

FAYETTEVILLE STATE UNIVERSITY

ELECTRONIC MAIL

Authority:	Issued by the Chancellor. Changes or exceptions to administrative policies issued by the Chancellor may only be made by the Chancellor.
Category:	General University Policies
Applies to:	●Administrators ●Faculty ●Staff ●Students
History:	Revised – August 28, 2017 Approved - June 2, 2003 Issued - June 2, 2003
Related Policies/ Regulations/Statutes	● <i>Data Ownership</i> ● <i>Information Security</i> ● <i>Network Use Policy</i> ● <i>UNC General Records Retention and Disposition Schedule</i> ● <i>E-mail as a Public Record in North Carolina: A Policy for Its Retention and Disposition</i> [North Carolina Department of Cultural Resources] ● <i>Public Records</i> [N.C.G.S. 132-1 et seq.]
Contact for Info:	Vice Chancellor for Information Technology and Telecommunications (910) 672-1477 Office of Legal Affairs (910) 672-1145

I. PURPOSE

The purpose of this policy (Policy) is to ensure the appropriate use of Fayetteville State University's (University) electronic mail system. Electronic mail (e-mail) is a tool provided by the University to complement traditional methods of communication and to improve education and administrative efficiency. University students and employees have the responsibility to use this resource in an efficient, effective, ethical and lawful manner.

Use of the University's e-mail system evidences a student's or employee's agreement to be bound by this Policy. Violations of this Policy may result in restriction of access to the University's e-mail system and/or other appropriate disciplinary action.

II. OFFICIAL COMMUNICATION MEDIUM

The University must be able to communicate quickly and efficiently with employees and enrolled students in order to conduct official University business. A University assigned employee or student email account is the University's official means for such communications. The University expects recipients of who receive University emails to read and, if required, respond to such emails in a timely manner.

Employees are prohibited from auto-forwarding University emails from an @uncfsu.edu account. Automatic email forwarding is where all of a user's emails are automatically transferred to a non-University email address. Auto-forwarding all email to non-University email accounts prevents the University from complying with the requirements of the North Carolina Public Records Act. (see below).

III. EMAIL AS A PUBLIC RECORD

An e-mail message is considered to be a public record when made or received pursuant to law or ordinance in connection with the transaction of the University's business. North Carolina State law defines a public record as follows:

“Public record” or “public records” shall mean *all* documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data processing records, artifacts, or other documentary material, *regardless of physical form or characteristics* made or received pursuant to law or ordinance or in connection with the transaction of public business by any agency of North Carolina government or its subdivisions. [emphasis added]

It is an employee's responsibility to abide by the law and classify and manage e-mail messages in accordance with the *UNC General Records Retention and Disposition Schedule* or in accordance with directives issued by the University's Office of Legal Affairs.

IV. RETENTION OF E-MAIL (applicable to employees only)

Employees are responsible for saving or archiving e-mail messages that constitute University records. Those email messages are considered public records and cannot be disposed of, erased or destroyed except in accordance with the *UNC General Records Retention and Disposition Schedule* or directives issued by the Office of Legal Affairs.

E-mail that must be retained may be retained in electronic or paper form, but must be retained for as long as the period specified in the University's records schedule or as directed by the Office of Legal Affairs. If retained in paper form, the copies must retain transmission and receipt information.

V. PRIVACY OF E-MAIL MESSAGES

E-mail messages created, received, and/or used on computers or mobile/portable computing devices owned or operated by the University are considered University property and the University may access and monitor e-mail at any time for any reason without notice. Thus, no individual should use a University e-mail account with the expectation that any particular e-mail communication, whether personal or University-related, will be private. It is important to note that email may be electronically accessed and regenerated by the University even after the emails have been deleted by the user. Any action taken to access and monitor e-mails will be taken for reasons the University, within its discretion, deems to be legitimate. These legitimate reasons may include, but are not limited to, the following:

- Courts may order the production of University records, including e-mail records, in connection with litigation.

- Appropriate law enforcement and other officials may, consistent with law, have access to documents for purposes of investigating allegations of violations of law or of University policy.
- Appropriate officials may need access to emails for business purposes.
- Requests by the public in accordance with the [North Carolina's Public Records Act](#).

Access to the content of emails for reasons such as those described above must be authorized, in writing, by the Office of Legal Affairs.

VI. UNACCEPTABLE USES OF E-MAIL ACCOUNTS

Unacceptable usage of a University e-mail account may result in legal liability, lost productivity, negative publicity, and/or damage to an employee's or the University's reputation, and may result in disciplinary action, up to and including dismissal.. The following include, but are not limited to such unacceptable uses:

- Use for personal purposes that interferes with an employee's obligation to carry out the employee's University duties in a timely and effective manner.
- Private or personal for-profit activities and unauthorized not-for-profit business activities. This includes personal use of e-mail for marketing or commercial transactions, advertising of products or services or any other activity intended to foster personal gain.
- Use for political purposes, such as promoting political causes and/or advancing a political party or a candidate for political office.
- Use that violates or conflicts with any applicable policies of the University or the UNC Board of Governors.
- Use of or attempted use of the e-mail accounts of others without their permission.
- Submitting e-mail and network credentials by clicking on hyper-links sent through phishing. This violation will result in automatic registration for multi-factor authentication. (Multi-factor authentication requires multiple security information to get access to e-mail.)
- Use for, or in support of, unlawful/prohibited activities to include, but not be limited to the following:
 - Tampering with computer hardware or software;
 - Knowingly vandalizing or destroying computer files;
 - Transmitting material deemed to be illegal or harassing. Harassment is defined as behavior that is:
 - unwelcomed and severe or pervasive;
 - directed toward a particular person or persons;
 - based upon that person's race, color, religion, national origin, sex, gender, sexual orientation, gender-identity, creed, disability, veteran status, political affiliation, or student organization affiliation; and

- so objectively offensive that it unreasonably interferes with the target person's employment, academic pursuits, or participation in University-sponsored activities such that it effectively denies equal access to the University's resources and opportunities.
- Transmitting sexually harassing materials (as defined by the University's Sexual Harassment Policy) ;
- Attempting to penetrate a remote site/computer without proper authorization;
- Violating federal and State laws dealing with copyrighted materials or materials protected by a trade secret;
- Intentionally seeking information about, obtaining copies of, or modifying contents of files, other data, or passwords belonging to other users, unless explicitly authorized to do so by those users;
- Attempts to subvert network security, to impair functionality of the network, or to bypass restrictions set by network administrators;
- Deliberate interference or disruption of another user's work or system;
- Seeking/exchanging information, software, etc., that is not related to one's job duties and responsibilities; or
- Unauthorized distribution of University data and information. This includes proprietary information or any other privileged, confidential, or sensitive information.

VII. ENFORCEMENT AND VIOLATIONS

Any violation of this Policy may result in restriction of a user's access to the University's information technology resources, in addition to disciplinary action up to and including dismissal (employees) or expulsion (students).

VIII. USE OF PERSONAL EMAIL ACCOUNTS

The use of personal email accounts to conduct official University business is strongly discouraged. Even though a personal email account may be used, such emails are considered public records. If a personal e-mail account is used for University business, employees should forward all such e-mail messages to their University e-mail account and/or make such emails available upon request.

IX. BROADCAST E-MAIL

Broadcast email messages are those sent to a large segment of the University community, such as faculty, staff, students and alumni. Such emails relate to the University's mission, vision, values and strategic plan; emergency, urgent or time sensitive messages; and University news, events, and recognitions. Only the Office of Public Relations is authorized to send such messages. Any broadcast messages sent must conform to guidelines established by the Office of Public Relations.