UNIVERSITY EMAIL USE POLICY AND PROCEDURES

PURPOSE

Roseman University of Health Sciences utilizes two solutions for electronic mail or email:

- a cloud-based platform utilizing Microsoft's Office 365 ("Exchange Accounts") for employees; and,
- a cloud-based system using Roseman's domain name pursuant to an agreement between the University and Google, Inc. ("Gmail Accounts").

Collectively these are known as "University Email Accounts." The purpose of this policy is to ensure the proper use of these electronic mail solutions. Email is a tool provided by the University and serves as a means of communication and administrative efficiency. Users have the responsibility to use this resource in an ethical and lawful manner.

OWNERSHIP OF EMAIL DATA

Roseman 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.

PRIVACY AND RIGHT OF UNIVERSITY ACCESS

While Roseman 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 specific circumstances, it may be necessary for unit heads and/or their designee(s) to access current and former University Email Accounts. These circumstances can include, but are not limited to, investigating security or abuse incidents, investigating violations of University policies, or in order to continue critical University business where the University Email Account holder will not or can no longer access the University Email Account. 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.

ACCOUNT CREATION

Employees:

University Email Accounts are created based on the official name as reflected by the Human Resources unit. Accounts will be created after the official Human Resources notification has been received by the Technology Services unit. Exceptions to this process must be coordinated through the Human Resources office. The legal first and last name will be used for the account creation. If Human Resources indicates a nickname or preferred name (e.g., middle name or John instead of Jonathan) on the notification form, Technology services will use that.

The format used is first initial of the first name and the full last name, e.g., jsmith@roseman.edu. Sequential numbers will be used at the end of the last name if the account is already in use.

Generic User or Unit Email Accounts:

Requests for generic and/or shared unit accounts can be accommodated. Unit heads and/or their designee(s) requesting these types of accounts will be required to submit the desired account name, the names of the individuals who need access to the account, and the rationale for the account. It is the unit's responsibility to inform Technology Services when that email account is no longer in use.

Technology Services recommends avoiding generic user accounts where possible and limiting access to them because of the potential security risks. Requests must be submitted through the Help Desk Ticketing System.

ROSEMAN UNIVERSITY
OF HEALTH SCIENCES

Students:
Student accounts are created after they have completed the seating deposit process for the academic program. The legal first and last name will be used for the account creation. Students with two last names may indicate on their seating deposit form if they have a last name preference (e.g., John Smith-Doe can request jdoe or jsmith). Prior to matriculation requests for name changes approved by the academic program's admissions office and/or Office of Registrar/Student Services can be made. After matriculation, email addresses will not be updated to reflect the name change. The student may only request to have the mail display name updated.

The format used is first initial of the first name and the full last name, e.g., jsmith@student.roseman.edu. Sequential numbers will be used at the end of the last name if the account is already in use.

Individuals Outside the University:
Unit heads and/or their designee(s) can request temporary email privileges for users outside of the University, e.g., consultants or temporary workers not processed through Human Resources. Unit heads and/or their designee(s) requesting these types of accounts will be required to submit user information, rationale for account, and the date when the account is no longer needed (if known). It is the unit's responsibility to inform Technology Services when that individual has left. Requests must be submitted through the Help Desk Ticketing System.

The format used is first initial of the first name and the full last name, e.g., jsmith@roseman.edu. Sequential numbers will be used at the end of the last name if the account is already in use.

EMAIL ACCOUNT MAINTENANCE
Employees:
Through Microsoft Exchange 365, Exchange Accounts are backed-up on a regular basis as a way of recovering from a systematic loss affecting the entire email system. Should an email need to be restored, users must submit a request through the Help Desk Ticketing System. Back-ups of the user's email after one year will not be available for restoration.

Students:
Deleted emails within Gmail over thirty days cannot be restored by the user. Google permanently deletes all items in the Trash after thirty days.

