Electronic Communications Policy

Document Number: ITS-0002 **Date Published(sys):** 7/26/2022

General Description

Policy Summary:

Purpose:

This policy establishes the University mandates and requirements for the responsible and respectful use of electronic messaging systems and communication services, and to clearly set forth the rights and responsibilities of the University's authorized users related with these services, and for users to be aware of what they can expect regarding the privacy of using the University's electronic communication services.
Additionally, compliance with the stated policy and supporting procedures helps ensure the confidentiality, integrity, and availability (CIA) of University's system components.

Scope:

The Electronic Messaging and Communications Policy applies to anyone using the University's computer systems, networks, and data systems. This includes faculty and staff members, students, alumni, contractors, guests, and other members of the University community.
This policy encompasses all electronic communications and associated attachments transmitted or received over the University network, and any associated resources owned or managed by the University.

Exceptions:

In a few instances, Trinity systems may require to be exempted from the Electronic Messaging and Communications Policy due to possible technical difficulties or third-party contractual obligations. Any such exceptions to the current policy must be documented and approved via Trinity's Exceptions Management Process.

Policy Content

Roles & Responsibilities

Implementing and adhering to organizational policies and procedures is a collaborative effort, requiring a true commitment from all personnel, including management, internal employees, and users of system components, along with vendors, contractors, and other relevant third parties. Additionally, by being aware of one's roles and responsibilities as it pertains to the University information systems, all relevant parties are helping promote the Confidentiality, Integrity, and Availability (CIA) principles for information security in today's world of growing cybersecurity challenges.

- Management Commitment: Responsibilities include providing overall direction, guidance, leadership, and support for the entire information systems environment, while also assisting other applicable personnel in their day-to-day operations. The CIO is to report to other members of senior management on a regular basis regarding all aspects of the organization's information systems posture.
- Internal Employees and Users: Responsibilities include adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any University system components. Additionally, users are to report instances of non-compliance to senior authorities, specifically those by other users. Users – while undertaking day-to-day operations – may also notice issues that could impede the safety and security of the University system components and are to also report such instances immediately to senior authorities.
- Vendors, Contractors, other Workforce: Responsibilities for such individuals and organizations are much like those stated for users: adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any such system components.

Policy

The University ensures that all applicable users adhere to the following policies for purposes of complying with the mandated organizational security requirements set forth and approved by management.

1. University-owned or operated electronic communication facilities are intended and must be used solely for the academic and administrative objectives of the University
2. Trinity acknowledges that users occasionally use e-mail and the Internet for personal purposes. However, personal use is prohibited if it entails a direct cost to the University or interferes with the employee's performance of job duties. Trinity's systems and services provided to users are property of Trinity and cannot be considered personal or private.
3. Users may not expect complete privacy of the information transmitted using these services.

4. Trinity reserves the right to monitor and/or log all activities of all users using Trinity's systems without notice. This includes, but is not limited to, files, data, programs, and electronic communications records without the consent of the holder of such records.

Email Privacy and Confidentiality

Trinity University respects the privacy and confidentiality of the electronic messages sent or received by its community in accordance with relevant laws, regulations, and University policies. While Trinity permits limited personal use of the email infrastructure, those availing themselves of such privilege are subject to the same rules, regulations, laws, and policies as University business email. All users of electronic communications must understand the expectation of privacy and confidentiality related to them. Insecure communication services must not be used for confidential communication or the transmission of sensitive data. See the University's *ITS-0013 Information Security Policy* for additional information.

The University community should also be aware of the following issues regarding electronic communications:

- Faculty, staff and students must use or distribute a work-related email or other electronically stored information only as is appropriate in the performance of the employee's work responsibilities.
- Tmail should not be used for commercial or political purposes.
- Tmail should not be used for fundraising activities not endorsed by the University.
- All Tmail users are expected to read all official University messages sent to their University email address and will be presumed to have done so in a timely manner. The Trinity email system is an official means of communication. The University views communication via email to constitute being duly informed for faculty, staff, and students.
- The University email system is a delivery system for communication and does not constitute a long-term storage system for documents delivered by email. Therefore, the email system ought not to be relied upon for the long-term retention of official records of the University. The University provides storage systems outside of the email system for long-term retention such as the network storage drive.
- Users of the Tmail system do not have a right of privacy in communications transmitted or stored on University information technology resources. Thus, the @trinity.edu email address should not be used to send or receive personal email that a Trinity employee wants to keep private.
- Emails are written records that could be subject to review with just cause. Email records and information in electronic form on central computers can be subpoenaed. Messages that the user has deleted may still exist on the system's backup media for weeks or months.
- Certain types of email and uses of email or other forms of electronic communications are prohibited; these include chain letters, obscene messages, harassing messages, and

unsolicited political messages. Also emails that infringe copyrights or violate other intellectual property rights and laws. Email that violates any University policy or is otherwise used for an illegal purpose is prohibited.
- Mass communication is prohibited using TU's email system, unless otherwise authorized by one of the TU's Vice Presidents.

