

UNIVERSITY POLICY

Policy Name:	Acceptable Use Policy for Information Technology Resources				
Section #:	70.1.1	Section Title:	Information Technology	Formerly Book:	N/A
Approval Authority:	Executive Vice President for Finance and Administration	Adopted:	2/1/2000	Reviewed:	8/22/2016
Responsible Executive:	Senior Vice President and Chief Information Officer	Revised:	8/31/2010; 1/23/2013; 10/10/2013; 7/3/2014; 10/27/2014; 8/22/2016		
Responsible Office:	Office of Information Technology, Information Protection and Security (OIT-IPS)	Contact:	oitpolicies@rutgers.edu		

1. Policy Statement

This policy outlines the acceptable use of University information and technology resources, which include, but are not limited to, equipment, software, networks, data, and stationary and mobile communication devices used to access Rutgers information and IT resources, whether the technology or devices are personally owned or owned, leased, or otherwise provided by Rutgers University-

2. Reason for Policy

Preserving access to information technology resources is a community effort which requires each member to act responsibly and guard against abuses. Therefore, both the community as a whole and each individual user have an obligation to abide by the standards established here for acceptable use.

3. Who Should Read this Policy

All members of the Rutgers University community.

4. Resources

Policies.rutgers.edu: [Information Technology - Section 70](#)
 Policies.rutgers.edu: [Clinical, Compliance, Ethics & Corporate Integrity - Section 100](#)
 Policies.rutgers.edu: [Data Breach Management Policy, Section 50.3.18](#)
 Policies.rutgers.edu: [Copyright Policy, Section 50.3.7](#)
 OIT Policies Website: <http://oit.rutgers.edu/policies>
 RU Secure Website: <http://rusecure.rutgers.edu/>

5. The Policy

A. Introduction

It is the policy of Rutgers University to maintain access for its community to local, national and international sources of information and to provide an atmosphere that encourages the free exchange of ideas and sharing of information. Nevertheless, Rutgers reserves the right to limit or restrict the use of its information technology resources based on applicable law, institutional policies and priorities, and financial considerations. Access to the University's information

technology resources is a privilege that requires each member to act responsibly and guard against abuses. Therefore, both the community as a whole and each individual user have an obligation to abide by the following standards of acceptable use.

This policy outlines the standards for acceptable use of University information technology resources, which include, but are not limited to, equipment, software, networks, data, and stationary and mobile communication devices owned, leased, or otherwise provided by Rutgers University.

B. User Responsibilities:

1. Each user may use only those information technology resources for which he or she has authorization. Violations include but are not limited to:

- using resources without specific authorization
- using another individual's electronic identity
- accessing files, data or processes without authorization

2. Information technology resources must be used only for their intended purpose(s). Violations include but are not limited to:

- misusing software to hide personal identity, or to interfere with other systems or users
- misrepresenting a user's identity in any electronic communication
- using electronic resources for deceiving, harassing or stalking other individuals
- sending threats, "hoax" messages, chain letters, spam, or phishing
- sending mass emails to the Rutgers community without following proper procedures. Please contact OIT's Enterprise Messaging division for more information.
- intercepting, monitoring, or retrieving without authorization any network communication
- using University computing or network resources for advertising or other commercial purposes
- circumventing or attempting to circumvent security mechanisms
- using privileged access to University systems and resources for other than official duties directly related to job responsibilities
- making University systems and resources available to those not affiliated with the University
- using former system and access privileges after association with Rutgers has ended

3. The access to and integrity of information technology resources must be protected. Violations include but are not limited to:

- Using third party, cloud and non-cloud, systems not authorized or approved by OIT's Information Protection & Security (IPS) Division to transmit, process, or store Rutgers data classified as restricted, including ePHI, Contact OIT's IPS division for additional information on using third party systems.

