RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

Policy Name:	**Information Technology Privacy**					
Section #:	**70.1.7**	**Section Title:**	**Information Technology**		**Formerly Book:**	**N/A**
Approval Authority:	Executive Vice President Finance and Administration		**Adopted:**		**Reviewed:**	
Responsible Executive:	Senior Vice President and Chief Information Officer		**Revised:**			
Responsible Office:	Office of Information Technology (OIT)		**Contact:**	oitpolicies@rutgers.edu		

1. Introduction

Rutgers respects the privacy of its employees and seeks to foster a climate free from improper monitoring of employees and the *records* they create and use. Any expectation of privacy is limited by the university's needs to comply with applicable laws, protect the integrity of its resources, and the rights of all users. The University must, at times, access *records* or monitor *record systems* that are associated with its employees. Because employees occasionally use university resources for personal matters, *work-related records* and employee's *personal records* may be located in the same place.

2. **Reason for Policy**

The university cannot guarantee the privacy of any *records*, including the *personal records*, of any University employee. This policy defines the rights, responsibilities, and expectations of the University and its employees regarding the conditions under which they may access *records* and monitor *record systems*. It also governs those circumstances where information stored on the university's information technology system may be accessed.

3. **Who Should Read This Policy**

All members of the Rutgers University community.

4. **Related Documents**

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. Definitions

- Records
  For purposes of this policy, a record is any document, file, computer program, database, image, recording, or other means of expressing fixed information that is created, received, used, or maintained within the scope of University business or employment at the University or that resides on University-controlled premises or property. Records are either work-related or personal.

- Record Systems
  Record systems are ways of storing, disseminating, or organizing *records*. They include, but are not limited to, computers, computing networks, telephones lines, voice mail, fax machines, etc.

which are University property or are controlled by the University.

- Work-Related Records
  Work-related records are either *business records* or *scholarly records*.

- Business Records
  A business record is any *record* created, received, used, or maintained by an employee in the normal course of his or her professional responsibility or work for the University. This includes *records* relating to an employee's professional development. Examples of business records are drafts or final documents, including but not limited to underlying or supporting documentation, of the following:

  Budget reports;
  Documents shared with or generated by third parties, such as purchase orders, bills for services or contracts with vendors;
  Data sets that do not meet the definition of *scholarly records*, such as financial or enrollment data;
  Feasibility studies or utilization analysis;
  Attendance records, work schedules, or work orders;
  Architectural drawings;
  Correspondence or memoranda related to University business;
  Student grades;
  Meeting minutes;
  Departmental web sites or e-mail groups; and
  Committee reports.

- Scholarly Records
  According to the 1940 Statement of Principles on Academic Freedom and Tenure, American Association of University Professors' Policy Documents & Reports (1995 ed.), "Institutions of higher education are conducted for the common good and not to further the interest of either the individual teacher or the institution as a whole. The common good depends upon the free search for truth and its free expression." Scholarly records fall within the "Ownership of Copyrighted Works Created at or in Affiliation with Rutgers University". They include, but are not limited to, records related to information gathering, knowledge production, methodology, distribution, handouts, reading lists, research, research plans, notes, charts, articles, presentations, books, scholarly commentary, consulting works, films, music, choreography, works of art, and all other *records* produced in the role of scholar, researcher, teacher, or faculty member.

- Personal Records
  A personal record is a *record* that is created, received, used, or maintained by an employee for a purpose not related in any way to his or her work for the University.

6. Policy

This policy governs those circumstances in which the University, when not governed by external law, will monitor or access *records* and *record systems*.

Other than as authorized within this policy, neither the University nor any employee acting on behalf of the University will access *records* or monitor the content of *record systems* located on or in University-controlled premises, University property, cloud-based file storage systems, University computers, networks, offices, and telephones.

There are many laws that govern the maintenance and disclosure of records. Federal and state laws, for example, require the University to:

- protect from unwarranted disclosure certain *records* of patients (HIPAA), students (FERPA), or library patrons;
- disclose records (Freedom of Information Act, see http://afrotc.rutgers.edu/foia.html, the Open Public Records Act, see http://records.rutgers.edu/about-nj-open-public-records-

act/about-new-jersey-open-public-records-act-%E2%80%9Copra%E2%80%9D, subpoenas, etc.); and/or
- monitor *record systems*.

Accordingly, Rutgers cannot guarantee the privacy of any *records*, including the *personal records*, of any University employee.

7. Regulations

University Obligations

- Standards for Accessing or Monitoring *Records*

  As described below, the University has established general standards for accessing or monitoring all types of *records* (*business, scholarly*, and *personal*) or *record systems*, and additional standards for accessing or monitoring each type of *record,* or in connection with a legal proceeding in which the Office of General Counsel is involved for which access is necessary in connection with that proceeding.

- Standards that apply to all *business, scholarly*, and *personal records* or *record systems*

  The University may access or monitor all *records* (*business, scholarly*, and *personal*) or *record systems* in the following circumstances:

  i. When the University must monitor *record sys*tems to avert reasonably anticipated threats or hazards to those *record systems*. An example includes scanning to detect computer viruses.; or

  ii. When the University is required by law to access, monitor, or disclose *records* or *record systems*.

  Reasonable efforts will be made to notify the individual of the need for access to information in which the individual 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.

- Standards that apply to each type of *record* (*business, scholarly*, and *personal*)

  i. Business Records
  The University may access *business records* or monitor the *business record* content of *record systems* in the following circumstances:
  1. When the University has a legitimate business need to know or access the information contained in *business records*, and the employee who controls the *business records* or access to the *business records* (e.g. password, assigned office holder, etc.) is unavailable or unwilling to give consent to access.

  ii. Scholarly Records

  For the purposes of this policy the monitoring and access standards that apply to *scholarly records* (or *records* that are labeled as such) will also apply to *personal records*.

  iii. Personal Records
  The University and its employees will not access or monitor the content of *personal records* (including *scholarly records*), or monitor the *personal records* (including *scholarly records*) content of *record systems*, except under the following circumstances:

1. When an employee who controls *personal or scholarly records* (e.g. password, assigned office holder, etc.) is unavailable or unwilling to give consent to access and when it is necessary for the University to determine whether there are *business records* contained therein, the University will access such *records* only to the extent necessary; or

2. When there is reasonable cause to believe that the employee has engaged in misconduct and may have used University resources improperly.

- Preserving and Protecting *Records*
  In circumstances where the University determines that there may be a specific risk to the integrity or security of *records*, the University may take measures to protect or preserve those *records*. 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 access to a *record system*. The University may access or monitor preserved or protected *records* pursuant to Part III of this policy.

Employee Obligations

- Standards of Employee Conduct for Accessing or Monitoring *Records*
  It is a violation of this policy for an employee to monitor *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*) and if the employee has accessed or monitored *records* or *record systems* for purposes other than the purposes for which the University has granted access.

8. Violations

Violations of this policy will be considered misconduct on the part of the employee and will be subject to all relevant institutional sanctions up to and including termination of appointment.