RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

~~RUTGERS~~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 and University Treasurer	**Adopted:**	2/1/2000	**Reviewed:**	12/13/2018
Responsible Executive:	Senior Vice President and Chief Information Officer	**Revised:**	08/31/2010; 01/23/2013; 10/10/2013; 07/03/2014; 10/27/2014, 08/22/2016; 02/27/2017 *(Reverted back to 10/27/2014 version)*; 12/13/2018		
Responsible Office:	Office of Information Technology (OIT)	**Contact:**	oitpolicies@rutgers.edu		

~~**Section:** 70.1.1~~

~~**Section Title:** Information Technology~~

~~**Policy Name:** Acceptable Use Policy for Information Technology Resources~~

~~Formerly Book: **N/A**~~

~~**Approval Authority:** Senior Vice President for Administration~~

~~**Responsible Executive:** Vice President for Information Technology and Chief Information Officer~~

~~**Responsible Office:** Office of Information Technology (OIT)~~

~~**Originally Issued:** 2/1/2000~~

~~**Revisions:** 8/31/2010; 1/23/2013; 10/10/2013 (Updated title), 7/3/2014; 10/27/2014~~

~~**Errors or Changes? Contact:** oitpolicies@rutgers.edu~~

1. Policy Statement

It is the policy of Rutgers University to allow 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 inappropriate use and abuse. Therefore, both the community as a whole and each individual user have an obligation to abide by the following standards of acceptable use.

~~2.~~ Users' expectations of privacy protection for electronic data must be balanced against the University's reasonable need to supervise, control, and operate the University's information

systems. Although the University will not monitor the content of electronic documents or messages as a routine matter, it reserves the right to examine all computer files and content in order to protect individuals and the University. ~~This policy outlines the acceptable use of university information technology resources, which include, but are not limited to, equipment, software, networks, data, and stationary and mobile communication devices whether owned, leased, or otherwise provided by Rutgers University.~~

2. Reason for Policy

This policy outlines the acceptable use of U~~u~~niversity information technology resources, which include, but are not limited to~~,~~: equipment, software, networks, systems, data storage devices, media, facilities, and stationary and mobile ~~communication~~ devices used to access Rutgers information technology resources, whether the technology or devices are personally owned, leased, or otherwise provided by Rutgers University. Information technology resources also include any and all Rutgers data, records, information, and record systems stored on or retrievable from such equipment, software, networks, systems, data storage devices, media, and facilities, or stationary and mobile devices. ~~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.

~~3.~~4. ~~Related Documents~~Resources

University Policy: Information Technology - Section 70: https://policies.rutgers.edu~~: Information Technology - Section 70~~

University Policy: Clinical, Compliance, Ethics & Corporate Integrity - Section 100: https://policies.rutgers.edu~~: Clinical, Compliance, Ethics & Corporate Integrity - Section 100~~

~~Policies.rutgers.edu: Identity Theft Compliance Policy, Section 50.3.9~~

University Policy 50.3.7: ~~Policies.rutgers.edu:~~ Copyright Policy~~, Section 50.3.7~~

University Policy 70.1.6: ~~Policies.rutgers.edu:~~ Email and Calendar Policy~~, Section 70.1.6~~

OIT Policies Website: http://oit.rutgers.edu/policies

RU Secure W-ebsite: http://rusecure.rutgers.edu/

~~4. Contacts~~

~~Information Protection and Security,~~
~~OIT 732-445-8011~~
~~rusecure@rutgers.edu~~

5. Definitions

N/A

6. The Policy

~~70.1.1 ACCEPTABLE USE POLICY FOR INFORMATION TECHNOLOGY RESOURCES~~

~~**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.~~

~~This policy applies to all users of Rutgers information technology resources. This includes but is not limited to, faculty, staff, students, guests, and external individuals or organizations.~~

A. User Responsibilities~~:~~

~~**B.**~~ Because the primary use of the University's communications and business systems is to further the institutional mission, members of the University community should not have the expectation of privacy in their use of electronic systems, whether work-related or personal. By their nature, electronic systems may not be secure from unauthorized access, viewing, or infringement. Although the U~~u~~niversity employs technologies to secure its electronic resources, as a rule confidentiality of electronic data cannot be assumed.

