

UNIVERSITY OF ROCHESTER INFORMATION TECHNOLOGY POLICY

PURPOSE

The University of Rochester recognizes the vital role information technology plays in the University's missions and related administrative activities as well as the importance in an academic environment of protecting information in all forms. As more information is used and shared in a digital format by students, faculty and staff, both within and outside the University, an increased effort must be made to protect the information and the technology resources that support it. Increased protection of our information and Information Technology Resources to assure the usability and availability of those Resources is the primary purpose of this Policy. The Policy also addresses privacy and usage of those who access University Information Technology Resources.

**UNIVERSITY OF ROCHESTER
INFORMATION TECHNOLOGY POLICY**

TABLE OF CONTENTS

SECTION I – INTRODUCTION	3
I. General Principles	3
A. Academic Freedom.	3
B. Supportive Academic Environment.	3
C. Accountability for University Resources.	3
D. Personal Use and Privacy.	3
E. Relationship to Division or Departmental IT Policies.	3
II. Scope	4
A. People to Whom Policy Applies.	4
B. Definition of Information Technology Resources.	4
SECTION II – PRIVACY	4
I. Access Restrictions for Personal Communications	4
II. Access Procedures	6
A. University Communications	6
B. Personal Communications.	6
C. Information Technology Management and Audit.	8
SECTION III - DATA CLASSIFICATION AND ACCESS RESTRICTIONS	8
I. Legally Restricted Information:	8
A. Social Security Numbers (SSN)	8
B. Patient Protected Health Information (HIPAA)	9
C. Student Information (FERPA) ¹	9
D. Financial Account, Credit and Debit Card Information	9
E. Employee Personnel Records.	9
II. Confidential Information:	11
III. Internal University Use Only Information:	11
IV. Public Information:	12
SECTION IV - ENFORCEMENT	12
SECTION V – APPROVAL AND REVIEW	12
SECTION VI - QUESTIONS – WHERE TO ASK	13

UNIVERSITY OF ROCHESTER INFORMATION TECHNOLOGY POLICY

Section I – Introduction

I. General Principles

A. Academic Freedom.

Academic freedom is a fundamental University value. This Policy will be administered in a manner that supports the principle of academic freedom.

B. Supportive Academic Environment.

The University of Rochester seeks to provide a supportive working, living, learning and clinical environment. To accomplish this, we actively look for ways to encourage exchange and discourse, to bring together faculty, students, and staff, and to build a community that encourages all of its members to succeed and grow.

C. Accountability for University Resources.

All members of the University community have responsibility to protect University resources for which they have access or custodianship. Members of the University community are accountable for their access to and use of University resources.

D. Personal Use and Privacy.

The University recognizes that students, faculty and staff have reasonable expectations of privacy in their uses of Information Technology Resources. However, rights to privacy are constrained in the University environment because (1) the University owns and supplies these Information Technology Resources to its faculty, staff and students fundamentally for the purpose of accomplishing its academic and patient care missions, (2) the Information Technology Resources contains many closely shared environments and resources and the rights of other users must be taken into account and (3) legal and ethical restrictions apply. Individuals may have access to unconstrained use through private or commercial systems located at their residence or elsewhere. Resources or systems owned and maintained by the University for the benefit of the academic community are primarily intended for use for the University, not personal or business communications.

E. Relationship to Division or Departmental IT Policies.

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. 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

UNIVERSITY OF ROCHESTER INFORMATION TECHNOLOGY POLICY

the more specific legal requirements and related policy will take precedence.

II. Scope

A. People to Whom Policy Applies.

This Policy applies to everyone who accesses University Information Technology Resources, whether affiliated with the University or not, whether on campus or from remote locations, including but not limited to students, faculty, staff, contractors, consultants, temporary employees, guests, and volunteers. By accessing University Information Technology Resources, the user agrees to comply with this Policy.

B. Definition of Information Technology Resources.

Information Technology Resources for purposes of this Policy include, but are not limited to, University-owned transmission lines, networks, wireless networks, servers, exchanges, internet connections, terminals, applications, and personal computers. Information Technology Resources include those owned by the University and those used by the University under license or contract, including but not limited to information recorded on all types of electronic media, computer hardware and software, paper, computer networks, and telephone systems. Information Technology Resources also includes, but is not limited to, personal computers, servers, wireless networks and other devices not owned by the University but intentionally connected to the University-owned Information Technology Resources (other than temporary legitimate access via the world wide web access) while so connected.

