RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

University Senate
Faculty and Personnel Affairs Committee

June 2, 2010

To: University Senate Executive Committee

From: Ann Gould and Paul Panayotatos, co-chairs, Faculty and Personnel Affairs

Re: University policy on e-mail privacy

In April 2009, Paul and I met with Roberta Leslie (Assistant Vice President Academic Affairs) and Shirley Weitz (Associate General Counsel) to discuss implementation of the E-mail privacy report to charge S-0310 passed by the Senate in October, 2004. We agreed during the meeting that the administration would work to sort out the status of the various existing policies and would get back to the Senate with proposed language to address the concerns raised in our report.

A link to the FPAC response to charge S-0310 is found at the following:

http://senate.rutgers.edu/fapcemailprivacy.html

Following our meeting, it became clear to Roberta and Shirley that many of the suggestions made in the original Senate report referred to language in policies and documents that were either no longer in operation or under revision. Working with Beckman Rich, Bernice Ginder, and Mike Gergel, the administration has now rewritten the **OIT Acceptable Use Policy** (OIT-AUP) to incorporate aspects of the original policy, the previously separate Acceptable Use Policy Guidelines, Section IV of the now defunct Standards for University Operations Handbook, as well as the email privacy concerns raised in the Senate report.

In the revised document, the administration attempts to spell out clearly the circumstances under which information technology resources may be accessed by university technicians and administrators (e.g. to comply with law, to ensure the integrity of university systems and resources, to protect the rights of other users and university property and operations). The administration feels that they have gone as far as they can to address privacy concerns without compromising university legal and fiduciary needs and responsibilities.

The administration forwarded the revised Acceptable Use Policy for consideration and comment by the FPAC before it is posted to the Rutgers University Library web pages. The new policy is appended to this memo. Here, I summarize the original Senate recommendation of 2004, the new OIT-AUP, and comments expressed by the FPAC at the April 2010 meeting and subsequent e-mail communications.

Senate response to S-0310:

When the FPAC originally looked into this matter in 2004, it became clear that compared to privacy statements published by 13 other Universities, policies on e-mail privacy at Rutgers were conservative and rigorous. The Rutgers policies did not, however, include language that 1) addressed user notification if e-mail or user files are examined; and 2) was explicitly applied to computer support units and systems administrators University-wide. In the 2004 Senate report, the following changes (underlined) were recommended:

1. To the **Acceptable Use of Network and Computing Resources**, Standards for University Operations Handbook:

   The University also reserves the right to examine material stored on or transmitted through its facilities if there is reason to believe that the standards for acceptable and ethical use have been violated, if required by law, or when it is necessary to maintain the performance, operation, or security of its systems.

2. To the 8th paragraph of the **Acceptable Use Policy for Computing and Information Technology Resources**, version posted on February 14, 2000:

   User files on University computer systems are kept as private as possible. Attempts to read another person's files will be treated with the utmost seriousness. The systems administrators will not override file protections unless necessary, and will treat the contents of those files as private information to the extent possible. Although all members of the community have an expectation_of privacy for information in which they have a substantial personal interest, this may be superseded by the University's requirement to protect the integrity of information technology_resources and the rights of all users as well as the need of the University to carry out its necessary operations.

   Thus the University reserves the right to examine material stored on or transmitted through its facilities if there is cause to believe that the standards for acceptable and ethical use are being violated by a member of the University community, if required by law, or when it is necessary to maintain the performance, operation, or security of its systems. All units that provide computer support and their system administrators are expected to adopt policies and procedures that reflect general expectations of users for privacy of items such as e-mail and other information with substantial personal content, while still providing access to the information and records needed for the University to function. Such inspections or monitoring will be conducted with advance notice to the user, unless, after consultation with University counsel, it is determined that notice would seriously jeopardize substantial interests of the University or of third parties. In such cases, notice will be withheld until the completion of the investigation or proceedings but will, nonetheless, be given a posteriori as soon as possible upon such completion.

