UNCW

PRIVACY & CONFIDENTIALITY
07.100.04

Authority: CIO

History: Approved by the CIO August 1, 2019 (replaces former 07.100.03 and 07.100.04); 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

Source of Authority: UNC System Office Policy Manual, Chapter 1400 “Information Technology”
International Organization for Standardization ISO/IEC 27002

Related Links: Policy 07.100 Responsible Use of Information Technology Resources

Responsible Office: Information Technology Services

I. Purpose

The university cherishes the diversity of values and perspectives intrinsic to an academic institution and, thus, is respectful of freedom of expression. The university also encourages all members of its community to use information technology systems and networks in meaningful and useful ways, and in a manner that is respectful of the rights, needs and privacy of others. Users must respect the privacy of other users’ information, even when that information is not securely protected.

Users shall respect the university’s, as well as their own, obligations of privacy and confidentiality. Only those with specific authorization may access, communicate or use confidential information.

II. Policy

A. Federal and state laws govern the confidentiality of certain information maintained by the university. Any person who has been authorized to use and/or access information technology resources shall be expected to regard all personal, confidential or proprietary information which may thereby become available to him/her as confidential, unless he/she obtains from the owner or designated administrator specific written permission to view, copy, modify, or otherwise access or use any part of it. Users must respect the privacy of others and comply with the confidentiality laws. Except as set forth in university polices, information technology resources will not be used to abridge the privacy or confidentiality of other users’ information or similar assets.

B. Though Information Technology Services strives to secure information technology resources, users must be aware that no information technology system is completely secure. Therefore, they have no guarantee of complete privacy in the material generated, sent or received by them. Particularly with regard to communications like email, the Internet/Web and similar forms of communication, the university cannot ensure the privacy of files, data and messages. Those who use email, the Web and similar forms of communication and/or who make information about themselves available on the Internet are forewarned that the university cannot protect them from invasions of privacy and other possible dangers that could result from the individual’s distribution of personal information. Neither can the university protect individuals against the existence or receipt of materials that may be offensive or annoying to them.

C. Access by authorized university employees to electronic information stored on the university's information technology resources may be necessary to ensure the orderly administration and function of university information technology resources. The university requires authorized employees, who as a function of their jobs routinely have access to electronic information and other electronically stored data, to maintain the confidentiality of such information. While respecting users’ confidentiality and privacy, the university reserves the right, on a case-by-case basis and consistent with this policy, to examine any computer files and electronic information. While general review of content will not be undertaken, monitoring of material stored on or transmitted by electronic resources may occur when deemed necessary by the university for the reasons specified below:

1. To enforce or investigate apparent violations of federal, state, and local laws and regulations, and policies and regulations of the University of North Carolina.

2. To safeguard the security, integrity and operating performance of information technology resources and data either at the university or elsewhere.

3. To retrieve information in emergency circumstances where there is a threat to health, safety or university property.

4. To obtain information related to university business, a supervisor or other university official may have access for work-related purposes, providing the owner of the information is not available to produce the information and approval to access another’s system has been expressly approved in advance by a director, department chair or more senior official.

5. To accomplish the repair, maintenance or testing of information technology equipment in order to ensure adequate performance for university needs. University personnel are expressly prohibited from exceeding their authority of access or from making any use of individual user data for any purpose other than services performed by them.

6. To satisfy a response to a public records request, administrative, or judicial order or request for discovery in the course of litigation. Users must be aware that public records statutes are very broad in their application. Some records are protected from disclosure. However, most university records and logs contained in electronic form require disclosure if a public record request is made. Users must remember this when creating any electronic information, especially email.

7. To protect the university against damaging consequences.