Section II – Privacy

I. Access Restrictions for Personal Communications

The University will not, without user permission, monitor, review or otherwise access Personal Communications (defined below) sent or received (e.g., email), created or stored on Information Technology Resources, except pursuant to the Access Procedures set forth in Section II, which permits access when determined reasonable by a senior administrative officer or for Information Technology Management. The reasons for which access to Personal Communications can be granted include, but not are limited to, the following circumstances:

UNIVERSITY OF ROCHESTER INFORMATION TECHNOLOGY POLICY

- To investigate or prevent a violation of law or University Policy;
- To protect health or safety or to provide assurance to the University or to health or other regulators or law enforcement authorities that harm has not occurred to patients, students or others.;
- To minimize or stop computer activity that interferes with the University's network or other computer operations;
- To comply with a subpoena, warrant, court order or similar legal process, including a discovery request or a litigation stay order issued by or investigation undertaken by the Office of Counsel in connection with a potential claim in anticipation of litigation; OR
- When the user is unwilling, unable or unavailable to consent, to access Personal Communications needed by another University employee in order to fulfill a teaching, research, patient care or other legitimate University function.

The access restrictions and approval process of this Policy do not apply to electronic communications and records supporting University Communications when accessed by authorized individuals for the purpose of carrying out University Business. The approval process described below applies only if access is sought to Personal Communications.

"Personal Communications" are limited to faculty and student research, teaching, learning or personal (i.e. non-University related) emails, documents and correspondence. All other emails, documents, and correspondence prepared by a faculty member, student or employee in connection with his or her job responsibilities are defined as "University Communications" and may be accessed as needed for the purpose of carrying out University Business without seeking prior approval.

"University Business" refers to the University's activities and functions, including, but not limited to, administrative functions in the areas of teaching, student life, patient care and research, as well as supportive administrative services. It includes all information related to patient care, although this information is subject to HIPAA and other patient privacy restraints.

UNIVERSITY OF ROCHESTER INFORMATION TECHNOLOGY POLICY

II. Access Procedures

A. University Communications

University Communications may be accessed for the purpose of carrying out University Business by individuals with authority to deal with communications related to their subject matter without prior permission from a University official. The purpose of the access is critical to the determination that prior permission from a University official is not necessary for access.

It is understood in the environment of Information Technology Resources that there may not always be a physical separation of electronic records between University Business and Personal Communications. If material is found during a legitimate search for University Communications that indicates a potential violation in Personal Communications of University policy, including this Policy, or illegal use, the individual(s) involved in the search should halt the search, secure the relevant Information Technology Resources and seek permission to access the Personal Communications under the procedure set forth under section B. Users are reminded of the General Principle in Section I that resources and systems owned and maintained by the University are intended for use for the University and not for personal or business communications. Individuals who want unconstrained use and privacy should use private or commercial systems located at their residence or elsewhere, not University IT Resources. Individuals using University IT Resources should recognize that complete privacy is not assured and should refrain from creating or keeping on University IT Resources communications that they wish to keep private.

B. Personal Communications

Anyone seeking access to Personal Communications (see definition in section I) without user consent must first present to a senior University official (President, Provost, Vice President of the University or Medical Center, Dean, CEO of Strong Memorial Hospital, Director of LLE or Director of MAG, and Vice Provost and Chief Information Officer, the "Official") reasonable cause for gaining such access. (See section I for examples of reasonable cause.) If the initiator of the request is a senior University Official, the request must be approved by another senior University Official. If the initiator of the request is the University President, the request must be approved by the Vice President and General Counsel. An individual cannot initiate a request for access and also be part of the decision-making process. Permission should

UNIVERSITY OF ROCHESTER INFORMATION TECHNOLOGY POLICY

generally be sought from the official in charge of the school or division relevant to the search if that official is available.

In requesting access to Personal Communications without user consent, the person seeking access should provide to the Official relevant information available to support the reasonable cause. The request regarding access should be in writing (email is preferable) to the Official with a copy sent to the Vice President and General Counsel. The decision of the Official must be in writing (email is preferable) directed to the person requesting access with a copy to the Vice President and General Counsel and, if access is granted, a copy to the Information Technology team member who will oversee access. The Office of Counsel will retain a record of access requests and decisions for three years. The Official may also consult with the General Counsel, as needed.

If access is granted, the Official should designate a Director-level member of the University Information Technology Service or relevant other Information Technology unit, as appropriate, to conduct the access and review or to directly supervise the review and access if carried out by a technician with the appropriate skills. To the greatest extent practicable, the ITS staff should access or review only communications or data necessary to meet the purpose underlying the request. If other information is gathered by necessity or accident, it should be returned to the user or securely discarded at the end of the investigation. The ITS reviewer should communicate his or her findings from the access or review to the individual whose request for access or granted or to such other person(s) as the Official designated.

