Policy for the Acceptable Use of Information Technology

Updated April 20, 2018

1. Title

Acceptable Use of Information Technology

2. Audience

This policy applies to all users of computing resources provided by the University of Redlands. Individuals covered by the policy include (but are not limited to) Redlands faculty, adjunct faculty, and visiting faculty, staff, students, alumni, guests, vendors or agents of the administration, external individuals and organizations accessing network services via Redlands' computing facilities.

Computing resources include all University owned, licensed, or managed hardware, software, cloud services, and University managed Social Media accounts and platforms, and the use of the University network via a wired or wireless connection, regardless of the ownership of the computer or device connected to the network.

These policies apply to technologies administered in individual departments, the resources administered by central administrative departments (such as the University Library and Information Technology Services), personally owned computers and devices connected by wire or wireless to the campus network, and to off-campus computers that connect remotely to the University's network services.

3. Introduction

As a member of the University community, you are provided with the use of scholarly and/or work-related tools, including access to the Library, to certain computer systems, servers, software and databases, to cloud services, to the campus telephone and voice mail systems, and to the Internet. You have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy (which may vary depending on whether you are a University employee or a matriculated student), and of protection from abuse and intrusion by others sharing these resources. You can expect your right to access information and to express your opinion to be protected as it is for paper and other forms of non-electronic communication.

In turn, you are responsible for knowing the regulations and policies of the University that apply to appropriate use of technology resources. You are responsible for exercising good judgment in the use of these resources.

As a representative of the University of Redlands community, you are expected to uphold the University's good name in your interactions with those outside the University.

4. Purpose

The computing resources at the University of Redlands support the educational, instructional, research, and administrative activities of the University and the use of these resources is a privilege that is extended to members of the Redlands community. As a user of these services and facilities, you have access to valuable University resources, to sensitive data, and to internal and external networks. Consequently, it is important for you to behave in a responsible, ethical, and legal manner.

In general, acceptable use means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements. If an individual is found to be in violation of the Acceptable Use Policy, the University will take disciplinary action, including the restriction and possible loss of network privileges. A serious violation could result in more serious consequences, up to and including suspension or termination from the University. Individuals are also subject to federal, state and local laws governing many interactions that occur on the Internet. These policies and laws are subject to change as state and federal laws develop and change.

This document establishes specific requirements for the use of all computing and network resources at the University of Redlands.

5. Policy

- **Compliance**
  All users of the University of Redlands information technology resources agree to comply and be subject to this Policy for the Acceptable Use of Information Technology (hereafter referred to as "policy"). The University of Redlands reserves the right to limit, restrict, or extend computing privileges and access to any user as the University deems appropriate.

- **Limitations**
  The University of Redlands' information technology resources are to be used only for the University of Redlands' activities for which they are assigned or intended. When accessing any remote resources utilizing University of Redlands' information technology resources, users are required to comply with both the policies set forth in this document and all applicable policies governing the use and access of the remote computer system.

- **User Accounts**
  User accounts are designed only to establish a system control mechanism for user identification and to afford users a physical location where they can store relevant academic and administrative data. At no time should user accounts be used to execute any computer software or computer programs other than those programs specifically granted and offered for user execution by the University of Redlands. Additional licensed software may be installed on the University-supplied computers in support of research, teaching, and administrative activities. Users should contact Technology Support Services regarding software compatibility, hardware requirements, etc. In general, this notification practice will ensure that the installation of the new software will not compromise the integrity of either the user's computer or information technology resources. All users are responsible for both the protection of their user account password and the data stored in their user account. Users are prohibited from sharing their user account password with anyone at any time. It is recommended that users change their user account password periodically to help prevent unauthorized access of their account. Any suspected unauthorized access of a user account should be reported immediately to the Office of Information Technology Services. For faculty, staff, and administrators, user accounts are deactivated when the user's employment ends. Users will be unable to access any resources (email, cloud storage, etc.) associated with the account. For students, user accounts are deactivated six months following the student's graduation or withdrawal from the University. All data, files and messages are deleted when the user account is deactivated.

- **Email Accounts**
  The University supplies all Faculty, Staff, Administrator and Student users an email account for the use of University activities. ITS strongly encourages users to use a personal email account for personal activities (such as banking, shopping and personal correspondences). The use of personal email from the University network is governed by this policy.
  Not all electronic information is protected communication under legal definitions, and the email messages are potentially subject to discovery or a subpoena request during legal actions.

