Roosevelt University

Acceptable Use of Electronic Resources

Policy 7.1

Responsible Executive: Vice President of Technology & Chief Information Officer

Originally Issued: 4/10/2008

Revised:

Effective date: 4/10/2008

1. Contents

2. Reason for Policy

The purpose of the Acceptable Use of Electronic Resources Policy is to ensure an information infrastructure that promotes the teaching, learning, research, professional and community service missions of the University. Electronic resources are powerful enabling technologies for accessing and distributing the information and knowledge developed at the University and for facilitating communication and collaboration among members of the University community and with the world at large. As such, they are strategic technologies for the current and future needs of the University.

Electronic resources give individuals the ability to access and communicate sensitive information. This policy is designed to secure the rights of others to the privacy of their personal information.

Electronic resources are often shared resources. This policy provides the basis for equitable sharing of resources among members of the University community.

This policy explains the rights and responsibilities that users share in sustaining the electronic resources made available to them by the University. This policy will provide a reference for University students, faculty, staff, alumni, trustees, contractors, and authorized guests, and will communicate the roles and responsibilities of those charged with maintenance, operation and oversight of University electronic resources.

Within the University community each person will have differing purposes for accessing electronic resources, however, each person also has a shared responsibility to utilize those electronic resources in a manner consistent with the University's policies and procedures. In addition, users are bound by the requirements of local, state, federal, and international laws and contractual commitments.

By striving for compliance, the University can assure its ability to provide, maintain and protect the confidentiality, integrity and availability of its data, systems, services and facilities.

3. Entities Affected by this Policy

3.1 Individuals Covered

This policy applies to all persons accessing or using University electronic resources. This includes University students, faculty, emeriti faculty, staff, alumni, trustees, contractors, agents, and all other persons authorized for access or use privileges by the University, commonly referred to as *users*.

3.2 Resources Covered

Electronic resources covered by this policy include, without limitation:

- all University owned, operated, leased or contracted computing, networking, telephony and information resources, whether they are individually controlled, shared, stand alone or networked;

- all University information maintained in any electronic form and in any medium regardless of where it is stored;
- all University voice and data networks, telephony systems, telecommunications infrastructure, communications systems and services, and physical facilities including all hardware, software, applications, databases, and storage media; and
- all creation, processing, communication, distribution, storage, and disposal of information by any combination of University electronic resources and non-University resources.

4. Policy Statement

4.1 Use of Electronic Resources

4.1.1 Confidential Data

All users are to utilize all appropriate precautions to maintain the accuracy, integrity and confidentiality of confidential data, ensure that no unauthorized disclosures occur, refrain from sharing confidential information with anyone not authorized to access it, and comply with all University, local, state and federal policies and laws with respect to confidentiality of information, such as the Family Educational Rights and Privacy Act (FERPA).

4.1.2 Expectation of Privacy

The University provides electronic resources to users to facilitate their advancement of the University's mission. The University will not routinely monitor an individual user's electronic data, software, or communication files. However, users should have no expectation of privacy in network activity or files stored on University equipment. Electronic messages (including email), and files that are transmitted, received, or stored with the use of the University's resources, whether or not saved or deleted, are the property of the University.

4.1.3 User Rights

All users:

- are granted access to and permitted use of the University's electronic resources for specific purposes based on the users' particular roles;
- have the authority to read, write, edit, or delete information in files or databases as established by the designated owners of the information;
- are provided access to the University's on-campus data network.

4.1.4 User Responsibilities

Users shall:

- share confidential information with any other person only after ascertaining that he or she has approved access to the data in question;

- be responsible for the security and integrity of information stored on his or her system, including:
    - making regular backups of information and files,
    - controlling and securing physical and network access to electronic resources and data,
    - properly logging out of sessions,
    - monitoring access to their accounts (If users suspect that their access codes have been compromised or that there has been unauthorized activity on their accounts, they are to report it and change access codes immediately), and
    - ensuring that software that protects against viruses, spyware, and other "malware" is installed, activated, and regularly updated on their systems;
- show a valid University ID to obtain access to computer labs/facilities, including those in libraries;
- choose a password that is consistent with the University's password policy and guard the security of that password;
- be responsible for all activity that occurs on their computer accounts;
- understand that it can be dangerous to share access codes with anyone;
- use only the access codes and privileges associated with their computer account(s) and utilize those account(s) for the purposes for which they were authorized;
- respect and honor the rights of other individuals, with regard to copyright and intellectual property, freedom from harassment, and use of electronic resources.