Generally, the user will be notified that access has been granted. In some circumstances, however, notice will not be given, such as in those cases when notice would compromise the reviewer's ability to achieve the underlying reason for the request, when a court or law enforcement agency directs the University not to give notice, when notice is impracticable under the circumstances or when the review is not directed at a particular user. The officer who grants access must decide in each case whether notice to the user is appropriate.

Some University employees, to perform their assigned duties, must have special privileges to access hardware and software, including specific files. Such employees are expected to abide strictly by this Policy, and are subject to discipline, including termination, for violating it.

In emergency situations in order to prevent destruction of equipment or data, it may be necessary for the University to seize or otherwise secure computers or other information technology pending initiation under this

UNIVERSITY OF ROCHESTER INFORMATION TECHNOLOGY POLICY

Policy concerning access to the information contained therein. The University reserves this right with respect to information technology governed by this Policy.

C. Information Technology Management and Audit

The University may use mechanisms to manage the information technology operations, including (but not limited to) spam and virus detection and elimination; limitation of network volume or blockage of access to specify file types or sites; or restriction of access to sites that present a security risk to the University's systems or experience high volumes of network traffic unrelated to the academic missions of the University. Use of such mechanisms must be approved by Director level University Information Technology(University IT) staff or any other person designated by the Chief Information Officer and must be consistent with legitimate University business needs. It may be necessary for the Office of University Audit or the University's outside auditors in the course of an audit to access Information Technology Resources and information stored thereon. Audits are authorized by the Board of Trustees or by a senior University officer and are governed by protocols that protect unnecessary disclosure of information.

Section III - Data Classification and Access Restrictions

Access to information owned by the University is generally broadly consistent with the concept of academic freedom and the open nature of the institution. However, there are types of information where access must be restricted and caution in handling and storing the information is necessary.

This policy is not intended to replace or supersede the specific policies identified below, and any conflicts will be controlled by the specific policies and not this one.

I. Legally Restricted Information:

The disclosure and use of the following types of information is restricted by law. See the specific policies referenced for a more specific definition of each type of information and of the rules and procedures concerning its use –

A. Social Security Numbers (SSN)

<https://tech.rochester.edu/policies/ssn-pii-policy/>

UNIVERSITY OF ROCHESTER INFORMATION TECHNOLOGY POLICY

B. Patient Protected Health Information (HIPAA)

<https://sites.urmc.rochester.edu/departments/hipaa/>

C. Student Information (FERPA)¹

<http://www.rochester.edu/registrar/policies.html>

D. Financial Account, Credit and Debit Card Information

<http://www.rochester.edu/adminfinance/treasury/docs/PolicyCreditCard.pdf>

E. Employee Personnel Records

<http://www.rochester.edu/working/hr/policies/pdfpolicies/108.pdf>
<http://www.rochester.edu/working/hr/policies/pdfpolicies/404.pdf>

Access and Use: Legally Restricted Information must be stored, used and disclosed to others only on a need to know basis to permit the individual faculty or staff member to perform their University functions for which the information was acquired and for which it is maintained. Access to legally restricted information must be carefully safe-guarded.

Protection of Legally Restricted Information from disclosure to or unauthorized access by anyone who does not have a legitimate need to access the information to comply with requirements of the law or to carry on necessary University functions is a primary responsibility of the Custodian.

Alternatives to using Legally Restricted Information should be identified and used whenever possible.

Disclosure of Legally Restricted Information to a third party agent or vendor is permitted only if the agent or vendor assumes a legally binding obligation to safe-guard the use and disclosure of the information. The electronic exchange of Legally Restricted Information outside of the University of Rochester must have proper approval. In addition,

- the appropriate Information Security Office must be consulted to ensure appropriate security controls are employed (See contact list below).
- Corporate Purchasing must be consulted to ensure appropriate contract language is incorporated into any agreement.

UNIVERSITY OF ROCHESTER INFORMATION TECHNOLOGY POLICY

Contact the Office of Counsel for appropriate contractual language.

Storage and Protection: Legally Restricted Information in paper form must be stored in locked or otherwise secured areas when not in active use. Legally Restricted Information in electronic form must be stored in secure designated data centers or, if authorized to be stored elsewhere, only in encrypted (or similarly protected) form. It must not be stored on desktop, laptop or other portable devices or media without encryption or similar protection. Contact Information Technology (University IT or ISD) or a Privacy Officer for advice and assistance.

Transmission: Reports and communications should not include Legally Restricted Information unless essential to perform the function for which the communication is made. Transmission of Legally Restricted Data must be by secure methods. If Legally Restricted Data is transmitted by e-mail or other electronic transmission, it must be encrypted or otherwise adequately protected.