- creating or propagating computer viruses, worms, Trojan Horses, or any other malicious code
 - preventing others from accessing an authorized service
 - developing or using programs that may cause problems or disrupt services for other users
 - degrading or attempting to degrade performance or deny service
 - corrupting or misusing information
 - altering or destroying information without authorization
- 4. Applicable state and federal laws and University policies must be followed. Violations include but are not limited to:**
- failure to respect the copyrights and intellectual property rights of others
 - making more copies of licensed software than the license allows
 - downloading, using or distributing illegally obtained media (e.g., software, music, movies)
 - uploading, downloading, distributing or possessing child pornography
 - accessing, storing or transmitting information classified as Restricted data (e.g., social security numbers, patient health information, driver's license numbers, credit card numbers) without a valid business or academic reason or transmitting such information without using appropriate security protocols (e.g., encryption).
 - Distributing information classified as Restricted, unless acting as an authoritative University source and an authorized University distributor of that information and the recipient is authorized to receive that information.
 - Using social media to communicate or store University information classified as Restricted.
- 5. Users must respect the privacy and personal rights of others. Violations include, but are not limited to:**
- accessing, attempting to access, or copying someone else's electronic mail, data, programs, or other files without authorization.
 - divulging sensitive personal data to which users have access concerning faculty, staff, or students without a valid business or academic reason.
- 6. University business must be conducted using the Official University email, and calendar service, Rutgers Connect, including other O365 comprised services:**
- as per this University policy; in order to meet federal, state and local, legal, regulatory and statutory requirements (e.g., HIPAA, OPRA, FERPA, GLBA); and in a manner which ensures business continuity, enables proper E-Discovery and handles data in a secure and compliant manner.

C. Privacy:

The University has an obligation to respect the data privacy of members of the University community. That obligation is balanced by the University's needs to obey applicable laws, protect

the integrity of its resources, and protect the rights of all users and the property and operations of the University. Thus, the University reserves the right to examine material stored on or transmitted through its information technology facilities if there is reason to believe that the standards for acceptable use in this policy are being violated, or if there is reason to believe that the law or University policy are being violated, or if required to carry on its necessary operations. The University also reserves the right to review all email and other data, including personal email, stored on Rutgers systems for fulfillment of E-Discovery and New Jersey Open Public Records Act (OPRA). Reasonable efforts will be made to notify the user of the need for access to information stored on or transmitted through the University's information technology resources unless prohibited by law, inconsistent with University policy, or inconsistent with the University carrying out its normal operations. For example, information stored on the University's information technology system may be accessed by the University under certain circumstances, including but not limited to:

1. Access by technicians and system administrators to electronic records in order to address emergency problems, routine system maintenance, or other uses related to the integrity, security and availability of the University's information technology systems, including but not limited to:
 - a. Emergency Problem Resolution – Technicians may access technical resources when they have a reasonable belief that a significant system or network degradation may occur.
 - b. System-generated, Content-neutral Information – Technicians may access and use system-generated logs and other content- neutral data for the purposes of analyzing system and storage utilization, problem troubleshooting, and security administration.
 - c. Incident Response - The incident response function within the University Information Protection and Security Office (IPS) is responsible for investigating reports of abuse or misuse of University information technology resources. Incident response staff may use system-generated, content-neutral information for the purposes of investigating technology misuse incidents.
 - d. Network Communications - Security analysts of the University Information Protection and Security Office (IPS) may observe, capture, and analyze network communications. "Network communications" may contain content data and in some cases this content may be viewed to complete analysis.
 - e. User Request – Technicians may access information technology resources in situations where a user has requested assistance diagnosing and/or solving a technical problem.
2. Information requested pursuant to OPRA which requires disclosure of electronic communication and other data on the University system. Such access is approved through the Office of Enterprise Risk Management, Ethics and Compliance.
3. Information required to comply with a valid subpoena, a court order or e-discovery. Such access is approved through the Office of General Counsel.
4. Audits and investigations undertaken by governmental entities or by the Office of Enterprise Risk Management, Ethics and Compliance or by University auditors including the Department of Internal Audit or other University units authorized to carry out University policy.
5. The need of the University to carry on its normal operations (e.g., in the case of accessing the electronic records of a deceased, incapacitated or unavailable individual).

D. Technician and System Administrator Responsibilities:

Technicians, System Administrators and others involved in providing University's information technology resources have additional responsibilities regarding Acceptable Use. Where possible the number of persons granted privileged access should be limited and the rights granted should be according to the "least-privilege access" principle. If content can't be restricted, persons in these positions should treat the contents as Restricted information.

E. Violations:

1. Violators of this policy are subject to suspension or termination of system privileges and disciplinary action up to and including termination of employment.
2. If a suspected violation involves a student, a judicial referral may be made to the Dean of Students at the school or college of the student's enrollment. Incidents reported to the Dean will be handled through the University Code of Student Conduct.
3. It is a violation of this policy to unnecessarily delay acting on a directive to take corrective action to secure data or electronic credentials.