Voice Use

The use of the University voicemail system should be used appropriately, efficiently in an ethical and lawful manner, consistent with University policies. Guidelines surrounding use of voicemail follow general rules of common sense and common courtesy, and include the following:

- Respect the privacy of others.
- University voicemail systems may not be used to defame, harass, intimidate, or threaten any other person(s), or to send unnecessarily repetitive messages.
- University voicemail may not be used to publish, post, transmit, or otherwise make available content that is copyrighted, obscene, or legally objectionable.
- Voicemail passwords and access to mailboxes should not be shared. Each individual is responsible for their own account.
- Do not forge or otherwise misrepresent your personal identity. This policy does not prohibit users from engaging in anonymous communications, providing that such communications do not otherwise violate one of the above stated policies.

Accessing Email

Trinity has the right and ability to access individual email accounts, despite the fact that a user has established personal login credentials. However, Trinity and its agents or custodians of the email system will not access or disclose the content of an individual's Tmail account unless the University has a good faith belief that the terms of acceptable use have been violated. In addition to a good faith belief of a violation, permission must be secured from the appropriate member of leadership designated for each constituency. They are as follows:

- **Faculty Authorized Leader**: Vice President for Academic Affairs
    - backup: Associate VP of Faculty Recruitment & Development *
- **Students Authorized Leader**: Vice President for Student Life
    - backup: Associate VP for Student Affairs & Dean of Students *
- **Staff (+ all others) Authorized Leader**: Vice President for Finance & Administration
    - backup: Chief Human Resources Officer *

* In situations where the authorizer's person listed above are unable to perform this duty in the manner or time frame needed, an officer of the University will be granted decision authority. Although not a complete list, the following conditions represent potential situations for access:

- Suspected violation of the law, regulation, or University policy.

- Enforceable governmental request, a subpoena, or legal request to which the University is required to respond.
- Suspected criminal conduct or to protect against harm to the rights, property, or safety of the University, its employees, or the public.
- When information is necessary to conduct University business and the user of the account is unavailable.
- When information is necessary to conduct University business and the user is no longer employed by the University.
- A health or safety emergency.

Although not a complete list, the following conditions represent unacceptable access to an individual's email account:

- Curiosity
- Permission from authorized leader is not requested or is not given

Access to Trinity Email – Employees

1. If a user is on leave from work, for any reason, a manager may be given access to that individual's account for business continuity purposes. Whenever possible, arrangements should be made before a leave if the need for access is foreseeable. Managers will need to demonstrate to the appropriate authorizer because access to a user's account is warranted and to the extent possible, access will be tailored to the need. Additionally, managers may request and be granted access to an individual's email account upon termination of employment for business continuity purposes. In these instances, the manager will typically be granted access for a period no greater than one month after an employee's last day of work. Exceptions may be made on a case-by-case basis with a compelling rationale. Upon the conclusion of this period, the account and its contents will be terminated.
2. University faculty designated "professor emeritus" will be provided a Trinity email account for life unless that account is found to be in violation of the University policies or if dormant and unused for more than one year.
3. Those who resign or are terminated will no longer have access to their Trinity email account effective on the date of resignation or termination.

Access to Trinity Email - Students

1. TUNetwork and Tmail accounts are provided for all students currently enrolled in at least one class in a Trinity undergraduate or graduate program and are not provided for life. Trinity student accounts will remain active for one year after graduation. An account will be marked as eligible for deletion when:

1. An undergraduate or graduate student has not registered for a class for one (1) year, which is defined as two consecutive semesters.
2. One (1) year after the student has graduated from the university and is not enrolled in graduate school.
3. The student has requested their account be deleted, provided they are no longer affiliated with the University.