Contact Information Technology (University IT or ISD) or a Privacy Officer for advice and assistance.

Destruction: When a record containing Legally Restricted Information is no longer needed, it must be disposed of in a manner that makes the Legally Restricted Data no longer readable or recoverable. Destruction of paper records containing Legally Restricted Data normally should be accomplished by shredding. Destruction of electronic records containing Legally Restricted Data begins with deleting the data from its storage location. Contact Information Technology (University IT or ISD) or a Privacy Officer for additional advice and assistance.

Specific Rules for FERPA¹ Student information is governed by FERPA and the University policies implementing FERPA. Because of the extensive educational activities of the University, many people within the University community have a legitimate need to access and transmit student records. The confidentiality of student records must be safe guarded, but the strict rules for storage and destruction of Legally Restricted Information set forth in this Policy are not always appropriate for student records. See the specific University policies on FERPA referenced above or contact the Registrar for more specific guidance.

Reporting Unauthorized Disclosure of Legally Restricted Information: Prompt reporting of unauthorized disclosure of Legally Restricted Information is essential for the University to meet its obligations under law, regulation, and contract. The University will not take disciplinary action against any person solely because of his or her good faith reporting of a disclosure. Individuals

UNIVERSITY OF ROCHESTER INFORMATION TECHNOLOGY POLICY

who report violations of this Policy will be protected from retaliation resulting from providing information. Individuals who report violations of this Policy to the Hotline can remain anonymous.

Immediately report any suspected unauthorized disclosure of or access to an SSN or material containing SSNs to any of the following:

	University	Medical Center
Privacy Officer	N/A	784-6154
Information Technology Security	273-2041	784-6115
Office of Counsel	273-5824	758-7619
Compliance Hotline	756-8888	756-8888

II. Confidential Information:

Information can be sensitive or proprietary and the University users may have reasons to treat it as confidential. Confidential Information includes many of the communications or records of the Board of Trustees and senior administrators. It includes faculty research or writing before publication or during the intellectual property protection process. It includes information that the University has agreed to hold confidential under a contract with another party. There are other examples.

Restriction of Information as Confidential: If a faculty or staff member is responsible for information that is sensitive, proprietary or otherwise in need of confidential treatment, the individual should clearly label the information "Confidential". The word Confidential should be placed prominently on the information in a form appropriate to the medium in which it exists with an understanding that the purpose of the label should be to warn others clearly that this information is Confidential and should be treated accordingly.

Storage, Transmission, Access and Destruction: The rules set forth in the section dealing with Legally Restricted Information should be applied to all Confidential Information.

III. Internal University Use Only Information:

Much information necessary for people to perform their work at the University is properly available to others at the University, but is not appropriate to be known by the general public. Information for Internal University Use Only is protected

UNIVERSITY OF ROCHESTER INFORMATION TECHNOLOGY POLICY

behind electronic firewalls or in private paper files in secured offices and is not accessible by the public at large. This is appropriate and will continue. Common sense and good practice dictate that this information remains accessible on a need to know basis by employees and sometimes by students, but not accessible by the media or outsiders. Examples are: budgets, strategic or unit business plans, proposals, contracts, many policies and procedures, correspondence, grant related documents, financial records, etc.

IV. Public Information:

Public information is information that is available to all members of the University community and may be made available to the general public. The University reserves the right to control the content and format of Public information. Examples include the University's audited financial statements, schedule of classes, approved census facts and the information on the public University website.

Section IV - Enforcement

Violations of this Policy will be handled under normal University disciplinary procedures applicable to the relevant persons or departments. The University may suspend, block or restrict 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. The University routinely monitors the use of Information Technology Resources to assure the integrity and security of University resources. The University may refer suspected violations of applicable law to appropriate law enforcement agencies.

Violations of this Policy can result in disciplinary action up to and including separation from the University and/or exclusion from University programs, facilities and privileges. Violations of law can lead to fines, injunctions and personal liability.

Section V – Approval and Review

To continue to support University technology resources, further Policy and procedural development is planned. Future Policy revision will likely include

UNIVERSITY OF ROCHESTER INFORMATION TECHNOLOGY POLICY

additional material concerning information security, data classification and network administration. The Policy will be reviewed and may be changed.

Approved by President Joel Seligman on December 12, 2006.

Revision approved on January 7, 2009.

Revision approved on March 17, 2011

Revision approved on July 25, 2014

Section VI - Questions – Where To Ask

If you have questions, call or email:

General Counsel

Gail Norris

Gail.norris@rochester.edu

585 275 2758

Vice President and Chief Information Officer

David Lewis

david.lewis@rochester.edu

585 275 5240