- **Social Media**
  Use of social media platforms may be part of an employee's work responsibilities. It is important to remember that by identifying oneself as an employee of the University of Redlands, we become representatives of the University and are responsible for posted content.
  You may wish to use social media in your personal life outside of work time as well. This policy does not intend to discourage nor unduly limit your personal expression or online activities.
  However, you should recognize the potential for damage to be caused (either directly or indirectly) in certain circumstances via your personal use of social media when you can be identified as a University employee. Accordingly, you should comply with this policy to ensure that the risk of such damage is minimized.
  You are personally responsible for the content you publish in a personal capacity on any form of social media platform.

- **Ownership**

Users can expect exclusive use of all data, information, files, or messages stored in their user accounts. University of Redlands reserves the right to inspect and disclose contents of data and email when an official investigation is triggered by indications, subject to University policies, of misconduct or misuse.

- **Data Security**
  University of Redlands strives to provide reasonable security against unauthorized intrusion and damage to data, information, files, and messages stored on its information technology resources within institutional priorities and financial capabilities. Users are strongly encouraged to back up their data on a regular basis. If a user needs to recover data after an accidental loss, Information Technology Services staff should be contacted. Every reasonable attempt will be made to recover the lost or corrupted data.
  Storage of any financial information, student information or any other business record must be in accordance with University Data Guidelines and stored on ITS approved platforms only.
  Because of variables associated with the digital storage of data, however, the University of Redlands cannot guarantee full restoration in every instance. The University of Redlands cannot be held accountable for unauthorized access by other users, nor can the University guarantee data protection in the event of media failure, fire, criminal acts, or natural disaster.

- **Copyright Infringement and Digital Piracy**
  Respect for the intellectual work and property of others has traditionally been essential to the mission of academic institutions. As members of the academic community, the University of Redlands values the free exchange of ideas. Just as the University of Redlands does not tolerate plagiarism, it does not condone the unauthorized copying of software, including programs, applications, operating systems, and databases. Use of University technology resources for illegally downloading copyright protected materials, such as music, movies, video games and computer software, is strictly prohibited.

- **Liability for Errors**
  The University of Redlands makes a reasonable effort to maintain an error-free hardware and software environment for its authorized users. Nevertheless, it is impossible to ensure that hardware or system software errors will not occur. The University of Redlands presents no warranty, either expressly stated or implied, for the services or access provided to its authorized users. The University of Redlands is not responsible for damages resulting from the direct or indirect use of its information technology resources.

- **Network Monitoring**
  Every computer attached to the campus network is subject to traffic monitoring in order to ensure effective use of available bandwidth and to detect and correct network problems as they occur, thereby ensuring the continued stability of the campus-wide computing environment.
  ITS will also monitor the network to ensure that the computing environment is safe and secure.
  Even with the University's right to monitor, users should continue to expect that their data, files, and email would remain accessible only by them. However, all files stored in user accounts are subject to internal inquiry should cause arise from reported misuse or abuse of information technology resources, and user accounts are potentially subject to discovery or subpoena requests that may result during legal actions. User data may be scanned for Personally Identifiable Information or other University business records.
  System monitoring is a mechanism for observing network usage and traffic, not a method for accessing private information or reviewing the content of the files.

- **Specific Issues of Responsible Use**
  In addition to the issues of responsible user behavior already described in this policy, the following more specific practices applicable to all University of Redlands' users are prohibited:
    - Access, use, inspection, or modification of data or functions that are neither allotted nor authorized as a part of the user's account
    - Accessing or attempting to access University servers, cloud systems or other computing resources from within the University computing environment without expressly granted authorization
    - Installing or executing unauthorized or unlicensed software on any computer resource
    - Access or use of another user's account and the data contained in that account without specific authorization
    - Theft, destruction, or deleting of data on University-owned computer resources

- Physical or electronic interference with other computer systems
- Dissemination or distribution of a user account password to any other person
- Cyberbullying of other University community members or from University resources
- Additionally, all employee account holders will be required to complete annual information security training. Failure to complete the training by the specified deadline may result in suspension of the account

This is not an all-inclusive list. Therefore, other University policies may also apply.

6. Summary

The use of information technology resources within the University is becoming pervasive and an essential aspect of almost all of the University's endeavors. This policy statement is intended to provide guidance in the acceptable use of information technology resources. Each member of the University community must assume responsibility for his or her own behavior while utilizing these resources and should accept that the same ethical behavior that guides in our non-computing environments should also serve as a guide in our computing and networking environment.

Information technology resources are of significant value, and their abuse can have a negative impact on other users and the mission of the University as a whole. Depending upon the severity of infraction, non-compliance with the guidelines presented in this policy may result in loss of University of Redlands computer and network access privileges or may result in criminal prosecution and/or termination.