2. An account holder must adhere to the responsibilities and policies dictated in University's *ITS-0001 Acceptable Use Policy* and the *ITS-0003 Electronic Messaging and Communications Policy* during a temporary leave of absence or one year period following graduation.
3. This process describes this interruption and the steps toward permanently closing TUNetwork and Tmail accounts:
    1. TUNetwork and Tmail account will be deleted one year after graduation. When an account has been marked for deletion, the student will receive an email notification to their Tmail account at least two weeks prior to deletion. When the account is deleted, the student will lose all access to any service which requires a Trinity username and password (i.e., Tmail, TigerPaws, Tiger's Lair, TLEARN, library systems, use of the computer labs), and all files, websites, emails, and contacts stored on the Trinity servers will be permanently deleted.
    2. It is the account owner's responsibility to manage his/her account responsibly, and to retain any required files on backup media.
    3. In the case of a student who becomes an employee, their account will be migrated to the respective department. As the account will be moved and not deleted, all personal files, emails, and contacts will be retained in the account.
    4. Accounts for those students who have officially withdrawn from the University will be deleted once the withdrawal process has been completed.

Policy Violation

Enforcement

To ensure adherence to the Electronic Messaging and Communications Policy and to protect the integrity of University resources, the University reserves the right as described above to monitor the electronic communications across their systems to protect the security of the University's information, network, computing resources, and its users.

Any behavior in violation of this policy is cause for disciplinary action. Violations will be adjudicated, as appropriate, by the CIO, the Office of the Dean of Students, the Office of Housing and Residential Life, and/or the Office of Human Resources. Disciplinary action and/or sanctions as a result of violations of this policy may result in, but are not limited to, any or all of the following:

- Disciplinary action up to and including immediate suspension or dismissal from position/employment.
- Attending a class or meeting on responsible use issues, as well as successful completion of a follow up quiz.
- Loss of university computing, email, and/or voicemail privileges.
- Disconnection from the campus network.
- University judicial sanctions as prescribed by the student Code of Conduct.
- Reassignment or removal from University housing and/or suspension or expulsion from the University;
- Prosecution under applicable civil or criminal laws.

Reporting Violations

Reports of problems or violations should be made through the Campus Conduct Hotline, which is a confidential, anonymous way to alert administrators of unsafe or unethical behavior. Phone 866-943-5787 or or report online at Lighthouse Anonymous Reporting .

Performance Evaluation

Consequences of Policy Violation:

Enforcement
To ensure adherence to the Electronic Communications Policy and to protect the integrity of University resources, Trinity University reserves the right as described above to monitor the electronic communications across their systems to protect the security of the University's information, network, computing resources, and its users.

Any behavior in violation of this policy is cause for disciplinary action. Violations will be adjudicated, as appropriate, by the CIO, the Office of the Dean of Students, the Office of Housing and Residential Life, and/or the Office of Human Resources. Sanctions as a result of violations of this policy may result in, but are not limited to, any or all of the following:

- Attending a class or meeting on responsible use issues, as well as successful completion of a follow up quiz;
- Loss of university computing, email, and/or voicemail privileges;
- Disconnection from the residential hall internet;
- University judicial sanctions as prescribed by the student Code of Conduct;
- Monetary reimbursement to the University or other appropriate sources;
- Reassignment or removal from University housing and/or suspension or expulsion from the University;
- Prosecution under applicable civil or criminal laws.

Reporting Violations

Reports of problems or violations should be made through the Campus Conduct Hotline, which is a confidential, anonymous way to alert administrators of unsafe or unethical behavior. Phone 866-943-5787 or email **cch@eiia.org**. Further information can be found at http://www.campusconduct.com

Terms & Definitions

Terms and Definitions:

Term:	Definition:
Dynamic Host Configuration Protocol (DHCP)	Used by network devices to obtain the parameters required for operation in an Internet Protocol network
Information and Technology Resources	The full set of information technology devices (telephones, personal computers, printers, servers, networking devices, etc.) involved in the processing, storage, accessing, and transmission of information owned by, controlled by, or contracted to Trinity University. Connection of these devices can be permanent, via cable, or temporary, through telephone or other communications links. The transmission medium can be physical (e.g., fiber optic cable via FTTX) or wireless (e.g.. satellite, wi-fi, Wi-Max).
Internet Protocol (IP) Address	The address of the client on the Internet which identifies the client making any given connection to a site. Every computer connected to the Internet has an IP address which enables the identification of that computer.
Recurring mass email messages	Mass email based messages that are sent by users, departments, or offices regularly or on a scheduled basis to many recipients of the Trinity University community. This includes, but is not limited to, newsletters.
Trinity email accounts	Individual email accounts provided by the university to students, faculty, and staff with an address of @trinity.edu.

Revision Management

Revision History Log:

Revision #:	Date:	Recorded By:
v3.0	7/26/2022 11:33 AM	Ben Lim
v2.0	5/19/2022 11:27 AM	Dan Carson
v1.0	8/14/2019 11:21 AM	Courtney Cunningham

Vice President Approval:

Name:	Title:
Ben Lim	Chief Information Officer