

University of Rochester

Policy on Acceptable Use of Information Technology and Resources

Overview

Information resources and technology at the University of Rochester support the educational, patient care, instructional, research, and administrative activities of the University, and the use of these resources is a privilege that is extended to members of the University of Rochester community. As a user of these services and facilities, you have access to valuable University resources, to [legally restricted and/or confidential information](#), and to internal and external networks. Consequently, it is important for you to behave in a responsible, ethical, and legally compliant manner.

Purpose

This document establishes specific requirements for the use of all computing and network resources at the University of Rochester.

In general, acceptable use means ensuring that the information resources and technology of the University are used for their intended purposes while respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements. If an individual is found to be in violation of the Acceptable Use Policy, the University may take disciplinary action, including restriction of and possible loss of network privileges or more serious consequences, up to and including suspension, termination, or expulsion from the University. Individuals may also be subject to federal, state and local laws governing many interactions that occur on the University's networks and on the Internet. These policies and laws are subject to change as state and federal laws evolve.

Scope

This policy applies to all users of computing resources owned or managed by the University of Rochester. Individuals covered by the policy include (but are not limited to) University faculty and visiting faculty, physicians, staff, students, alumni, contractors, volunteers, guests or agents of the administration, and external individuals and organizations accessing network services via the University's computing facilities.

Computing resources include all University-owned, licensed, or managed hardware and software, University assigned user accounts, and use of the University network via a physical or wireless connection (including RESNET), regardless of the ownership of the computer or device connected to the network.

These policies apply to technology whether administered in individual departments and divisions or by central administrative departments. They apply to personally owned computers and devices connected by wire or wireless to the University network, and to off-site computers that connect remotely to the University's network services.

Acceptable Use

In making acceptable use of resources, individuals covered by this policy must:

- Use resources only for authorized purposes.
- Protect their userid(s) and system from unauthorized use. Each individual is responsible for all accesses to University information resources and technology by their userid(s) or any activity originating from their system. An individual's userid and [password](#) act together as their electronic signature.
- Access only information to which they have been given authorized access or that is publicly available.
- Protect electronic protected health information (ePHI) in compliance with HIPAA Privacy and Security Rules, [URMC HIPAA policies](#), and other applicable laws.
- Use only legal versions of [copyrighted software](#) in compliance with vendor license requirements.
- Be considerate in the use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connection time, disk space, printer paper, manuals, or other resources.
- Restrict personal use of the University's information resources and technology to incidental, intermittent and minor use that is consistent with applicable law and University Policy
- Include only material germane to University matters in University, school, or departmental electronic communications, such as e-mail, Websites, blogs, etc.*

* Personal web sites, chat rooms, web logs (also known as blogs) and other forms of publicly available electronic communications hosted on or linked from University information resources and technology must comply with this Acceptable Use Policy and prominently include the following disclaimer: "The views, opinions and material expressed here are those of the author and have not been reviewed or approved by the University of Rochester."

In making acceptable use of resources, individuals covered by this policy must not:

- Gain access to or use another person's system, files, or data without permission (note that permission from an individual user may not be sufficient - some systems may require additional authority).
- [Reveal a password](#) to any other individual, even those claiming to be an IT support technician (over the phone or in person). If, in the professional judgment of the user, it is necessary to share a password with an IT support technician or any other individual, the password must be changed as soon as possible thereafter. Once shared, a password is considered compromised and must be changed immediately. Alternatively, the appropriate Helpdesk may be contacted for assistance with giving others appropriate authority to access an individual's files or e-mail on their behalf.
- Use computer programs to decode passwords or access-control information.
- Attempt to circumvent or subvert system or network security measures.
- Engage in any [activity that is intended to harm systems](#) or any information stored thereon, including creating or propagating malware, such as viruses, worms, or "Trojan horse" programs; disrupting services; damaging files; or making unauthorized modifications to University data.
- Make or use illegal copies of [copyrighted software](#), store such copies on University systems, or transmit them over University networks.
- Use e-mail, [social networking sites or tools](#), or messaging services in violation of laws or regulations or to harass or intimidate another person, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by using someone else's name or userid.
- Waste shared computing or network resources, for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, or by sending chain letters or unsolicited mass mailings.
- Use the University's systems or networks for commercial purposes; for example, by selling access to your userid or by performing work for profit with University resources in a manner not authorized by the University.
- State or imply that they speak on behalf of the University or use University trademarks and logos without authorization to do so.
- Violate any applicable laws and regulations or University policies and procedures that govern the use of IT resources.
- Transmit commercial or personal advertisements, solicitations, endorsements or promotions unrelated to the business of the University.
- Use "auto-forward" rules to send business e-mail to a non-University e-mail account if the e-mail contains any legally restricted and/or confidential information.
- Send or receive legally restricted and/or confidential information via the Internet without making reasonable accommodations for the security of such information.

- Modify, without proper authorization, any of the University's information resources and technology, including the work products of others.

Related Policies

University of Rochester Copyright Policy -

<http://www.library.rochester.edu/copyright/URpolicy>

University Faculty Handbook -

http://www.rochester.edu/provost/assets/PDFs/Faculty_handbook.pdf

Information Technology Policy - <http://www.rochester.edu/it/policy/>

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

University of Rochester Medical Center (URMC) Code of Conduct -

<http://www.urmc.rochester.edu/compliance-office/compliance-plans-policies/urmc-code-of-conduct.cfm>

University Code of Conduct for Business Activities -

<http://www.rochester.edu/working/codeofconduct/>

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.