University Policy
Adopted by the University Policy Committee
April 13, 2022

University of Rochester
Policy on Email Use

Overview

Electronic mail (email) is a primary means of communication both within the University of Rochester and externally. It allows quick and efficient conduct of business, but if used carelessly or unlawfully, it carries the risk of harm to the University and members of its community.

Purpose

The purpose of this policy is to describe the permitted uses of University email. This policy is not meant to supersede or replace, but should be read together with other University policies. The Information Technology Policy [https://tech.rochester.edu/policy/] contains detail that is relevant to the use of email. Capitalized terms that are used but not defined in this Policy are intended to have the definitions detailed in the Information Technology Policy.

Compliance with this Policy helps the University to achieve two goals:

1. Improve the successful delivery of University communications to all faculty, staff, patients and students
2. Reduce the risk of University data classified as High Risk going through email systems not managed by the University

Who Must Follow This Policy

This policy applies to everyone who is provided email services managed by or for the University of Rochester including, but not limited to, University faculty and visiting faculty, physicians, staff, students, contractors, consultants, volunteers, and guests, any one of which being referred to as a “user” in this policy.

A. Use of Email Accounts

1. University Workforce

Email services are intended to allow all University faculty and staff (including TAR, Adjuncts etc.) to conduct University business. Personal use of email is not prohibited, provided that personal use (a) does not materially interfere with performance of an employee’s work responsibilities, (b) does not interfere with the performance of the University networks and (c) is otherwise in compliance with this and other

University policies. There is no guarantee that information transmitted or stored in the course of personal use of University Email services will be confidential or securely preserved.

Even the most careful user will occasionally send an email to unintended recipients. Users have no control over the forwarding or alteration of emails once sent. High Risk data transmitted by e-mail or other electronic transmission, must be encrypted or otherwise adequately protected. Data are classified as High Risk when protection of such data is required by law or regulation. Protection is necessary in order for the University or its affiliates to meet compliance obligations, or the unauthorized disclosure, access, alteration, loss or destruction of those data could have a material impact on the University or its affiliates' mission, assets, operations, finances, or reputation, or could pose material harm to individuals. For more information refer to https://www.rochester.edu/provost/wp-content/uploads/2020/07/Data-Classifications-Policy-Final-June2020.pdf

2. Students

The University currently provides email services to all students including non-matriculated students. Student use of email is subject to the student conduct codes, as well as this Policy, the University's Information Technology Policy and the University's Acceptable Use Policy.

3. 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.

B. Official Email Address

Students and University workforce members will be assigned an Official Email Address, which will include a mailbox assigned to one of the Official University email systems:

- *University Office 365*

  Note: currently working through a transition of URMC Exchange to Office 365 and during the transition, Medical Center faculty and staff may have a mailbox in on-premise Exchange until their Office 365 box is provisioned.

  Note: Alumni may opt into retaining their University email address and to have mail forwarded to a designated personal email box (beginning January 2022).

- *Student Email system (Gmail)*

  Note: Students with mailboxes in Gmail will retain that email as an alumnus.

The Official University Email Address is the email address that is provisioned upon entry to the University. The Official Email Address is to be used for all University Email correspondence, for populating lists for classes, and for the official online directory. Official communications from University

Offices, such as the President's Office, Human Resources, the Provost, Security and others, will be directed to the Official Email Address.

If an individual has both a student and employee affiliation, the University may provision a separate email box for each affiliation. Email services should be provided only while a user is employed by or enrolled at the University Exceptions may be granted for conditions such as email extensions for emeritus status, retirements, etc.,

Note: Email services may be terminated with notice if the University determines continuation of services is not in the University's best interest.

1. Use of Email Address to populate University Managed IT Systems

The Official University email address will be the email used to populate any University Managed IT System where "email address" is necessary for the effective business process operation of the system, e.g., Blackboard, URStudent, HRMS.

2. Use of Email Address as an authentication method for Cloud based services

The Official University email address will be the email used as the authentication credential for University contracted cloud based services where email address is the internal authentication method for the service; ie: Box.

3. Email Aliases

The University allows email aliases for the official University of Rochester email address. For the purpose of this policy, the email alias does NOT take precedence over the Official University email address. https://tech.rochester.edu/services/email-aliases/

C. Email Forwarding

Manually forwarding University Email that contains information classified as University High Risk is only permissible for valid business purposes and when done using appropriate security precautions.

Automation tools, protocols, or rules to enable auto-forwarding (POP, IMAP etc.), to move email from a University managed Email system to a non-University managed email system is not permissible without a formal exception from the IT Policy Committee.

Personal email accounts or servers set up to receive or transmit University related business messaging is not permissible without a formal exception from the IT Policy Committee.

D. Confidentiality, Security, and Privacy

The password associated with an Email account may be used to authenticate identity in other University online services. To safeguard the user's identity and privacy and the confidentiality of sensitive third-party information stored in Email accounts and devices assigned to the user by the University and other University systems accessible using the email password, a user must not share their account or give their password to anyone. Subjecting confidential information to disclosure by sharing a user's password is a violation of University policy and may result in a violation of law and/or breach of contracts to which the University is a party.

