

TEMPLE UNIVERSITY

POLICIES AND PROCEDURES

Title:	Email Policy
Policy Number:	04.74.11
Issuing Authority:	Office of the President
Responsible Officer:	Vice President for Information Technology
Date Created:	December 10, 2002
Date Last Amended/Reviewed:	March 5, 2026
Date Scheduled for Review:	March 2030
Reviewing Offices:	Information Technology Services

I. Scope of Policy & Rationale

This policy recognizes email as the official and effective method of communication at Temple University. It applies to all individuals with a university-provided email account, including students, alumni, faculty, staff, and affiliated contractors ("University users") and guests.

The policy covers all university-owned, managed, email, communications, and collaboration platforms including on-campus servers and cloud-based services and applies to email communications sent, received, or stored using these systems, regardless of device or location.

II. Policy Statement

1. Any use of email using an @temple.edu address, or using university technology resources to send or receive email must be done in accordance with Temple's Technology and Software Usage Policy ([04.71.11](#)), Data Usage, Governance, and Integrity Policy ([04.71.10](#)) and Accessibility of Information and Technology ([04.71.13](#)).
2. Because Temple recognizes email is an official means of communication, Temple has the right to send official communications to any University user via email and has the right to expect that those communications will be received and read in a timely fashion.
3. All University users eligible for email accounts are assigned an @temple.edu email address upon entry into the University, which is designated as the official address for all University communications and is listed in university directories and other applicable records.
4. Users may create a limited number of additional email addresses through email aliases; however, Information Technology Services reserves the right to remove any

alias that is offensive, misleading, misrepresents the user, or represents a commercial entity. All mailboxes are subject to a maximum storage limit to ensure reliable system performance. Email access may be temporarily suspended at any time due to misuse. Email access is revoked at the time of separation from the university.

5. All faculty, staff, and students must use one of the following email address domains; temple.edu, @tuhs.temple.edu, @tuj.temple.edu, @fccc.edu, or @wrti.org, when communicating about university business (administrative, academic or research related). This also applies to communications with students. Authorized subdomains in the format@subdomain.temple.edu must be used exclusively for:
 - a. Bulk email communications and mass notifications must be distributed through university-approved ListServes or third-party bulk email services. Departments or individuals may establish mailing or distribution lists using an @temple.edu address, provided the list complies with applicable university requirements and allows recipients to opt out or unsubscribe.
 - b. The University will maintain an official mailing list using @temple.edu addresses for official, legal, and emergency University communications. Use of the official mailing list requires approval from the President, cognizant vice president/dean, or Vice President for Information Technology and may not be used for solicitations or other non-official communications.
 - c. Communications from university-approved third-party Software as a Service (SaaS) platform must use a subdomain and not the root @temple.edu domain Automated system-generated messages.
 - d. All subdomain usage must be approved by Information Technology Services in consultation with the Chief Information Security Officer. A list of approved platforms and authorized subdomains and their associated platforms will be maintained by Information Technology Services.
6. Personal email accounts (e.g., Gmail, Yahoo, Outlook.com) may not be used for official university business, even when using email forwarding or aliases that appear to originate from Temple domains.
7. The university will throttle (limit the rate or volume of messages sent) the number messages that can be sent directly from a user's mailbox internally and externally. Bulk email must be drafted and sent through an approved bulk sender.
8. Users will not attempt to impersonate their @temple.edu email account via any external third-party systems not associated with the University.
9. Users will not store confidential university data in their @temple.edu email account or utilize it as a system of record for business processes. An appropriate information management system should be acquired to satisfy this need

10. The university is not responsible for email retention or email recovery of @temple.edu email accounts. All data, including email, associated with @temple.edu accounts will be purged in accordance with the Information Technology Service security requirements and other applicable policies and procedures. The University strongly encourages all University users to use a non-@temple.edu email address for personal matters and non-University business and to maintain their own backups of any important personal email. Temple University is not responsible for retrieving or restoring personal data during or after an individual's separation from the University.
11. All mailbox contents of the @temple.edu email account are property of the university and as such may be discoverable to the Courts upon legal notice.
12. The university, in its discretion, may engage the services of a third-party vendor or vendors to provide email services. In addition to applicable university policies, all University users will be required to agree to and be bound by the vendor(s) terms of use.
13. The University is not responsible for supporting email retention or recovery from third-party email applications or clients that are not university-approved.
14. Eligibility to retain an @temple.edu email address upon graduation or separation from the University is governed by the University Alumni Email Program. For eligibility requirements and program details, refer to the University Alumni Association.
15. Staff and faculty are not eligible to retain an @temple.edu email address after separation from the university. Faculty granted an Emeritus faculty appointment will retain access to email (Temple Faculty Handbook).
16. Student/Alumni who have email electronically forwarded from the @temple.edu account to another email account do so at their own risk. Temple University is not responsible for the handling of @temple.edu mail sent or forwarded to outside service providers. Having email redirected does not absolve the Student/Alumni from the responsibilities associated with communications sent to his or her email address.
17. University users are expected to check their email accounts frequently to stay current with Temple University communications. Some communications may be critical, so it is imperative that individuals check their accounts regularly.
18. University users must not transmit confidential or sensitive data via email unless University-approved encryption or secure email methods are used. Unencrypted email is not a private or secure communication mechanism due to the open nature of the internet and the ease with which messages and attachments may be accessed, copied, forwarded, or distributed without authorization per the Data Usage, Governance, and Integrity Policy (04.71.10) An @temple.edu email address may be used by departments for setting up a shared departmental mailbox.

