University of North Carolina at Chapel Hill Policy on Privacy of Electronic Information

I. Introduction and Purpose of the Policy

This Policy clarifies the applicability of law and certain other University policies to electronic mail and the University's Policy on the privacy of electronic information. Users are reminded that all uses of the University's information technology resources, including electronic mail, are subject to all relevant University policies and relevant state and federal laws, including federal copyright law.

Appropriate use of University electronic resources includes instruction, research, service, and the official work of the offices, departments, recognized student and campus organizations, and other agencies of the University, and as described below, incidental personal usage by faculty, staff, and students. Since resources are not unlimited, the University may give priority for resources to certain uses or certain groups of users in support of its mission. Consistent with the University's non-discrimination policy, the use of information resources should not be denied or abridged because of race, creed, color, sex, sexual orientation, religion, national origin, age, or physical disability.

II. Privacy of Email Files

The University encourages the use of electronic mail and respects the privacy of users. It does not inspect or monitor electronic mail routinely, nor is the University responsible for its contents. Nonetheless, users of electronic mail systems should be aware that, in addition to being subject to authorized access as detailed below, electronic mail in its present form cannot be secured and is, therefore, vulnerable to unauthorized access and modification by third parties. Receivers of electronic mail documents should check with the purported sender if there is any doubt about the identity of the sender or the authenticity of the contents, as they would with print documents.

Users of electronic mail services also should be aware that even though the sender and recipient have discarded their copies of an electronic mail record, there may be back-up copies of such electronic mail that can be retrieved on University systems or any other electronic systems through which the mail has traveled.

University electronic mail services may, subject to the foregoing, be used for incidental personal purposes provided such use does not interfere with University operation of information technologies including electronic mail services, burden the University with incremental costs, or interfere with the user's employment or other obligations to the University.
Access by authorized University employees to electronic mail stored on the University's network of computers may be necessary to ensure the orderly administration and functioning of University computing systems. Such access, gained for purposes such as to back up or move data, ordinarily should not require the employee gaining access to the electronic mail to read messages. The University requires employees, such as system administrators, who as a function of their jobs routinely have access to electronic mail and other electronically stored data to maintain the confidentiality of such information.

Access to electronic mail on the University's network of computers that involves reading electronic mail may occur only where authorized by the University officials designated below and only for the following purposes:

a. troubleshooting hardware and software problems, such as rerouting or disposing of undeliverable mail, if deemed necessary by the Security Officer of Academic Technology and Networks (ATN) or his or her authorized designee;

b. preventing or investigating unauthorized access and system misuse, if deemed necessary by the Security Officer of ATN;

c. retrieving or reviewing for University purposes University-related information *

d. investigating reports of violation of University policy or local, state, or federal law *

e. investigating reports of employee misconduct*

f. complying with legal requests for information (such as subpoenas and public records requests) *; and
g. retrieving information in emergency circumstances where there is a threat to health, safety, or University property involved *.

* The system administrator will need approval from the Provost and the Vice Chancellor and General Counsel or their designee(s) approved by the Chancellor to access specific mail and data for these purposes. The extent of the access will be limited to what is reasonably necessary to acquire the information for a legitimate purpose.

In addition to the foregoing, when a University employee leaves employment or when a student graduates or otherwise withdraws from the University, a system administrator may, with approval of the unit head to which the employee was assigned or in which the student was enrolled, remove the departing employee’s or student's email files from University systems in order to conserve space or for other business purposes. An employee’s email may be retained and accessed by the unit as necessary for use in connection with University business. A student's email should be deleted unless otherwise required in connection with University business. In all such cases the extent of the access will be limited to what is reasonably necessary to acquire the information for a legitimate purpose. Units and departments are encouraged to make arrangements for disposition of email files with departing employees and students in advance of their departure.

III. Privacy of Data, other than Electronic Mail, Stored on University Computers and Networks

As is the case with electronic mail, access by authorized University employees to electronic data stored on the University's network of computers may be necessary to ensure the orderly administration and functioning of University computing systems. Such access may require the employee gaining access to the data to read specific files. The University requires system administrators and other employees who, as a function of their jobs, routinely have access to electronically stored data, to sign statements agreeing to maintain the
confidentiality of such information.

In order to conduct its business without interruption, the University must have access to data stored on University computers and networks. Accordingly, for legitimate business purposes, the head of any University administrative unit or department may in his or her discretion authorize the accessing or retrieval of any files other than electronic mail stored on University computers under that unit or department's control. Where necessary and appropriate, University network support personnel may assist with retrieval of such information on behalf of a unit or department, even if the information is stored at a site other than the unit or department's computer systems.

There is no guarantee of privacy or confidentiality for documents or data stored on University-owned equipment.

IV. Public Records Considerations

Electronic mail and other data stored on University computers may constitute a public record like other documents subject to disclosure under the North Carolina Public Records Act or other laws, or as a result of litigation. However, prior to such disclosure, the University evaluates all requests for information submitted by the public for compliance with the provisions of the Act or other applicable law.

Destruction of such records is governed by the Records Retention Policies of one's unit of employment. Information about such policies is available from one's supervisor. Incidental personal electronic mail may be destroyed at the user's discretion.

V. Conclusion

Wherever possible in a public setting, individuals’ privacy should be preserved. However, there is no guarantee of privacy or confidentiality for data stored or for messages stored or sent on University-owned equipment. Persons with questions about the applicability of this Policy to specific situations should contact the Office of University Counsel.

Violations of University policies governing the use of University electronic resources, including mail services, may result in restriction of access to University information technology resources in addition to any disciplinary action that may be applicable under other University policies, guidelines or implementing procedures, up to and including dismissal. Suspected violations of University Policy may be reported to postmaster@unc.edu.

This policy is maintained by the Office of the Vice Chancellor and University Counsel

February 27, 2002

All revision dates: 2/27/2002

Attachments: No Attachments