3. To the **Guidelines for Interpretation and Administration of the Acceptable Use Policy for Computing and Information Technology Resources**, version posted on February 14, 2000, a new section on privacy was proposed:

   Privacy

All units of the University that provide computer support and their system administrators are subject to the policies and procedures of the present document that balances general expectations of privacy with the needs of the University to maintain the proper operation and security of its systems, to investigate possible violations, and to have access to information needed to function. Items in which individuals have a substantial personal interest, such as the content of e-mail and other correspondence, or material which under University policies are copyright by the individual, should normally be accessed only in circumstances such as the following:

- with the permission of the owner
- in situations where it is reasonable to expect that the owner would agree, e.g. when the owner is unavailable, and it is material that would normally be made available to others
- as necessary to investigate alleged violations of University policy for which probable cause has been affirmed by the supervisor of the investigator, or problems relating to the operation or security of University systems
- as required by law

Where permission is not given, both the scope of the information accessed and the number of people who see it should be limited to the minimum needed for the purpose. Where permission is not given, all accesses should be reported to the owner, unless, after consultation with University counsel, it is determined that notice would seriously jeopardize substantial interests of the University or of third parties. In such cases, notice will be withheld until the completion of the investigation or proceedings but will, nonetheless, be given a posteriori as soon as possible upon such completion.

The new OIT-AUP:

The new policy outlines standards for acceptable use of computer and information technology resources, including equipment, software, networks, data, and communication devises. The policy applies to faculty, staff, guests, and external parties.

1. **Part B. User responsibilities**. The OIT-AUP policy states that although "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...Rutgers does reserve the right to limit or restrict the use of its computing and 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."

   Outlined in Section B are the responsibilities of those who use computing and information technology resources for which they have access. These include:

   - Users may use only those computing and information technology resources for which they have authorization.

- Computing and information technology resources must be used only for their intended purpose(s).
- The access to and integrity of computing and information technology resources must be protected.
- Applicable laws and university policies must be followed including but not limited to respecting the copyrights and intellectual property rights of others.
- Users must respect the privacy and personal rights of others.
- Users are urged to take appropriate precautions such as safeguarding their account and password, taking full advantage of file security mechanisms, backing up critical data and promptly reporting any misuse or violations of this policy.

2. **Part C. Privacy. The OIT-AUP policy states that "**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."

Examples where information may be accessed include:

- Access to electronic records by technicians and administrators 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. Examples include (summarized here) i) emergency situations where technicians believe that a significant system or network degradation may occur; ii) instances where technicians may access neutral content such as system logs for the purposes of maintenance and troubleshooting; iii) instances where the University Information Protection and Security Office (IPS) may investigate reports of abuse or misuse of technology resources or may "observe, capture, and analyze network communications;" and iv) by user request.
- Information requested pursuant to the New Jersey Open Public Records Act. In such cases, all reasonable efforts are made to notify the user in question prior to the release of information.
- Information required to comply with a valid subpoena, subject to approval through the Office of General Counsel.
- Audits/investigations by University of governmental entities.
- The need to carry on with normal operations; for example, in the case of accessing records for diseased, incapacitation, or unavailable individuals.

2. **Part D. Technician and system administrator responsibilities**. These personnel are responsible for ensuring the integrity, security, and availability of the resources they are managing. They will not override system protections unless necessary and will treat the content as private information to the extent possible, carrying out duties while treating private information with the utmost confidence.

3. **Part E. Violations**. Violators are subject to suspension, termination of privileges, and other penalties. Violations by students may be referred to the Dean and handled through the University Code of Student Conduct. Violations by staff or faculty might include a referral to the individual's supervisor.

Considerations of the OIT-AUP by the FPAC:

The new OIT-AUP is commendable, clearly addressing in a single document privacy concerns as well as the responsibilities of those who use and administer Rutgers communication technology. The committee commented, however, that the new policy does not adequately address the following:

1) *Notice and permissions* (advance or after the fact) in cases where the privacy of individuals, who have an expectation of privacy in communications in which they have a substantial personal interest, is violated. Except where information is requested pursuant to the New Jersey Open Public Records Act, the policy contains no guarantee of notice or a promise that the scope of information accessed and the number of people who see it is limited to the minimum needed for the purpose.
2) Policy compliance by *all technicians and system administrators*, including not only those who manage university-wide systems but also those who administer local area networks within individual departments or programs. In many cases, technology privacy statements are not followed or are not in place. An effort to ensure that privacy violations do not occur at these levels is needed.
3) The explicit consequences of privacy violation for users of technology as well as systems administrators, technicians, guests, and external parties.

The FPAC appreciates the opportunity to comment on the new OIT-AUP, and Paul and I are happy to further discuss any privacy concerns with the administration.