19. Vendor-provided email services must be reviewed and approved in accordance with the Technology and Software Usage Policy (04.71.11), Data Usage, Governance, and Integrity Policy (04.71.10) and Accessibility of Information and Technology (04.71.13).
20. Targeted electronic mailings to entire student and/or employee populations are restricted to official/authorized university business announcements. These targeted electronic mailings must be authorized by president, provost, or vice-presidential level.
21. Information Technology Services will not send out announcements regarding individual department offerings, such as events or symposiums, new course offerings, etc.
22. Third-Party Email Integration and Security Requirements:
 - A. All third-party email service providers sending email on behalf of the university or using university domains or subdomains must implement and maintain compliance with Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocols, including:
 - DomainKeys Identified Mail (DKIM) signature authentication,
 - Sender Policy Framework (SPF) records,
 - DMARC policy enforcement at a level of "quarantine" or "reject",
 - SSO must utilize Security Assertion Markup Language (SAML) or another university-approved authentication protocol.
 - B. Ongoing Compliance and Auditing: Information Technology Services will conduct periodic audits of third-party email providers to ensure ongoing compliance with email integration and security requirements. Vendors must provide access to authentication logs and DMARC reports upon request.

III. Email Retention

1. Email (excluding Deleted Items and Trash) is retained in the University user's email box for as long as (a) the user remains in good standing and the account remains open and (b) the user does not delete the email.
2. When a university user deletes an email the default process is that the deleted email goes to the "Deleted Items" or "Trash" folder depending on their email service or client. Additionally, email can be moved or filtered to a Spam or Junk Mail folder. Email is held for thirty days in these folders from the time of the deletion or until the user manually empties the folder. After 30 days email in the Deleted, Trash, Spam and/or Junk Mail Folders are removed from the folder and permanently deleted.
3. Email recovery for university matters will only be undertaken after approval from the cognizant vice president/dean and Chief Information Security Officer and subject to

reimbursement of costs by the department or requesting party. The university cannot recover email on unauthorized third-party hosted email systems.

4. No university Email that is offloaded to a non-TUmail email client and removed from the official email service is not retained. It is up to the individual user to back up and store any email removed from the official email service.
5. When an individual leaves the University the AccessNet account and services will be deleted following the schedule outlined in the [System Access by Enterprise University Role and the Security Requirements Guidelines](#).
6. Request for access to another person's email account must adhere to privacy guidelines and can only be done with the approval of the cognizant vice president/dean, Chief Information Security Officer, and Vice President for Information Technology, in consultation with the Office of University Counsel.
7. When litigation is pending or threatened against the University or its employees, the law or legal process may impose a duty upon the university to preserve all relevant documents and records, including email. A litigation hold directive can only be issued by the Office of University Counsel.

IV. Incident Reporting

1. Violations of this policy may result in disciplinary action in accordance with university policies and procedures. Disciplinary action may include, but is not limited to, verbal or written warnings, mandatory training, restriction or removal of system access, suspension, or termination of employment or affiliation.
2. Any incident of suspected hacking or intrusion attempts, compromised system, suspicion of password compromise, on-line harassment, or known violation of this policy will be addressed pursuant to the instructions of the incident response team maintained by the Vice President for Information Technology (ciso@temple.edu).

History:

1. Last Amended:

This policy was substantially revised to reflect current University communication and collaboration practices, including expanded coverage of cloud-based and integrated platforms, updated account lifecycle requirements, and strengthened cybersecurity and third-party email security requirements. The revision also aligns the policy with related University policies and guidance, including accessibility and faculty responsibilities on March 5, 2026.

This policy supersedes and replaces the Student Electronic Information (e-Mail) policy (04.74.11) Adopted by the Vice President for Computer & Information Services on

December 10, 2002, and updated and amended October 30, 2008,
and August 16, 2021.

This policy supersedes Email Retention Procedures adopted by the Chief
Information Security Officer on January 9, 2013.

November 2022: Updated to reflect current Bylaws and job titles.

2. Cross References:

Technology and Software Usage Policy, ([04.71.11](#))

Data Usage, Governance, and Integrity Policy, ([04.71.10](#))

Accessibility of Information and Technology Policy, ([04.71.13](#))

Temple Faculty Handbook ([02.78.02](#))