SYSTEM POLICY:	Technology Administrative Policy
SUBJECT:	SU Email Administration and Use
AUTHORIZING BODY:	Southern University Board of Supervisor
RESPONSIBLE OFFICE:	Division of Information Technology - DoIT
DATE ISSUED:	March 31, 2017
LAST UPDATED:	March 31, 2017

RATIONALE

The purpose of this policy is to ensure the proper use of Southern University campuses email system used by faculty, staff and students (the "University Email Accounts") which are hosted at "Office 365" (O365) using campuses domain name pursuant to an agreement between the University and Microsoft, Inc. Electronic Mail is a tool provided by the University to complement traditional methods of communication and to improve education and administrative efficiency. Users have the responsibility to use this resource in an efficient, effective, ethical and lawful manner. Use of the University Email Accounts evidences the user's agreement to be bound by this policy. Violations of the policy may result in restriction of access to the University Email Accounts and/or other appropriate disciplinary action.

SCOPE AND APPLICABILITY

This policy applies to all employees and students attending Southern University. The policy covers the use of the email system at the SU System Office and campuses, as well as off campus use at remote locations. Campuses and other entities under the direction of the SUS are responsible for compliance at their respective institutions.

POLICY

Account Creation

University Email Accounts are created based on the official name of the student, faculty, and staff as reflected in Human Resource, Payroll and Registrar records. Requests for mail aliases based on name preference, middle name, nicknames, etc., cannot be accommodated. Only 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. User ID's will remain in the University system and will not be reused at any time.

Ownership of Email Data

The University owns both the 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.

Personal Use

While incidental personal use of a University Email Account is acceptable, conducting business for profit using a University Email Account is forbidden. Use of a University Email Account for political activities (supporting the nomination of any person for political office or attempting to influence the vote in any

election or referendum) is forbidden. Any use of a University Email Account to represent the interests of a non-University group must be authorized by an appropriate University official.

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 a University Email Account. Under certain circumstances, it may be necessary for the Division of Information Technology (DoIT) 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 violations of Microsoft's Acceptable Use Policy or the University's contract with Microsoft. DoIT 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 those individuals with a need to know or as required by law. Microsoft also retains the right to access the University Office 365 Accounts for violations of its Acceptable Use Policy.

Data Purging and Record Retention

Individuals are responsible for saving email messages as they deem appropriate. Unless a legal hold has been placed on an account, messages in University Email Accounts are subject to Microsoft's purge policies, which may change from time to time without notice. Microsoft currently provides the following guidelines for purging folders:

- ✓ Trash – 30 days
- ✓ Spam - 30 days

Employees 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, or records are sought pursuant to an audit, a government investigation or in similar circumstances must preserve University records, including emails or instant messages.

Data Backup

The University Office 365 Email Accounts are backed up by Microsoft on a regular basis as a way of recovering from a systematic loss impacting the entire email system.

Expiration of Accounts

Individuals may leave the University to take other employment, retire, transfer to another college, or simply go on to other activities. There are many situations at the University where the length of email privileges or expiration of accounts will differ, as set forth below. Notwithstanding the guidelines below, the University reserves the right to remove email privileges at any time.

- ✓ **Faculty** – Faculty who leave the University 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 suspended indefinitely without notice.

- ✓ **Staff** – 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 suspended indefinitely without notice.
- ✓ **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.
- ✓ **A student who is expelled** - If a student is expelled from the University, email privileges will be terminated immediately upon the directive of the Student Affairs.

In the event the University terminates or otherwise ceases its contractual relationship with Microsoft regarding the Office 365 Email Accounts, the University Email Accounts will be migrated to another platform in accordance with the terms of the Microsoft contract. Notice will be provided as soon as reasonably possible.

Appropriate Use

When using email as an official means of communication, students, faculty and staff should apply the same professionalism, discretion, and standards that they would use in written business communication. Furthermore, students, faculty and staff should not communicate anything via email that they would not be prepared to say publicly. Users of email shall not disclose information about students or employees in violation of University policies or laws protecting the confidentiality of such information.

