



## **Policy for the Responsible Use of Information Technology**

Last Update: November 2, 2004

The rapid emergence of the Internet, the growth of the World Wide Web, the incorporation of electronic mail in various curricula, and the availability of distributed information resources across a common network has caused the University of Redlands to examine the many issues involved in the responsible use of information technology using institutional resources. This policy is the product of that examination, and adherence by all University of Redlands faculty, administrators, staff, and students is required. Adherence to this policy will promote a computing environment that will perpetuate the University of Redlands' academic, research, and service mission. It is imperative that the campus community accedes that technological resources require responsible behavior from all of its users. Simply stated, the continued and efficient accessibility of information technology resources is the responsibility of the entire University community.

### **Purpose**

Information technology resources, which include hardware, software, network, applications, systems, and data, play an increasingly important role in education, research, and administration at University of Redlands. This policy is designed to define the appropriate and responsible use of the campus computing and network facilities. In support of its mission of education, research, and public service, the University of Redlands seeks to provide its faculty, administrators, staff, and students with the broadest possible access to information technology resources consistent with institutional priorities and financial capabilities and subject to the normal principles of legal and ethical behavior that govern the University generally.

### **Scope**

Since technology now serves as a gateway to information and interaction for research and education, this policy applies to everyone at the University of Redlands who utilizes any University information technology resources.

### **Compliance**

All users of the University of Redlands by using any information technology resources agree to comply and be subject to this Policy for the Responsible 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 1) to establish a system control mechanism for user identification and 2) 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 desktop/laptop computers in support of research, teaching, and administrative activities. Users should contact User Services/Help Desk 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 anytime, thereby granting unauthorized access to University of Redlands' information technology resources. It is recommended that users change their user account password periodically to help prevent compromise and unauthorized access of their user account. Any suspected unauthorized access of a user account should be reported immediately to the Office of Information Technology Services. User accounts are deactivated and removed from further access and use when the user's affiliation (e.g., employment, matriculation, current enrollment, etc.) is terminated. All data, files, or messages are deleted from user accounts when accounts are deactivated.

### **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 electronic messages 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 backup 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.

Because of variables associated with the magnetic storage of data, however, the University of Redlands cannot guarantee full restoration in every instance. The University of Redlands can not 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.

### **Electronic Mail (e-mail)**

Not all electronic information is protected communication under legal definitions, and the e-mail messages stored in files are potentially subject to discovery or a subpoena request during legal actions.

### **Software Copying**

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.

### **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.

Even with the University's right to monitor, users should continue to expect that their data, files, and e-mail 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.

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
- 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

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

### **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 responsible 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 serve as guides in our non-computing environments should also serve as guides 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.