| University-wide Policy:<br>OIT0100- Email Policy Information Technology | |
|---|---|
| **Version: 1** | **Effective Date: 5/19/2020** |

**Title:** OIT 0200 – Email Policy

**Owner:** Chief Information Officer

**Responsible Department:** Office of Information Technology

**Purpose:**

This document establishes the policy for acceptable use of electronic mail or email that is furnished by the university. Note that email is the official means of communication authorized by St. Thomas University (STU). The University community is based on principles of honesty, academic integrity, respect for others, and respect for others' privacy and property; thus, The University seeks to:

1. Protect the confidentiality and integrity of electronic information and privacy of its Users, to the extent required or allowed under federal and state law; and
2. Ensure that the use of electronic communications complies with the provisions of University policy and state and federal law; and
3. Allow for the free exchange of ideas and support of academic freedom.

**Scope:**

This policy applies to all Users of and information technology (IT) resources owned, operated, or provided by STU including its campus, institutes, and administration.

Information and or all intellectual property created, transmitted or stored on University IT resources is the property of the University unless it is specifically identified as the property of other parties.

**Definitions:**

1. **Sensitive Information –** Information that is protected against unwarranted disclosure. Protection of sensitive information may be required for legal, ethical, privacy, or proprietary considerations. Sensitive information includes all data which contains: Personally Identifiable Information, Protected Health Information, student education records, card holder data, or any other information that is protected by applicable laws, regulations, or policies.
2. **Unit –** An operational entity such as a Campus, Institute, division, or department.
3. **Users** includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University's information technology resources.

**Procedures:**

The University adopted the policy principles as established in the National Institute of Standards (NIST) 800 series of publications, and this policy is based on those guidelines.

The Vice President for Administration has designated the Chief Information Officer (CIO) as the position responsible for information security at the University.

The University must develop or adopt and adhere to a program which demonstrates compliance with this policy and related standards. This program is the responsibility of the Chief Information Officer.

Each User of University resources is required to be familiar and comply with University policies. Acceptance of this policy is assumed if a User accesses, uses, or handles University resources.

**Policy:**

**I. General**

a. St. Thomas University (STU) provides email services to faculty, staff, students, and to other third-party contractors and visitors. Use of STU email services must be consistent with STU's educational goals, mission, and policies while also complying

with local, state, and federal laws. Email also is the preferred way of communications at STU, and therefore, community members are expected to check their university issued email on a regular basis.

b. STU attempts to provide secure, private and reliable email services by following sound information technology practices. However, STU cannot guarantee the security, privacy, or reliability of its email service. Email must not contain information that is restricted by any federal, state, or local law i.e. FERPA, etc. No personally identifiable information should be communicated via email. Should sensitive data need to be shared a link to a secure document must be shared that requires the recipient to securely log in to view said data.

c. The University owns all STU Email Accounts. Subject to underlying copyright and other intellectual property rights under applicable laws and University policies, the University also owns data transmitted or stored using the University Email Accounts. University issued accounts should be used for business or educational purposes only. STU reserves the right to access and disclose the content of all messages for any purpose without prior notice, and supervisors may review the electronic mail communications of workers they supervise to determine whether they have breached security, violated policy, or taken other unauthorized actions.

d. All STU related work or communications must be conducted through University issued email accounts, rather than personal accounts. For employees, all email sent through STU issued emails must contain the sender's first and last name, job title, email address, and telephone number in the signature.

e. All incoming email is scanned for viruses, phishing attacks and SPAM. Suspected messages are blocked from the User's inbox. Due to the complex nature of email, it is impossible to guarantee protection against all SPAM and virus infected messages. It is therefore incumbent on each individual to use proper care and consideration to prevent the spread of viruses. In many cases, viruses or phishing appear to be sent from a friend, coworker, or other legitimate source. Do not click links or open attachments unless the User is sure of the nature of the message.

f. Requests for shared departmental accounts will be accommodated, but require a designation of an account administrator, who will monitor the addition, deletion, or modification of names within the account, as well as manage the account as per these guidelines.

## II. Appropriate Use

a. With respect to University Email Accounts, the exchange of any inappropriate email content outlined below and described elsewhere in this policy, is prohibited. Users receiving such email should immediately contact the Office of Information Technology, who in certain cases may also inform the Public Safety, Human Resources, Student Affairs, the CARE team, or the Compliance Office depending upon the content of the communication.

b. The exchange of any email content outlined below is prohibited:

   i. Generates or facilitates unsolicited bulk email;

   ii. Infringes on another person's copyright, trade or service mark, patent, or other property right, or is intended to assist others in defeating those protections;

   iii. Violates, or encourages the violation of, the legal rights of others, or federal and state laws;

   iv. Is for any malicious, unlawful, invasive, infringing, defamatory, or fraudulent purpose;

   v. Intentionally distributes viruses, worms, Trojan horses, malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature;

   vi. Interferes with the use of the email services, or the equipment used to provide the email services, by customers, authorized resellers, or other authorized Users;

   vii. Alters, disables, interferes with, or circumvents any aspect of the email services;

   viii. Tests the email services in order to find limitations, vulnerabilities or evade filtering capabilities;

   ix. Constitutes, fosters, or promotes pornography;

x. Is excessively violent, incites violence, threatens violence, or contains harassing content;

xi. Creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement;

xii. Improperly exposes trade secrets or other confidential or proprietary information of another person;

xiii. Misrepresents the identity of the sender of an email.

c. Other improper uses of the email system include:

i. Using or attempting to use the accounts of others without their permission.

ii. Collecting or using email addresses, screen names information, or other identifiers without the consent of the person identified (including without limitation, phishing, spidering, and harvesting);

iii. Use of the service to distribute software that covertly gathers or transmits information about an individual;

iv. Conducting business for profit under the guise of the University

v. Political activities, specifically supporting the nomination of any person for political office or attempting to influence the vote in any election or referendum on behalf of or under the sponsorship of the University.

d. This list is not intended to be exhaustive but rather to provide some illustrative examples.

## III. Termination of Accounts

a. Individuals may leave the University for a variety of reasons, which gives rise to differing situations regarding the length of email privileges or expiration of accounts. The policy governing those privileges are set forth below. Notwithstanding the guidelines below, the University reserves the right to revoke email privileges at any time.

i. **Faculty** – Faculty members who leave the University will have email privileges removed effective on their last worked day. Exceptions will be made if a professor is granted emeritus status.

ii. **Staff** – Staff members who leave the University will have email privileges removed effective on their last worked day.

iii. **Students** – Students removed from the University due to disciplinary or academic issues will have their email privileges revoked as appropriate. If a student takes a leave of absence from the University, then the student's email privileges will be removed 366 days after the beginning of the last term in which the student was registered.

b. Upon departure of an employee from the University, Human Resources will notify the Office of Information Technology to deactivate the former employee's email account. Each semester, the Registrar's Office will notify the Office of Information Technology of the no longer active students. This notification will be sent within a week of the conclusion of the Add/Drop period for the academic semester.

## IV. Violation of University Email Policy

a. Violations of this policy will be handled under normal University disciplinary procedures applicable to the relevant persons or departments. In addition, a violation may result in:

i. suspension, blocking, or restriction of access to information and network resources when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of University resources or to protect the University from liability;

ii. disciplinary action up to and including separation from the University;

iii. a department being held financially responsible for the costs incurred as result of a data breach, loss or illegal disclosure.

## V. Policy Review Cycle

a. This policy will be reviewed every three years. This version supersedes and replaces previous policy versions.

**References:** n/a