Users are required to promptly change their Email password upon receiving credible evidence that their password has become known by or disclosed to another party and/or when requested to do so by University IT Services or their supervisor.

Although the University does not monitor Email content routinely, users must not assume that Email content will remain private and confidential. A user's expectation of privacy in Emails is defined and limited by the University's Information Technology Policy. Access to Email by anyone other than the user may be permitted as described in that policy or otherwise required by law. In addition, Email can be altered or forwarded by a recipient without the sender's knowledge, and may also be discoverable in litigation or may be disclosed to comply with a subpoena.

Google retains the right to access to the Gmail Accounts for violations of its Acceptable Use Policy, or in response to subpoena or National Security Letter. (http://www.google.com/a/help/intl/en/admins/use_policy.html).

Microsoft retains the right to access to the O365 Accounts for violations of its Acceptable Use Policy, or in response to subpoena or National Security Letter. (http://www.microsoft.com/online/legal/v2/?docid=13&langid=en-us)

E. Misuse

As mentioned above, Email is a communication technology. Any policy of the University that applies to communications also generally applies to Email. Use of Email in violation of other University policies is also a violation of this policy. See the University of Rochester Acceptable Use Policy https://tech.rochester.edu/policies/acceptable-use-policy/ for more details.

Examples of improper uses of University Email:

- Concealment or misrepresentation of names or affiliations (e.g., misrepresenting oneself as another user);
- Use of University email to send spam;
- Alteration of source or destination address of email;

- Use of email for partisan political or lobbying activities;
- Use of email for commercial activities or personal gain;
- Use of email to violate the University's policy on Harassment and Discrimination;
- Use of email to violate the law.

F. Local Policies Permitted

Divisions and Departments within the University may adopt additional information technology policies that are specific to their operations, provided that such requirements are consistent with this Policy and the unit provides a copy of more specific unit policies to the University Chief Information Officer and the Office of Counsel. In the event of inconsistency, the provisions of this Policy will prevail, unless the more specific policies are necessary to meet legal requirements governing certain types of information, in which case the more specific legal requirements and related policy will take precedence.

G. Spam & Phishing

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, or credit card details (and sometimes, indirectly, money), often for malicious purposes, by masquerading as a trustworthy entity in an electronic communication.

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 and other malware. In many cases, viruses or phishing appear to be sent from a friend, coworker, or other legitimate source. Users should not click links or open attachments unless they are sure of the nature of the message. If any doubt exists, the user should contact the Helpdesk at UnivITHelp@Rochester.edu or HelpDesk_ISD@URMC.Rochester.edu

Spam messages can be forwarded to abuse@rochester.edu where they may be added to the filter list.

H. Retention and Disposal

Users should avoid retaining large amounts of Email (whether in the Inbox, Sent Items, Deleted Items or personal folders) for long periods of time. The University's Policy on Retention of University Records makes clear that Email box is not an appropriate place to retain University records; records that are in a user's Email should be removed to other paper or electronic storage media intended for archival purposes. Microsoft currently limits each email box to a maximum of 100 gigabytes. Microsoft reserves the right to change this store limit, with prior notice to the University of Rochester.

I. Sanctions

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:

- 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;

- disciplinary action up to and including separation from the University;

- department being held financially responsible for the costs incurred as result of a data breach, loss or illegal disclosure. University reserves the right to seek any remedy allowed by applicable law against any individual who, in connection with the use of University Email services or related University electronic resources, intentionally or in the exercise of gross negligence causes material loss or damage to the University or any third party to whom the University owes a duty of care.

Administration, Review, and Approval

Administration of this policy is assigned to University IT Services. Questions may be addressed to UnivITHelp at 275-2000.

Reviewed by the Data Security Task Force, and Adopted by the Provost and General Counsel on January 1, 2012.

Reviewed February 11, 2021 by the IT Policy Committee and adopted by the University Policy Committee on xxx, 2021.

Related Policies

I. University of Rochester Information Technology Policy
http://www.rochester.edu/it/policy/

II. University of Rochester Acceptable Use Policy
http://www.rochester.edu/it/policy/

III. Electronic Transfer of Protected Health Information via Facsimile and Electronic Mail
http://intranet.urmc-sh.rochester.edu/policy/hipaa/Privacy/P29.pdf

IV. University Faculty Handbook
http://www.rochester.edu/provost/FacultyHandbook/

V. Human Resource (HR) Policies
http://www.rochester.edu/working/hr/policies/

VI. University of Rochester Medical Center (URMC) Code of Conduct
http://www.urmc.rochester.edu/compliance-office/compliance-plans-policies/urmc-code-of-conduct.cfm

VII. University Code of Conduct for Business Activity
http://www.rochester.edu/working/codeofconduct/

VIII. Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Policies
http://intranet.urmc-sh.rochester.edu/policy/HIPAA/PolicyManual/