



EAST TENNESSEE STATE
UNIVERSITY

Email Use

Policy Name: Email Use

Policy Purpose

This policy specifies the guidelines and minimum requirements governing the acceptable use of email services provided by East Tennessee State University (ETSU or University). It outlines the responsibilities of users in maintaining secure and appropriate use of electronic communications.

Applicability

This policy is applicable to ETSU students and employees.

Responsible Official, Office, and Interpretation

The Chief Information Officer (CIO) is responsible for the review and revision of this policy. For questions about this policy, please contact Information Technology Services. The CIO has the final authority to interpret this policy.

Defined Terms

A defined term has a specific meaning within the context of this policy.

Authentication

The process of verifying the identity of a user or entity in a computer system, ensuring that only authorized individuals can access certain resources, systems, or data.

Authorized User

An individual who has been granted permission to access a specific system, resource, or data based on their role, responsibilities, or need to know.

Biometric Authentication:

A cybersecurity process that verifies a user's identity based on unique biological characteristics such as fingerprints, voices, retinas, or facial features.

Email Address

Policy Name: Email Use

A unique identifier for an email account that allows a user to send and receive electronic messages (emails). The Email Address is made up of the Username and the domain name (@etsu.edu), separated by the “@” symbol.

ETSU Account

An account is a personalized identity that allows a user to access specific services, systems, and resources at ETSU. The ETSU Account includes cybersecurity permissions to secure the account and maintain proper access control.

Mailbox

A storage location on a mail server where a user’s emails are held and managed. The Mailbox comprises folders such as the inbox, sent items, and other custom items and is accessed through an email application or webmail interface.

Multi-factor Authentication

A cybersecurity process that requires users to provide two or more verification factors, such as passwords, PINs, or security questions, to gain access to secure resources and systems

Strong Passcode

A secure and complex code that includes a variety of characters, such as numbers, special symbols, uppercase and lowercase letters, used to reduce the risk of unauthorized access to accounts and devices

Username

A unique identifier assigned to an individual or entity to gain access to a computer system, network, service, or application.

Policy Name: Email Use

Policy

1. Email Account Eligibility

1.1. Employee Account Eligibility.

All ETSU Authorized Users are assigned an ETSU Account that is associated with a user's access to email and other University services. The ETSU Account is associated with a unique Username, which helps identify each user. The Username is used to establish the Email Address for students and employees.

Employee account and email access begins with an employee's contract start date as assigned by the Office of Human Resources. Employees who are awarded emeritus status are permitted continued access to University email services after their employment ends. Access to ETSU email accounts for all other employee classifications, including retired employees, is terminated upon the expiration of their employment contract as determined by the Office of Human Resources.

Email services are provided while an employee is employed by the University until their last contracted day worked. Once an employee's email account is terminated, they may no longer access the contents of their Mailbox, nor should they export their Mailbox to a personal account before departure. The employee's department may elect to retain access to an employee's email account and Mailbox up to six months after the employee's departure. Employees who change departments may be assigned a new Username upon request from the original department. Additionally, employees enrolled in courses as a student may be assigned a new Username when changing departments or upon departure from the University.

1.2. Student Account Eligibility.

Students receive access to email and other University services upon application to the University. ETSU email services will remain active while the student is actively enrolled at the University. Student email access is removed for those not actively enrolled in a course for one year

1.3. Other Account Eligibility.

Individuals or entities with special relationships and a legitimate business purpose at ETSU, who are neither directly employed nor enrolled as students, may be granted limited email privileges, including an ETSU Email Address. These accounts are subject to the same restrictions and requirements as employee accounts and access may be revoked at any time. An ETSU employee must request

Policy Name: Email Use

these special accounts and is responsible for any activity that occurs from their use. Periodic renewal is required, and the account must have continuous ownership by an ETSU employee. Student organization requests must originate from the organization advisor.