- ✓ No private Personally Identifiable Information (PII) about University faculty, staff, students, alumni or other University members should be transmitted via email or stored in an unencrypted format. This includes but is not limited to Social Security number, bank account information, tax forms or other sensitive data.
- ✓ No technical data with potential for military defense application or otherwise subject to export control or other international trade control laws may be transmitted or stored in an unencrypted format.
- ✓ 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.
- ✓ Students who are employed by the University may not store information relating to their employment on their Office 365 Account.
- ✓ Approval and transmission of email containing essential University announcements to students, faculty, and /or staff should be obtained from appropriate University unit(s), such as the Office of Communication.

Use of distribution lists or 'reply all' features of email should be carefully considered and only used for legitimate purposes as per these guidelines. In some cases where email messages generate a high number of responses due to the subject matter, it may be appropriate to utilize discussion boards in lieu of email.

User Responsibility

DoIT maintains the University official email system. 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 Office 365 Accounts) are responsible for receiving University-wide broadcast messages and personal mail by checking the University's official email system, newsgroups, and the University World Wide Web Homepage. An alternate method of checking University email is to utilize the Forwarding Feature, which can be set to forward email to an individual's personal email account.

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 deemed to be authored by the account holder, and it is the responsibility of that holder to ensure compliance with these guidelines.

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 group account, as well as manage the account as per these guidelines. These accounts should be reviewed periodically by the group administrator to verify accuracy of member identities and the member list.

Temporary User

Faculty, staff, departments can request temporary email privileges for users outside of the University. Full time Faculty or Staff requesting these types of accounts will be required to submit user information, rationale for account, expiration date, & sponsor information. Such requests shall be approved by the appropriate Dean or Vice Chancellor. A mandatory one year re-sponsorship is required to maintain the account. Those accounts that are not re-sponsored after one year will have email privileges removed.

Supported Email Clients

University-supported email clients are Outlook and Outlook Web Apps (OWA). If a problem is encountered with the use of an alternate method, Helpdesk personnel will work with the individual to access email via the supported methods and will verify functionality of the supported environment. The University DoIT department is continually evaluating tools and technologies and reserves the right to modify the list of supported clients with appropriate notification.

Inappropriate Use

University Email Accounts are subject to the SU System Appropriate Technology Use Policy and Microsoft Office 365 Acceptable Use Policy. In addition, any inappropriate email usage, examples of which are described below and elsewhere in this policy, is prohibited. Users receiving such email should immediately contact DoIT, who in certain cases may also inform the Department of Public Safety.

The exchange of email content that:

- ✓ Generates or facilitates unsolicited bulk commercial 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 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.
- ✓ Is otherwise malicious, fraudulent or may result in retaliation against the University by offended viewers.

Other improper uses of the email system include:

- ✓ The use or attempt to use the accounts of others without their permission. Newsgroups are provided as a service to faculty, staff, and students for posting University-related information. These will be monitored by those responsible for their content; any posted material deemed inappropriate may be removed without prior notification.
- ✓ Collecting or using email addresses, screen names information or other identifiers without the consent of the person identified including without limitation, phishing, Internet scamming, password robbery and harvesting;
- ✓ Use of the service to distribute software that covertly gathers information about a user or covertly transmits information about the user;
- ✓ Any conduct that is likely to result in retaliation against the University's network or website, or the University's employees, officers or other agents, including engaging in behavior that results in any server being the target of a denial of service attack (DoS).

These guidelines provide some examples of permitted or prohibited use of email. This list is not intended to be exhaustive but rather to provide some illustrative examples.

SPAM & Viruses

Incoming email on the University Email Accounts is scanned for viruses and for messages deemed to be 'SPAM', or unsolicited advertisements for products or services sent to a large distribution. 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 appear to be sent from a friend or coworker, therefore attachments should only be opened when the user is sure of the nature of the message. If any doubt exists, the user should contact the Helpdesk.