I. Purpose

The university cherishes the diversity of values and perspectives endemic in an academic institution and so is respectful of freedom of expression. The university also encourages all members of its community to use electronic communications in meaningful and useful ways, and in a manner that is respectful of the rights, needs, and privacy of others. For example, users should respect the privacy of other users’ information, even when that information is not securely protected.

II. Procedure

A. The university may authorize confidential passwords or other secure entry identification to help ensure the integrity and privacy of data. Although a respect for privacy is fundamental to the university’s policies, users must understand that almost any information can in principle be read or copied. When University information systems and networks are functioning properly, a user can generally assume the files and data he or she generates to be private information, unless

1. The creator of the file or data takes action to reveal it to others, or

2. The university or its designated representatives must access that information for specific purposes as defined below.

B. Users should be aware that no information system is completely secure. Therefore, they have no guarantee of complete privacy in the material generated, sent or received by them over the university’s electronic resources. Persons both within and outside of the university may find ways to access files and messages. Accordingly, the university cannot and does not guarantee users’ complete privacy and users should be continuously
aware of this fact. Particularly with regard to communications like e-mail that traverse the Internet, the university cannot ensure privacy of files, data, and messages. It is impossible to ensure that no one other than the addressee will read e-mail messages. Those who use e-mail, the Web, and similar forms of communication and/or who make information about themselves available on the Internet should be 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. The university does not condone censorship, nor does it endorse the inspection of electronic files other than on an exceptional basis. However, access by authorized university employees to electronic information stored on the university's electronic resources may be necessary to ensure the orderly administration and function of university electronic resources. Such access ordinarily should not require the university’s gaining access to the content of the user’s electronic information. The university requires employees such as system administrators, 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 regulations and policies of the University of North Carolina.

2. To prevent the exchange, receipt, or transmission of proprietary software or copies of electronic information in disregard of copyright restrictions or contractual obligations. It is the policy of the University of North Carolina at Wilmington 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").

3. To safeguard the security, integrity, and operating performance of computers, networks, and data either at the university or elsewhere.

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

5. 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.
6. To accomplish the repair and maintenance of equipment. Users should be aware that on occasion duly authorized university information systems technological personnel have authority to access individual user files or data in the process of performing repair or maintenance of computing equipment the university deems is reasonably necessary, including the testing of systems in order to ensure adequate storage capacity and performance for university needs. Information systems technological personnel performing repair or maintenance of computing equipment are expressly prohibited from exceeding their authority of access for repair and maintenance purposes or from making any use of individual user files or data for any purpose other than repair or maintenance services performed by them.

7. To satisfy a response to a public records request, administrative or judicial order or request for discovery in the course of litigation. Users should 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 should remember this when creating any electronic information, especially e-mail.

8. To protect the university against damaging consequences.

D. Finally, the community of computer users at large has rights and expectations that must be considered. When individuals misrepresent either themselves or the university, or when they act by computer in a manner unacceptable within the university or in the larger community, the integrity and mission of the university itself is endangered.