EMAIL ACCOUNT REMOVAL
Employees:
Upon termination of employment, the individual's access will be removed. Unit heads and/or their designee(s) can request temporary access to these accounts as well as email forwarding. Employee email accounts will be permanently deleted after sixty days unless notified otherwise by the unit head and/or their designee(s). Administrative position Exchange Accounts (Directors and higher) will be permanently deleted after one year unless notified otherwise by the unit head and/or their designee(s). Unit heads and/or their designee(s) can also request the account to be deleted sooner than specified.

Terminated employees can request temporary access to their email account (e.g., faculty member actively working on a grant or publication). This must be approved by the Unit Head and/or their designee(s) and the Director of Human Resources. Access will be removed after sixty days. Exceptions to this process must be approved by the Unit Head and/or their designee(s) and the Director of Human Resources. Approved requests must be sent to the Vice President for Technology Services and/or their designee(s).

It is the unit's responsibility to reset the passwords of any shared or generic accounts if that individual had access to them.

Students:
Withdrawn student Gmail Accounts will be deleted if a student has not been enrolled in a program for more than forty-five days unless the Dean/Program Director and/or their designee(s) have requested to keep the account active.

If the student was a member of a student organization and had access to the organization's email account, it is the organization advisor's responsibility to reset the password.

Alumni:
Graduated students will continue to have access to their Gmail Account for one year after their graduation date. After that date, the Gmail Account will be deleted. Roseman will not issue email accounts to alumni.

APPROPRIATE USE AND USER RESPONSIBILITY

The Technology Services Unit maintains all of the University's official email systems, Exchange Accounts and Gmail Accounts. All students and employees are expected to read their emails on a regular basis and manage their accounts appropriately. An email message regarding University matters sent from a Roseman employee is considered to be an official notice.

Unless there is an identified and approved Roseman business purpose, data that is identified as protected shall not be transmitted via email. Protected information that must be sent by email is required to be encrypted. Protected information includes but is not limited to personally identifiable information (PII), Social Security numbers, bank account information, tax forms, background checks, sensitive research data, or other protected data. All users must maintain confidentiality of student information in compliance with the Family Education Rights and Privacy Act (FERPA) of 1974, and patient information in compliance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

To help reduce the amount of community emails from the programs and service units, announcement and unit related news information should be included in the weekly employee and student Roseman email newsletters distributed by the Marketing Unit.

For FERPA compliance purposes, any emails from Roseman employees that are being distributed to more than one student must use the Blind Carbon Copy (BCC) option in the email.

Use of the Roseman Distribution Lists or "Reply All" features of email should be carefully considered and only used for legitimate purposes.

In an effort to prevent the unauthorized use of email accounts, the sharing of passwords for accounts is strictly prohibited. Each individual is responsible for his/her account, including the safeguarding of access to the account. If a user has been assigned access to a unit generic email account, the sharing of passwords is strictly limited to only those authorized to use that account. See the **Computer and Network Acceptable Usage Policy** for more information on responsible use.

PERSONAL EMAIL ACCOUNTS

Employees are prohibited from using personal email accounts for Roseman business.

EMAIL SPAM AND PHISHING

All incoming email is scanned for viruses and spam. Messages that are suspected to have this content are blocked. However, it is impossible to guarantee protection against all email threats due to the continuous evolution of phishing techniques. It is critical that individuals use their best judgment when replying to emails, opening attachments, and clicking on links that may be in the emails. Users should contact the Technology Services Help Desk if there are any questions on the legitimacy of an email. Spam messages can be forwarded to spam@roseman.edu.

PROCEDURES AND SANCTIONS

Persons in violation of this policy are subject to a full range of sanctions, including, but not limited to, the loss of Roseman's technology resources access privileges, disciplinary action, and dismissal from the university. Some violations may constitute criminal offenses, as defined by local, state, and federal laws and the university may prosecute any such violation to the full extent of the law.