4.1.5 User Restrictions

Users may not:

- comment or act on behalf of the University over the Internet, including email, without the authority to do so;
- make use of accounts, access codes, privileges or electronic resources to which they are not authorized;
- send email chain letters or unauthorized mass mailings;
- alter the source address of messages, or otherwise forge email messages;
- tamper with, modify or alter restrictions, or protection placed on their accounts, the University system, or network facilities;
- use the University's Internet access in a malicious manner to alter or destroy any information available on the Internet, or on any network accessible through the Internet, that they do not own or have explicit permission to alter or destroy;
- introduce, create or propagate computer viruses, worms, Trojan Horses, or other malicious code to electronic resources within or outside of the University;

- damage computer and network systems, obtain extra electronic resources or gain access to accounts for which they are not authorized;
- eavesdrop or intercept transmissions not intended for them;
- physically damage or vandalize electronic resources;
- attempt to degrade the performance of the system or to deprive authorized users access to any University electronic resources;
- use University systems to relay mail between non-University email systems;
- engage in activities that harass, degrade, intimidate, demean, slander, defame, interfere with, or threaten others;
- modify or remove computer equipment, software, or peripherals that are part of the University's computer and network resources without authorization from the Vice President for Technology and Chief Information Officer;
- install network or computing devices that are not authorized by the Vice President for Technology and Chief Information Officer or his/her designees. Such devices include but are not limited to wireless access points, network server hardware and software, and network devices such as hubs, routers, and switches. Unauthorized equipment is subject to confiscation.

4.1.6 University Processes

4.1.6.1 Data Backup and Recovery

Electronic data, software, and communications files stored on central servers are copied to backup media and stored. Backups are intended to enable recovery of data in case of major system failures; however, individual email messages may be recovered. Users are responsible for backing up their own personal computer data.

4.1.6.2 Monitoring of System Activity

All activity on systems and networks may be monitored, logged, and reviewed by system administrators or discovered in legal proceedings. In addition, all documents created, stored, transmitted or received on University computers and networks may be subject to monitoring by systems administrators.

4.1.7 University Rights

4.1.7.1 Accessing Electronic Content

The University has the right to access, monitor and disclose the contents and activity of an individual user's account(s) and to access any University-owned electronic resources and any non-University-owned electronic resource on University property that is connected to University networks. This action may be taken:

- to maintain the network's integrity and the rights of others authorized to access the network,

- if the security of a computer or network system is threatened,
- if misuse of University resources is suspected,
- if the University has a legitimate business need to review such files, or
- when compelled by court order.

This action will be taken with written authorization from the Vice President for Technology and Chief Information Officer and the designated responsible administrator (as defined in the "Enforcement" section of this document).

4.1.7.2 Monitoring and Blocking Content

The University has the right to monitor or block electronic content in three ways. The University may:

- employ what are commonly called "SPAM blockers" to eliminate messages from known purveyors of junk email;
- block access to Web sites that are known to spread viruses, spyware, adware, or other malicious content;
- block or limit access to resources that illegally distribute music, video, or other content.

4.1.7.3 Controlling Network Bandwidth

The University may also control the amount of network bandwidth available at any given time for specific types of applications or classes of users. Examples include allocating increased bandwidth for resident students and student laboratories during hours when offices are not typically open and classes are not in session, and constraining the bandwidth allocated for streaming audio and video if there is no demonstrated academic application for the service.

4.1.8 University Restrictions

University employees, including personnel in the Division of Information Technology, may not:

- monitor the content of an individual user's electronic data, software, or communication files without authorization as outlined in this policy;
- inspect individual user's files, diskettes, tapes, and/or other computer-accessible storage media without following the processes outlined in this document;
- monitor or block electronic content except under the conditions specified in this document.

4.1.9 Copyrights and Licenses

Software may not be copied, installed, or used on University electronic resources except as permitted by the owner of the software and by law. Software subject to licensing must be properly licensed and all license provisions (including installation, use, copying, number of simultaneous users, terms of the license, etc.) must be strictly observed.

All copyrighted information, such as text and images, retrieved from electronic resources or stored, transmitted or maintained with electronic resources must be used in conformance with applicable copyright and other laws. Copied material used legally must be properly attributed in conformance with applicable legal and professional standards.

