

## Acceptable Use Policy – Computing and Information Technology Resources

Originator: Vice Provost, Information Technology Services

Date: April 2008

Policy #04-1 (Revised)

### Background:

The University has a responsibility to protect the University of Rhode Island and its information technology (IT) resources from illegal or damaging actions, intentional or unintentional, on the part of individuals or computer systems. IT resources include data and equipment such as personal computers, graphics devices, printers, and multi-user processors. IT resources also include University connectivity to electronic information such as computer and telephone networks, dial-up lines, and wireless access. The University has an established culture of openness, trust and integrity that guides the restrictions contained in this policy.

Participation in a community of networked computers and users requires adherence to an ethical code of conduct not unlike society at large. The fact that an activity is technologically possible does not legitimize its use.

The University provides IT resources for the shared and responsible use by members of its community who are, in turn, expected to use them in an efficient, ethical, professional, and legal manner consistent with the University's objectives. Inappropriate use exposes the University and community members to risk of data loss, unintended disclosure as well as other legal and liability issues.

### Applicability:

This policy applies to all users of University IT resources including faculty, staff, students, and guests. It also applies to technology resources administered by individual departments as well as centrally, to personally owned computers and devices connected to the campus network by wire as well as through wireless, and to off-campus computers that connect remotely to the University as well as on-campus computers.

### Purpose:

The purpose of this policy is to articulate the acceptable use procedures for users of information technology resources provided by the University of Rhode Island. Individual departments and units may have additional policies specific to their unique missions and operational considerations.

### General Provisions:

#### *Computer/Network Accounts and Use*

No one shall use another individual's user ID or credentials to access University technology resources unless explicitly permitted to do so by the owner of the ID or credentials, or an appropriate University office. Such access should be granted only when necessitated by the efficient conduct of University business and when the person to whom access is granted has similar access to non-electronic information. Individuals who obtain access under these conditions may use it only for the intended purpose for which it was granted and are responsible for policy violations. In any other case of

persons sharing a user ID or access credentials, both the owner of the ID and the individual granted access can be held responsible for policy violations.

#### *Resource Use*

The University expects that users respect the finite capacity of IT resources and requires them to avoid excessive use of those resources. The University strives to share its IT resources in an equitable manner according to the needs and resources of the University community. The University, through Information Technology Services, may dynamically establish limits to IT resources if cost or demand for such resources exceed capacity or University priorities change.

Among other inappropriate activities, individuals shall not use University information technology resources to libel, slander, or harass others, violate others' privacy, use network scanning programs without permission, attempt entry to non-public hosts, tamper with security measures or with the ability of others to make use of those resources. The University may take immediate action to restore the proper functioning of University systems if it determines that such use is in progress.

#### *Unauthorized Access*

Users have a responsibility to maintain and protect the integrity of all shared University information technology resources. Unauthorized access is prohibited. Attempts to breach the security of systems and data will result in disciplinary actions and possible criminal prosecution. Users must request authorization to resources that may be accessible but are not clearly marked as authorized for access.

#### *Copyrighted Materials Usage*

US law protects copyrighted materials, which must be used lawfully. The University prohibits using, copying, or distributing copyrighted materials on University information technology resources unless such use is covered by federal fair use guidelines or permission has been granted by the copyright owner.

#### *Personal Use*

##### *University Employees:*

The University provides IT resources and services to employees of the University for business use. Employee personal use that is not part of legitimate University business is permitted when it is not excessive, does not interfere with normal business activities, and when it otherwise complies with this policy. Prohibited personal use for employees includes, but is not limited to, political campaigning, solicitation, unauthorized financial gain, or conducting business that has no official relationship with the University. Additional limits may be imposed by a supervisor, appropriate office, applicable University policies, or state laws.

##### *University Students:*

Student personal use must adhere to the provisions of this policy and to the University of Rhode Island Student Handbook.

### *Security and Privacy*

The University employs various measures to protect the security of its information technology resources and of user data and accounts. Users have a reasonable expectation of unobstructed use of information technology resources, certain degrees of privacy, and protection from abuse and intrusion. Security precautions cannot always guarantee users' security or privacy, however. Users should exercise caution in using University resources to store or transmit confidential data.

### *Disclosure*

In disciplinary proceedings, the University, at its discretion, may submit results of investigative actions to authorized University personnel or law enforcement agencies. Suspect communications created with University information technology resources may also be subject to Rhode Island's Public Records Statutes to the same extent as hardcopy communications. In addition, users may be subject to legally binding demands such as subpoenas and search warrants. Ultimately, it is the University that owns University IT resources, not employees who use them.

### *Inspection of Electronic Information*

Information located on University IT resources is subject to examination, as deemed necessary, to maintain or improve functioning of technology resources, investigate alleged violations of University policies or federal and state laws, and to comply with or verify compliance with federal or state laws.

The University reserves the right for designated technology administrators to access users' stored information during normal system performance monitoring and maintenance, and when investigating cases of computing abuse. Such access shall be approved by the Vice Provost of Information Technology Services in consultation with the Provost and General Counsel when necessary.

### Policy Enforcement

Disciplinary measures for violations are normally applied by the University office or department appropriate to the violation. Violators may be subject to additional penalties and disciplinary actions by the University and are also subject to international, federal, state and local laws governing interactions that occur on information technology systems and the Internet. The University may restrict or deny access to information technology resources temporarily or permanently, prior to the initiation or completion of disciplinary procedures when it appears necessary to protect the integrity, security, or functionality of the University's IT resources.

The University shall restore privileges as expeditiously as possible. Anyone who has personal data located on or equipment connected to a University information technology resource to which access has been blocked either temporarily or permanently can request from the office handling the case that the data be removed, transmitted, or copied in a timely manner.

### Impact on Other Policies

None known to date.

Effective Date: *Interim or Permanent*  
April 2008 [Permanent]

Review

This policy should be reviewed as new developments or provisions necessitate.

Policy Contact

ITS Security Architect

Authority

Vice Provost, Information Technology Services  
Faculty Senate  
University President