TIFFIN UNIVERSITY
155 Miami Street, Tiffin, Ohio 44883
800.968.6446 . tiffin.edu

Email Policy

1. Purpose

Tiffin University currently utilizes a single solution for email; a cloud-based system using Tiffin's domain name pursuant to an agreement between the University and Google, Inc. ("Gmail Accounts").

The purpose of this policy is to ensure the proper use of this solution.

Electronic Mail is a tool provided by the University and serves as a primary means of communication to improve education and administrative efficiency. Users have the responsibility to use this resource in an efficient, ethical and lawful manner. Use of University Email Accounts evidences the user's agreement to be bound by this policy.

2. Policy

2.1 Account Creation

University Email Accounts are created based on the official name of the staff or faculty member as reflected in Human Resource, Payroll or Provost's Office records. Student accounts are created based on user ID reflective of the name on file with the Registrar. Requests for name changes to correct a discrepancy between an email account name and official University records will be processed, in which case the email account

name will be corrected. This could be due to error or a person legally changing their name. Requests for mail aliases based on name preference, middle name, etc., are evaluated on a case-by-case basis.

2.2 Ownership of Email Data

The University owns all University 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.

2.3 Privacy and Right of University Access

While the University will make every attempt to keep email messages secure, privacy is not guaranteed and users should have no general expectation of privacy in email messages sent through University Email Accounts. Under certain circumstances, it may be necessary for TU staff or other appropriate University officials to access University Email Accounts. These circumstances may include, but are not limited to, maintaining the system, investigating security or abuse incidents or investigating violations of this or other University policies, and, in the case of Gmail Accounts, violations of Google's Acceptable Use Policy or the University's contracts with Google. TU staff or University officials may also require access to a University Email Account in order to continue University business where the University Email Account holder will not or can no longer access the University Email Account for any reason (such as death, disability, illness or separation from the University for a period of time or permanently). Such access will be on an as-needed basis and any email accessed will only be disclosed to individuals who have been properly authorized and have an appropriate need to know or as required by law.

All email users are bound by the appropriate acceptable use policy of both Tiffin University and Google.

Google also retains the right to access to the Gmail Accounts for violations of its Acceptable Use Policy. (http://www.google.com/a/help/intl/en/admins/use_policy.html)

2.4 Data Purging

Gmail Accounts

Email messages held under Gmail will be subject to Google's storage and retention policies, which may change from time to time, with or without notice. As of this writing, retention time is 3 years after graduation and storage is unlimited.

Individuals should not rely on an email account to archive data and each person is responsible for saving individual messages and attachments as appropriate. Google Drive data is not backed up by the University and we are not responsible for lost or deleted files. Network shares should be used to store all sensitive and critical data as they are backed up and redundant.

2.5 Record Retention

It is the responsibility of employees to preserve University records, including emails or instant messages in particular circumstances:

· Those who have actual knowledge of matters in which it can be reasonably anticipated that a court action will be filed.

· A subpoena has been served or notice of same has been given.

· Records are sought pursuant to an audit or similar pending or possible investigation.

2.6 Data Backup

Because restoration of the entire email system is a lengthy process, requests for email account restoration is generally granted only in the case that loss of the data significantly affects a TU business process.

Restoration services for Gmail Accounts are only offered for messages that have been deleted no longer than 25 days.

2.7 Expiration of Accounts

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.

- **Faculty who leave before retirement** – Faculty who leave before retirement may keep their email account for one year from the end of the last term in which they taught. If such separation is for cause, email privileges may be immediately revoked without notice.
- **Staff who leave before retirement** – Staff members who leave the University will have email privileges removed effective on their last worked day. If such separation is for cause, email privileges may be immediately revoked without notice.
- **Retired Faculty** – Faculty who have retired from the University may be permitted to retain their email privileges.
- **Retired Staff** – Staff who have retired from the University may be permitted to retain their email privileges
- **Graduating students** – Graduating student will have access to their account for 3 years from the date of their graduation.
- **Students who leave before graduation** – Students who leave the University without completion of their degree or other program may keep their email privileges for one academic year from the last term when they were registered.
- **Expelled students** - If a student is expelled from the University, email privileges will be terminated immediately upon the directive of the Dean of Students Office.
- **Alumni** – students who have graduated from the University will be permitted to retain their email privileges for three years after graduation.

