, Harassment, and Sexual Misconduct. Concerns involving minors must be reported immediately to the 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. This document and its policies seek to link established codes of conduct for the use of information technology resources by members of the university community.

B. This is a dynamic document that is continuously reviewed by Information Technology Services and the Information Technology Advisory Council.
VI. Introduction/Purpose

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

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

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

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

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

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

L. Ensure 100% legality in every aspect of the use of electronic information technology resources at the university.

VII. Scope/Coverage

This policy applies to every user of the university’s electronic information technology resources including students, faculty, staff, and visitors. Electronic information technology resources” means information owned or possessed by the university, or related to business of the university, regardless of form or location, and the hardware and software resources used to electronically store, process or transmit that information owned, leased or used by the university and its partners.
VIII. Policy

G. General Statement

The electronic information technology resources of the university are powerful tools, shared among all members of the campus community, and designed to support the teaching, learning, instructional, research, administrative, service; and other activities of the university and. They 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 information technology 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 policies concerning authorized and responsible use. These guidelines policies are designed to preserve and protect users, their data and, other assets, the university, and the electronic computing information technology resources and communication systems themselves, and are set forth below.

A. 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.

B. 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

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

The UNCW Board of Trustees charges the UNCW CIO to maintain UNCW ITS policies in accordance with requirements set forth in the UNC System Office Policy Manual, chapter 1400 “Information Technology.”

The UNCW CIO will provide, on a regular basis at scheduled meetings, an IT Governance update to the UNCW Board of Trustees Audit, Risk & Compliance Committee.
H. 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 information technology 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 technology 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.

C. 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 the 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").

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

K. Accepting any account and/or using university electronic information technology 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—UNCW policies.

VIII. IX. Enforcement / Addressing Concerns

D. The university reserves the right to place restrictions on the use of its electronic information technology 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 information technology resources including computer accounts, resources or facilities may constitute misconduct and accordingly subject the violators 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.

E. 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 of concern shall consult with the vice chancellor for ITSDCIO, 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.

F. 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.

D. Concerns involving gender-based discrimination, harassment or sexual misconduct must be reported in accordance with Policy 02.205 Unlawful Discrimination, Harassment, and Sexual Misconduct. Concerns involving minors must be reported immediately to the University Police.

IX.X. Review and Disclaimer

C. 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 information technology resources by members of the university community.

IX. 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

D. Technology Resources refer to http://www.unew.edu/policies/07-200-respmngmtresources.htm