1.3.1. Sponsored Accounts

Sponsored accounts include, but are not limited to, associated agencies, vendor and service accounts, guests of the University, and the Medical Education Assistance Corporation (MEAC). Sponsored accounts must be approved by the appropriate department head. Account sponsors are required to renew the accounts annually and may be assessed a fee for email or other services.

1.3.2. Departmental Accounts

ETSU departments and organizations requiring an ETSU email account with access to full email services may purchase a Departmental Account. Departmental Accounts are assessed an annual fee equivalent to the purchase price of the Microsoft license. In addition to email services, Departmental Accounts may have access to login to other University services including the ETSU network.

1.3.3. Shared Mailboxes

A Shared Mailbox is linked to a departmental Email Address, allowing multiple individuals to send and receive emails or schedule meetings through a shared calendar. There is no fee associated with Shared Mailboxes as they function as an option within an existing Mailbox.

2. Official ETSU Username and Email.

2.1. Student and Employee Email Accounts.

To ensure secure and effective communication, streamline administrative processes, and maintain a professional environment, all employees are required to use their assigned Email Address as the primary and official means of electronic communication within the organization. Students must use their assigned Email Address when communicating with University offices, faculty, and for other official University communications. Students and employees may request a Username change if they have had a legal name change, if the Username was created with incorrect information, or the generated Username results in an inappropriate word.

2.2. Other Email Accounts.

Policy Name: Email Use

Departments and organizations using Departmental Accounts or Shared Mailboxes may request a Username that represents their department name or acronym. Usernames will be assigned on a first-come, first-served basis. Usernames containing inappropriate or misleading language will not be approved.

3. Email Use.

3.1. Acceptable Use – All Email Accounts.

The use of ETSU email services is exclusively for University-related activities and communication. This privilege entails specific responsibilities for users, subject to University policies and local, state, and federal regulations. All usage must adhere to legal and ethical standards, demonstrate honesty, and exhibit restraint in utilizing shared resources.

Acceptable use of University email services includes communications and activities that conform to the purpose, goals, and mission of the University. Employees should utilize email services for the appropriate execution of their job duties and responsibilities.

3.1.1. Acceptable use of University email services includes, but is not limited to:

- 3.1.1.1. Communications between students, faculty, and staff, that comply with the above guidelines;
- 3.1.1.2. Communications related to teaching and learning, job duties, projects, tasks, and collaborations;
- 3.1.1.3. Engaging in activities that involve research and information gathering to support activities related to the user's educational pursuits and responsibilities at the University;
- 3.1.1.4. Correspondence with vendors, external partners, and collaborators for University-related purposes;
- 3.1.1.5. Fundraising activities carried out on behalf and for the benefit of the University;
- 3.1.1.6. Communication and information exchange relating directly to the mission, charter, and work tasks of the University, including email in direct support of work and course-related functions, or collaborative projects.

3.2. Unacceptable Use – Employee Email Accounts.

Policy Name: Email Use

University employee email services should be reserved for official communication related to work responsibilities. Usage may be monitored. Violations may result in disciplinary action as outlined in the [ETSU Acceptable Use of Information Technology Resources Policy](#).

3.2.1. Unacceptable use includes, but is not limited to:

- 3.2.1.1. Deceptive or fraudulent communication, including phishing attempts designed to extract personal, financial, or confidential information from recipients or misrepresentation of themselves or the University;
- 3.2.1.2. Transmitting content that is offensive, discriminatory, profane, defamatory, harassing, unlawful, or otherwise deemed inappropriate;
- 3.2.1.3. Sending emails with viruses, malware, or harmful attachments;
- 3.2.1.4. Political campaigning or fundraising, including sending messages in support of or against any particular candidate or party;
- 3.2.1.5. Commercial activities for employee personal financial benefit not authorized by the University;
- 3.2.1.6. Non-incident personal use outside the scope of the employee's job duties and responsibilities.
- 3.2.1.7. Forwarding an employee Mailbox to a non-ETSU address, Mailbox, or email service.