2.8 Appropriate Use and User Responsibility

No data that is classified as protected by the Data Classification Policy shall be stored in or transmitted via email. This includes but is not limited to personally identifiable information, Social Security number, bank account information, tax forms, background

checks, sensitive research data, or other Protected Data. See the University Data Classification Policy for further information.

Users who use email communications with persons in other countries should be aware that they may be subject to the laws of those other countries and the rules and policies on others systems and networks. Users are responsible for ascertaining, understanding and complying with the laws, rules, policies, contracts and licenses applicable to their particular uses.

Approval and transmission of email containing essential University announcements to students, faculty, and /or staff will follow the guidelines determined by the Digital Communications Committee.

Use of distribution lists or 'reply all' features of email should be carefully considered and only used for legitimate purposes as per these guidelines.

Any use of a University Email Account to represent the interests of a non-University group must be authorized by an appropriate University official.

In order to prevent the unauthorized use of email accounts, the sharing of passwords is strictly prohibited. Each individual is responsible for his/her account, including the safeguarding of access to the account. All email originating from an account is assumed to have been authored by the account holder, and it is the responsibility of that holder to ensure compliance with these guidelines.

TU maintains the University's official email systems; faculty, staff and students are expected to read email on a regular basis and manage their accounts appropriately. An email message regarding University matters sent from an administrative office, faculty, or staff member is considered to be an official notice. Faculty, staff, or students who choose to use another email system (apart from the Gmail Accounts) are responsible for receiving University-wide broadcast messages and personal mail by checking the University's official email system.

2.9 Departmental Accounts

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

2.10 Personal Email Accounts

In order to avoid confusing official University business with personal communications, employees must never use non-university email accounts (e.g. personal Verizon, Comcast, etc.) to conduct Tiffin University business.

2.11 Inappropriate Use

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 TU, who in certain cases may also inform the Department of Public Safety, The Department of Human Resources, The Dean of Students or The Office of General Counsel.

The exchange of any email content outlined below is prohibited:

- Generates or facilitates unsolicited bulk email;
- 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;
- Violates, or encourages the violation of, the legal rights of others or federal and state laws;
- Is for any malicious, unlawful, invasive, infringing, defamatory, or fraudulent purpose;
- Intentionally distributes viruses, worms, Trojan horses, malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
- 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;
- Alters, disables, interferes with or circumvents any aspect of the email services;
- Tests or reverse-engineers the email services in order to find limitations, vulnerabilities or evade filtering capabilities;
- Constitutes, fosters, or promotes pornography;
- Is excessively violent, incites violence, threatens violence, or contains harassing content;
- 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;
- Improperly exposes trade secrets or other confidential or proprietary information of another person;
- Misrepresents the identity of the sender of an email.

Other improper uses of the email system include:

- Using or attempting to use the accounts of others without their permission.
- 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);
- Use of the service to distribute software that covertly gathers or transmits information about an individual;
- Conducting business for profit under the aegis of the University
- Using Tiffin University email to sign up for personal websites and services.
- 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.

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

3. Scope

This policy applies to all individuals who use or maintain a Tiffin provisioned email account.

Complete listings of all University IT Policies can be found here: https://www.tiffin.edu/its/policy

4. Procedures

TU staff can provide recommendations and support for this policy through specific considerations and technologies.

4.1 SPAM & Phishing

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. If any doubt exists, the user should contact the Helpdesk at pctech@tiffin.edu

SPAM messages can be forwarded to pctech@tiffin.edu where they may be added to the filter list.

5. Definitions

SPAM is defined as unsolicited and undesired advertisements for products or services sent to a large distribution of users.

Phishing is defined as the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

6. Approval and Revisions

Version 2.0 Approved December 10th, 2019 by TAC