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

~~o~~• using resources without specific authorization

~~o~~• using another individual's electronic identity

~~o~~• accessing files, data, or processes without authorization

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

~~o~~• misusing software to hide personal identity, or to interfere with other systems or users;

~~o~~• misrepresenting a user's identity in any electronic communication;

~~o~~• using electronic resources for deceiving, harassing, or stalking other individuals. University Policy 60.1.12: Policy Prohibiting Discrimination and Harassment;

• sending threats, "hoax" messages, chain letters, or phishing;

~~o~~• sending mass emails to the Rutgers community without following proper procedures;

- ~~o~~• intercepting, monitoring, or retrieving without authorization any network or other electronic communication;

- ~~o~~• using U~~u~~niversity computing or network resources for private advertising or other private commercial purposes. https://oit.rutgers.edu/official-email;

- ~~o~~• circumventing, disabling, or attempting to circumvent or disable security mechanisms without authorization;

- ~~o~~• using privileged access to ~~u~~University systems and resources for other-than official duties directly related to job responsibilities, with the exception of incidental private use;

- ~~o~~• making ~~u~~University systems and resources available to those not affiliated with the ~~u~~University;

- ~~o~~• using former system and access privileges without authorization after association with Rutgers has ended or using system and access privileges to a former department's resources without authorization after the transfer to the new department.

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

- ~~U~~using third party, cloud and non-cloud, systems not authorized or approved by OIT's Information Protection & Security Division to transmit, process, or store Rutgers data classified as restricted. University Policy 70.1.2: Information Classification; ~~https://policies.rutgers.edu/sites/policies/files/70.1.2 - current.pdf~~;

- ~~o~~• creating or propagating computer viruses, worms, Trojan Horses, or any other malicious code;

- ~~o~~• preventing others from accessing an authorized service;

- ~~o~~• developing or using programs that may cause problems or disrupt services for other users;

- ~~o~~• degrading or attempting to degrade performance or deny service;

- ~~o~~• corrupting or misusing information;

- ~~o~~• altering or destroying information without authorization.

iv. Applicable state and federal laws and University policies must be followed. Violations include but are not limited to:

a) Laws

- ~~o~~• failure to respect the copyrights and intellectual property rights of others;

- ~~o~~• making more copies of licensed software than the license allows;

- ~~o~~• downloading, using, or distributing illegally obtained media (e.g.,-

software, music, movies);

- uploading, downloading, distributing, or possessing electronic content explicity prohibited by federal, state, or local law (i.e., child pornography)

b) Policies

- 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). University Policy 70.1.2: Information Classification ~~https://policies.rutgers.edu/sites/policies/files/70.1.2 - current.pdf~~ and https://rusecure.rutgers.edu/data-classification;~~.~~

- d~~D~~istributing data/information classified as Restricted, unless acting as an authoritative University source and an authorized University distributor of that data/information and the recipient is authorized to receive that data/information;~~.~~

- u~~U~~sing ~~media tools (e.g., Facebook, YouTube, Doximity, Sermo)~~social media to communicate or store University data/information classified as Restricted;~~.~~

- ~~Using third party email services (e.g. Hotmail, Yahoo) or non-encrypted email services to transmit Rutgers information classified as Restricted.~~

- ~~Forwarding or auto-forwarding Restricted information to a non-Rutgers email service.~~

- ~~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 media tools (e.g., Facebook, YouTube, Doximity, Sermo) to communicate or store University information classified as Restricted.~~

- ~~U~~using third party cloud storage or data sharing tools (i.e., iCloud, Carbonite, Dropbox) to store University information classified as Restricted.

