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 – February 2, 2024 Revised – October 6, 2023 Revised – August 21, 2018 Revised – August 28, 2017 Approved - June 2, 2003 Issued - June 2, 2003
Related Policies/ Regulations/Statutes	●Information Security ●Acceptable Use of Information Resources ●UNC General Records Retention and Disposition Schedule ●Public Records [N.C.G.S. 132-1 et seq.] ●E-mail as a Public Record in North Carolina: A Policy for Its Retention and Disposition [North Carolina Department of Natural and Cultural Resources]
Contact for Info:	Vice Chancellor for Information Technology and Chief Information Officer | (910) 672-1200 Division of Legal, Audit, Risk and Compliance | (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 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. Automatic email forwarding is where all of a user's employee 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.

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 Division of Legal, Audit, Risk and Compliance.

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 Division of Legal, Audit, Risk and Compliance.

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 Division of Legal, Audit, Risk and Compliance. 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 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 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 Division of Legal, Audit, Risk and Compliance.

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 perform the employee's University duties in a timely and effective manner.

- Employee's use for 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.

- Employee's use for political purposes. Political activities include any action directed toward the success or failure of a candidate, political party, or partisan political group. This includes campaigning and/or taking an active part in managing a campaign.

- 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.

- 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.
    - Engaging in conduct prohibited by University policies.
    - 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 prohibited. 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 Strategic Communications is authorized to send such messages. Any broadcast messages sent must conform to guidelines established by the Office of Strategic Communications.