Rice University Policy No. 832

APPROPRIATE USE OF INFORMATION TECHNOLOGY

I. General Policy

Rice University provides a variety of computing and network resources to the Rice community. These resources are to be used in a manner consistent with federal and state laws and regulations, university policies and specialized policies and guidelines created by the Office of Information Technology (OIT).

Rice values freedom of expression, the diversity of values and perspectives and the protection of sensitive University and personal data for all members of the Rice University community. All Rice University users are responsible for compliance with all Rice policies, contractual obligations, and federal and state laws and regulations, including protecting the sensitive personal information of others.

II. Definitions

Rice-managed technology: Any hardware, software, data or services purchased or contracted by or through Rice University, including Rice networks and systems.

Rice data: Any data connected to Rice University functions that is the product of Rice University employees or contractors and others acting on its behalf.

Rice user: Any person connected to or using Rice networks or systems, or having legitimate access to Rice data through any device.

III. Elaboration of Policy

Acceptable Use

Use of all University information technology and digital resources must be consistent with the University's research, educational and outreach mission, University policies and procedures, and any legal or contractual requirements of the University (including license agreements and terms of service). In addition, Rice users are responsible for using Rice-managed technology and Rice data in a responsible manner. Use of University networks and systems unrelated to the University's mission must be limited in time and scope and must not interfere with University functions or operations or employee duties.

Prohibited Uses

Use of the University's information technology and digital resources shall not violate applicable federal, state, and local laws, including U. S. copyright law, or applicable University policies, and, if travel is involved, the laws of the relevant nation or state (including U.S. export control requirements). Individuals should not use University technological resources for partisan political purposes.

Any communication, which is defamatory, harassing, interferes with other uses of University resources or constitutes an improper disclosure of protected University or sensitive personal data is prohibited.

Access to information

Rice University may be required by law to access and disclose information from computer and network users' accounts, or may find it necessary to do so in order to investigate potential violations of law or University policy, protect Rice's legitimate interests, uphold contractual obligations, or comply with other applicable Rice policies.

Rice may also be required to access information to diagnose and correct technical problems. Rice reserves the right to limit access to its networks or to remove material stored or posted on Rice computers when it appears that applicable Rice policies, contractual obligations, or federal or state laws are violated.

Protection of University Resources and Data

Users of University information technology and digital resources are responsible for protecting University data (including sensitive personal data), including its confidentiality, integrity, access, retention and disposal. Such protection includes, but is not limited to:

- Complying with approved password/credential management procedures to safeguard Rice accounts.
- Limiting, with only de minimus non-Rice activities, use of the resources to activities supporting Rice's mission and following defined procedures and use descriptions.
- Protecting Rice data by observing security procedures, appropriately classifying data and managing the data in the appropriate manner per the classification requirements.
- Complying with protections for treatment of sensitive personal data and following all federal, state and local laws and Rice policies, procedures, codes of conduct and rules while using Rice managed technology or Rice data.
- Being an informed user of email accounts to minimize exposure to phishing and other malware attempts.
- Reporting any suspected fraudulent or inappropriate activity, any violation of security or appropriate use protocols or suspicious or unusual activity associated with the use of Rice managed technology or Rice data to violation@rice.edu.
- Being informed and knowledgeable regarding the use of the IT resources provided by Rice and acquiring adequate training prior to use.

IV. Exceptions

All exception requests must be submitted in writing to the Vice President for Information Technology/Chief Information Officer and must follow the University exception standards defined in Rice Policy 101.

V. Policy Maintenance and Periodic Review

The Office of the Vice President for Information Technology/Chief Information Officer will review this and all IT policies on a regular basis.

VI. Cross References to Related Policies

University Policy 101 University Policy Development and Management
University Policy 807 Partisan Political Activities
University Policy 808 Protection of Personally Identifiable Information

VII. Responsible Official and Key Offices to Contact Regarding the Policy and its Implementation

Responsible Official: Vice President for Information Technology/Chief Information Officer
Other Key Offices: Chief Information Security Officer

VIII. Procedures and Forms

Specific Guidelines for the use of Information Technology are available at this link.
Other procedures and forms may be accessed on the OIT website, available at this link.

*Signed David W. Leebron*_____
David W. Leebron
President

Policy History
Revised: March 17, 2017; February 15, 1999; and 1993
Clerical Change: April 25, 2017 (updated links in Section VIII, and corrected obvious typo in III, para 3)