v. University business should be conducted using University provided information technology systems, resources, and services.~~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.~~

vi. Accessing information and Records: Recognizing that not all circumstances can be anticipated, access to information and records residing on University information technology resources will ordinarily be governed by the following:

a) University Responsibilities: The University's obligations in relation to information technology resources include ensuring compliance with applicable laws and University policies and procedures, protecting the integrity and operation of its resources, and preserving information as necessary to protect the interests of the University and to enable it to satisfy these obligations. Accordingly, the University may access Rutgers-related electronic information on any device on which it is stored or may be accessed, and may access a user's records and information stored on University information technology resources systems or equipment for the above-mentioned purposes. Such access must be for specific, articulable reasons, must be appropriately circumscribed, and is limited to authorized personnel. The University understands that some users may have personal information and/or records on University systems and it respects the privacy of all users as to such information insofar as possible in complying with its above-mentioned obligations.

i. Standards for Accessing or Monitoring Information and Records: The University may access or monitor any/all information, records, record systems, and/or information technology resources in the following circumstances:

1. As necessary or appropriate to avert reasonably anticipated or already apparent threats or hazards to University information, records, or information technology resources. An example includes scanning to detect computer viruses;

2. As and when required by law or to comply with legal or contractual obligations of the University;

3. In connection with a legal proceeding in which the Oeffice of General Counsel is involved or an investigation conducted by or on behalf of the Office of Employment Equity or University Ethics and Compliance, for which access is necessary or appropriate;

4. When there is reasonable cause to believe that the employee has engaged in misconduct, has violated University policies or regulations, or may have used University resources improperly and that the information and records to be accessed or monitored are relevant to the misconduct or violation in question;

5. When the University otherwise has a legitimate need to access the information, records, or information technology resources.

Reasonable efforts will be made to notify the individual of the need for access to information or records in which the individual has a substantial personal interest in information or records stored on or transmitted through the University's information technology resources or other electronic system unless prohibited by law, inconsistent with University policy, or inconsistent with the University carrying out its normal operations and/or aforementioned obligations.

ii. Preserving and Protecting Records: In circumstances where the University determines that there may be a specific risk to the integrity or security of records, data, information, or information technology resources, the University may take measures to protect or preserve them. For instance, the University may take a "snapshot" of a computing account to preserve its status on a given date, copy the contents of a file folder, or restrict user access to information technology resources in whole or in part.

b) Employee Obligations

i. Standards of Employee Conduct for Accessing or Monitoring Records: It is a violation of this policy for an employee to monitor information technology resources or record systems or access records beyond the standards established within this policy. It is also a violation of the policy if the University has granted access to the employee (to monitor or access records or systems) and the employee has accessed or monitored records or record systems for purposes other than the purposes for which the University has granted access.

B. Violations

Employees who violate this policy may be subject to relevant institutional sanctions and discipline up to and including termination of employment.

~~**C.** Privacy:~~

~~The university recognizes that all members of the university community have an expectation of privacy for information in which they have a substantial personal interest. However, this expectation is limited 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. 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.~~

~~Reasonable efforts will be made to notify the user of the need for access to information in which he or she has a substantial personal interest 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:~~

~~i. 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 technologymisuse 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.

ii. Information requested pursuant to New Jersey Open Public Records Act which requires disclosure of electronic communication and other data on the university system subject to the exemptions within that Act. Such access is approved through the Office of the University Custodian of Records and all reasonable efforts are made to notify the user in question prior to the release of such information.

iii. Information required to comply with a valid subpoena, a court order or e-discovery. Such access is approved through the Office of General Counsel.

iv. 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.

v. 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:

i. Violators of this policy are subject to suspension or termination of system privileges and disciplinary action up to and including termination of employment.

ii. 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.

iii. It is a violation of this policy to unnecessarily delay acting on a directive to take corrective action to secure data or electronic credentials.