4.1.10 Non-University Use

Computer and network resources are provided to support University functions. The University permits the use of its computer and network resources for limited personal activities, but personal use must conform to University policies and must not interfere with the primary goals of supporting teaching, learning, research, and service.

Users may not use electronic resources for:

- private business or personal commercial enterprise;
- compensated outside work, except as authorized by the Graduate Dean and Vice Provost for Research pursuant to an approved grant or sponsorship agreement;
- the benefit of organizations not related to the University, except those authorized by the vice president or dean for the University-related service;
- partisan political activities;
- lobbying activities not approved by the Vice President for Governmental Relations.

University electronic resources may not be used for commercial purposes, except as specifically permitted under other written policies of the University or with the written approval of Senior Vice President, Finance & Operations and CFO. Any such commercial use must be properly related to University activities and provide for appropriate reimbursement to the University for taxes and other costs the University may incur by reason of the commercial use.

Users are also reminded that the ".edu" domain on the Internet has rules restricting or prohibiting commercial use; activities not appropriate for the ".edu" domain that otherwise are permissible within the University's electronic resources should be performed on other domains.

4.2 **Policy Enforcement**

4.2.1 Responsible Administrators

The University designates “responsible administrators” for cases involving possible misuse of electronic resources or the inspection of email or other user files. The responsible administrators are: the President for cases involving members of the Executive Council, the Provost and Executive Vice President for cases involving academic deans and faculty, the Vice President for Human Resources for cases involving staff and administrators, and the Vice President for Enrollment and Student Services for cases involving students.

4.2.2 Suspected Misuse

In any and all cases where acceptable use comes into question, management of the University reserves the right to determine what is appropriate and acceptable and what is not. This section outlines the procedures that will apply in the case of suspected violations of University policies.

4.2.3 Reporting Misuse and Cooperation with Officials

All users are encouraged to report to the Vice President for Technology and Chief Information Officer, or through procedures outlined in the University's Whistle Blower Policy, any suspected violations of University computer policies. Users, when requested, are expected to cooperate with University officials in any investigation of system abuse. Failure to cooperate may be grounds for cancellation of access privileges, or other disciplinary actions.

4.2.4 Disciplinary Action

If University officials have sufficient evidence of misuse of computing resources, and if that evidence points to the computing activities or the computer files of an individual, they shall pursue one or more of the following steps, as appropriate, to protect other users and electronic resources.

- Provide notification of the investigation to the designated responsible administrator; the appropriate vice president and, if applicable, dean; and the Vice President for Technology and Chief Information Officer. This step should be taken in every case.
- Temporarily suspend or restrict the user's computing privileges during the investigation.
- If necessary, with written authorization from the designated responsible administrator and the Vice President for Technology and Chief Information Officer, inspect the user's files, diskettes, tapes, and/or other electronic media.
- Refer the matter for possible disciplinary action through the University's established procedures.

The University retains final authority to define what constitutes proper use and may prohibit or discipline use the University deems inconsistent with this or other University policies, contracts and standards. The University also reserves the right to change the policies, information, requirements and procedures announced in this policy at any time. Changes required by University contractual commitments shall become effective and binding upon users upon execution of any such contract by the University. A user shall be deemed to have accepted and be bound by any change in University policies, information, requirements or procedures if such user uses electronic resources at any time following announcement or publication of such change.

4.3 **Individual Unit Policies**

Individual units within the University may define supplemental policies or conditions of acceptable use for electronic resources under their control with the written review and

approval of the Vice President for Technology and Chief Information Officer. These additional policies or conditions must be consistent with this policy but may provide additional detail, guidelines and/or restrictions. This policy will supersede any inconsistent provision of any unit policy or condition.

4.4 Warranties and Liabilities

The University makes no warranties of any kind, whether expressed or implied, for providing electronic resources to any user. The University bears no responsibility for the accuracy or quality of information or services obtained through electronic resources. The University will not be responsible for any damages suffered from the use of University electronic resources, including loss of data, delays, service interruptions, missed deliveries or failed deliveries. Use of University electronic resources is at the user's own risk, including the reliability or security of information obtained, transmitted, received, or stored.

This policy document is based, in part, on the acceptable usage policy documents of Stanford University and Marquette University.

5. Web Address

www.roosevelt.edu/acceptableUse

6. Related Documents

Code of Student Conduct

Employee Professional Code of Conduct

Confidentiality Policy

7. Implementation

The Vice President for Technology and Chief Information Officer is responsible for developing procedures to implement this policy.

8. Online Resources and Forms

None.