3.3. Unacceptable Use – Student Accounts.

Student email services remain the property of the University and should be used in accordance with University policies and all local, state, and federal laws. Violations may result in disciplinary action as outlined in the [ETSU Acceptable Use of Information Technology Resources Policy](#).

3.3.1. Unacceptable use includes, but is not limited to:

- 3.3.1.1. Deceptive or fraudulent communication, including phishing attempts designed to extract personal, financial, or confidential information from recipients or misrepresentation of themselves or the University;
- 3.3.1.2. Transmitting content that is offensive, discriminatory, profane, defamatory, harassing, unlawful, or otherwise deemed inappropriate;

Policy Name: Email Use

3.3.1.3. Sending emails with viruses, malware, or harmful attachments.

4. Privacy and Email.

As with other written communication, any email sent or received from an authorized ETSU email may be considered a public record under the Tennessee Public Records Act and may be subject to public disclosure. Emails are subject to subpoena and specific account activity may be monitored through request from University approved officials. ETSU email is the property of ETSU and may be searched or placed under a litigation hold without prior knowledge or notification to the account holder.

While the University maintains the security of email communications systems, privacy is not guaranteed, and users should have no expectation of privacy when sending and receiving emails through University email services. The content of ETSU email is not routinely monitored on an individual level, but the University deploys a variety of software applications to ensure the security of all ETSU email and data, and individual email may be accessed to maintain the safety and security of University resources.

5. Email Records.

An email may be considered a University record if it conveys approval or denial of a decision, contains evidence of receipt or expenditure of funds, documents the official position of the University, or provides evidence of an official University transaction. Employees must preserve email content that constitutes a University record in line with similar records.

6. Email Security.

The University employs a combination of external tools and internal controls to ensure the protection of sensitive information, prevent unauthorized access, and uphold the integrity of electronic communication channels. To enhance security measures, access to all University employee and student email requires the use of Multi-factor Authentication. If University email services are enabled on a personal device, a Strong Passcode or Biometric Authentication will be enforced on the device. These requirements aim to provide an additional layer of security, significantly reducing the risk of unauthorized access and enhancing the overall safeguarding of sensitive data within the University's digital environment.

Policy Name: Email Use

The University will make reasonable efforts to maintain the integrity and effective operation of its email systems, but users are advised that those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Users who intend to communicate sensitive or confidential information should follow established encryption email guidelines. All email messages dealing with personal identifiable information (PII), or protected health information (PHI) must be encrypted.

If an individual's ETSU email is identified as compromised or involved in a phishing campaign, preemptive mitigation measures will be enacted based on the severity of the security breach. The prompt execution of these mitigation measures ensures the protection of University data and systems by effectively halting or preventing the spread of malicious email activity. Impacted users may experience temporary suspension of access to ETSU email or other services. Users who experience a loss of account access are directed to promptly contact the Information Technology Services Help Desk to address any issues and restore access to University email services.

Procedures

N/A

Applicable Forms and Websites

[Departmental Account Request Form](#)

[Shared Mailbox Request Form](#)

[Sponsored Account Request Form](#)

[Username Change Request Form](#)

Previous Policy:

Electronic Mail Privacy

Authority and Revisions

Policy Name: Email Use

The ETSU Board of Trustees is charged with policy making pursuant to TCA § 49-8-203, et seq. On March 24, 2017, the Board delegated its authority to ETSU's President to establish certain policies and procedures for educational program and other operations of the University, including this policy. The delegation of authority and required process for revision to this policy can be found on the [Policy Development and Rule Making Policy webpage](#).

To suggest a revision to this policy, please contact the responsible official indicated in this policy. Before a substantive change to the policy section may take effect, the requested changes must be: (1) approved by the responsible office; (2) reviewed by the Office of University Counsel for legal sufficiency; (3) posted for public comment; (4) approved by either Academic Council or University Council; and (5) approved by ETSU's President.