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 illegally, 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 [http://www.rochester.edu/it/policy/index.html] 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 given to them 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 and students, and
2. Reduce the risk of University data classified as Legally Restricted or Confidential going through email systems that are not managed by the University.

Who Must Follow This Policy

This policy applies to, but is not limited to, University faculty and visiting faculty, physicians, staff, students, contractors, volunteers, and guests who are provided email services managed by or for the University of Rochester.

A. Use of Email Accounts

1. University Workforce

Email services are primarily intended to allow faculty and staff to conduct University business. Personal use of email is allowed, provided that personal use (a) does not materially interfere with performance of 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.
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 they are sent. Accordingly, users must not use email to communicate data classified as University legally restricted information without appropriate security layers such as email encryption when sending to recipients external to UR email services (sending within internal email services are considered to be adequately secure). Common examples of this type of information include: social security numbers, credit card numbers, student grades and education records, personnel records, individual donor gift records, and health information subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

2. Students

The University currently provides email services to all 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.

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:

- URMC exchange
- UR exchange
- Arts, Sciences, and Engineering Email system (Zimbra)
- Student Email system (Gmail)
- Laser Laboratory Email system

The Official University Email Address is the address from which, and to which, University business-related Email is to be sent and received. The Official Email Address will be used for all University Email correspondence lists, 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.

Accordingly, users shall be presumed to have received all official University Email messages sent to their Official University 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.
C. Email Forwarding

Manually forwarding University Email that contains information classified as University legally restricted is only permissible for valid business purposes and appropriate security precautions such as email encryption must be taken. Automation tools such as auto-forwarding, POP, IMAP etc., to move email from a University managed Email system is only permissible to internally-administered University Email systems. (Academic and administrative units are permitted to operate such systems in addition to the centrally available resources, but the use of any such facilities shall also be subject to this policy and other University polices (e.g., University HIPAA policies, University IT Policy)).

D. Confidentiality and Security

All Email containing information protected by HIPAA policies must comply with the Electronic Transfer of Protected Health Information via Facsimile and Electronic Mail policy http://intranet.urmc-sh.rochester.edu/policy/hipaa/Privacy/P29.pdf.

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. In addition, Email can be altered or forwarded by a recipient without the sender’s knowledge, may also be discoverable in litigation or may be disclosed to comply with a subpoena.

The password associated with an Email account may be used to authenticate identity in other university online services. To safeguard your identity and your privacy, do not share your account or give your password to anyone.

E. Misuse

As mentioned above, Email is simply another 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 [http://www.rochester.edu/it/policy/acceptable.html] 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 Email to send spam (unsolicited non-University commercial Email);
- Alteration of source or destination address of Email;
Use of Email to violate the University’s policy on Harassment and Discrimination; and

Use of Email to violate the law.

F. Local Policies Permitted

Academic, clinical, and administrative units may supplement this policy with their own Email use standards and guidelines for local computing and network facilities. Typically, such additional rules would address situations of limited computing resources. In the event such local policies or standards are inconsistent with this Policy, this Policy shall govern unless a more restrictive policy exists at the local level.

G. Retention and Disposal

Users should avoid retaining large numbers 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 one’s 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.

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

Review and Approval

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

Modified on March 1, 2012. Reviewed by the Data Security Task Force, and Adopted by the Provost and General Counsel on March 8, 2012. Incorporated language to indicate internal email systems were presumed to be secure and provided example of types of auto forwarding.
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 Activities
     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/

Individuals are also required to comply with any other University or departmental policies governing interactions that occur on the University’s networks and on the Internet.