507 POLICY - Information Technology Services (ITS)

507.1 Statement of Policy

Redlands Community College ("Redlands") has made significant investments in telecommunications technology to promote and support the exchange of information in furtherance of the mission and goals of the College. Use of these resources must be consistent with the mission, goals, and policies of the College and must be in compliance with applicable law. Every computer account, user account, e-mail mailbox, phone extension, and voicemail mailbox (collectively, "Account") issued by the College remains the property of the College.

507.2 Applicability of Policy

This policy applies to all use of the College telecommunications technology, including, but not limited to, servers, desktops, laptops, telephones, printers, switches, firewalls, and any other network, equipment, hardware device and software that could be utilized in any manner and for any purpose (collectively, the "Redlands Enterprise Network" [REN]) and Internet access through the REN for any purpose.

507.3 Authorized Users

The authorized users of the REN are those persons who are members of the College community or who have specific authorization to use the REN. For purposes of this policy, the students, employees, and staff, including contractors, of the College are considered to be the members of the College community. The person to whom the Account is issued is responsible for the Account and its use. This responsibility continues until the person is no longer a student, employee, or contractor of the College, at which time all rights regarding the Account are terminated. College Alumni are the exception to this policy. Alumni shall retain access to their College-issued e-mail mailbox, which requires a limited access Account. Using another person's Account or allowing someone else to use an Account makes both parties subject to disciplinary action. Guidelines for keeping an Account secure are published in the Procedures section of the Policies and Procedures Manual.

507.4 Objectives of ITS

- Establish policies and procedures for appropriate use of campus technology.
- Strategic planning, oversight and direction of Redlands Information Technology infrastructure, resources and services.
- Maintain the IT Business Continuity and IT Security plans.
- Ensure the integrity and security of Redlands network, systems, and databases.
- Provide controlled access via authentication to Redlands computers, systems, databases and designated controlled areas.
- Determine minimum computer performance standards, and support general use hardware and software utilized by Redlands users.
- Acquire, operate and support the hardware and/or software which authorizes and manages network access for authorized machines and users.
- Manage ITS budgets for computing costs (hardware, software, maintenance, leases, licenses, and supplies), and project future budget needs.
- Assist Redlands with acquisition procedures for computing software and hardware (e.g. evaluating products, developing specifications, negotiating contracts, site planning, etc.).
- Acquire, install and provide technical support for Redlands classroom computers, computing devices, and classroom technology.
- Management, operation and support of campus telephone/voice mail systems.
- Management and support of campus network(s).
- Liaison with all vendors for materials parts and services required to maintain Redlands computer systems and network(s).
- Consult and provide input with Facilities Management, architects, general contractors and electrical contractors to support networking and AV systems in new building construction, building renovations and modifications.
- Produce special reports as required by Redlands administration and/or departments, and State or Federal entities.
- Develop and maintain custom business processes to meet the needs of Redlands users.

507.5 Prohibited Use of Redlands Enterprise Network

The use of the REN is prohibited for:

- illegal purposes;
- transmitting threatening, obscene or harassing materials;
- interfering with or disrupting network users, services or equipment (disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer viruses and using the network to make unauthorized entry to any other

computers accessible via the network);
- profit-making from the selling of services and/or the sale of network access;
- excessive private or personal business.

507.6 Specifically Prohibited Activities

The following activities are specifically prohibited:

- tampering with Redlands Community College-owned computer or communication hardware and/or software;
- defining and/or changing IP addresses on any machine;
- intercepting or attempting to intercept e-mail and file transfers;
- originating or attempting to originate mail from someone else;
- attempting to log-on to computers without an Account.
- bypassing/tampering with/or removing multi-factor authentication for access to any computer, data, or software application on any Redlands Community College owned or operated device or software application without explicit permission from the President, Executive Vice President, or CIO.

507.7 Account Data

Access to data within Accounts issued by Redlands Community College without written permission of the authorized Account user is prohibited. However, if probable cause exists to believe such data files or programs contain information relevant to a College business requirement or legal proceeding, a person other than the authorized Account user may examine such data files or programs. Permission for such access may be granted only by the College's President. Access to Accounts and/or data by the Department of Technology for routine REN maintenance work is permitted.

507.8 Disclaimer of Liability

Redlands Community College is not responsible for, and shall not be held liable for, the actions of users of the REN, or for damages caused or suffered by such users. Further, the College is not responsible for, and shall not be held liable for, any loss of data, for delays, non-deliveries, mis-deliveries, or for service interruptions. The College is not responsible for the accuracy or quality of information obtained through use of the REN.

507.9 Suspension and Revocation of Privileges

Access to and use of the REN is a privilege. Inappropriate or unauthorized use will be grounds for suspension or revocation of REN access and use privileges. Any use or attempted use of the REN which is in violation of any applicable College policies or procedures shall be grounds for suspension or revocation of REN access and use privileges. Confirmed misuse of the REN may also result in liability for monetary damages and for expenses incurred by the College in connection with the misuse; expulsion from the College; termination of employment; and/or legal action. One who misuses the REN may be subject to civil lawsuits and prosecution for criminal offenses.

507.10 Standards and Conditions of Use

Use of the College Network must be in compliance with all applicable College policies and procedures. The standards and conditions of use are published in the Procedures section of the Policies and Procedures Manual.

Adopted February 2001
Revised December 2010
Revised October 2022
Revised September 2025

507 PROCEDURE - Information Technology Services (ITS)

507.3:1 Guidelines for Account Creation

System access, based on user need, is requested via an Information Services (ITS) ticketing system. Requests for access must be submitted by the automated Human Resources system (HR initiated) or by the relevant Department Head.

If the request does not issue from either of the above sources then requests for system or data access will be directed to the following employees:

- Student Data – Executive Director of Student Services or Registrar
- Employee Data – Director of Human Resources
- Financial Data – Executive Vice President
- Surveillance Cameras – Executive Vice President
- Other Access – Case by case basis.

Faculty and Staff Accounts are created only after written notification from the Office of Human Resources. A manual process that includes creation of an Account using industry standard least user access privileges is performed. The employee will then set up a single sign-on account through Go Redlands by entering their personal email address and/or cell phone number.

Student Accounts are created automatically through a standard process that includes exportation of user information from a student information system into an authentication system. Unique usernames are provided directly to the student by the Admissions and Advising office. Students will set up a single sign-on account through Go Redlands by entering their personal email address and/or cell phone number.

Contractor Accounts are created only after written notification by the College's CFO of a contractual requirement. The management of the Technology Department shall review the access requirements on an individual basis and provide an Account using industry standard least user access privileges needed to fulfill the contract obligations.

Support Accounts are created as needed and identified to the management of the Technology Department. The management of the Technology Department will review the access requirements on an individual basis and provide an Account using industry standard least user access privileges needed to fulfill the contract obligations.

507.3:2 Guidelines for Keeping an Account Secure

A. Account log-on information (username and password) should not be shared with anyone for any reason at any time.
B. The account holder will set up his/her account by following the prompts on the Go Redlands webpage.
C. Passwords must be a minimum of nine (9) characters, should include upper and lowercase letters, and should have at least one (1) number.
D. Account users should not use items of common knowledge about themselves as passwords (such as birthdate, child's name, favorite pet, etc.).
E. Any user who suspects that his or her Account security has been breached should contact the Department of Technology's Helpdesk for remediation immediately.

507.8:1 Suspension and Revocation of Privileges

An authorized user's privilege of accessing and using the REN may be suspended or revoked by the College President or his or her designee.

507.8:2 Grounds for Suspension or Revocation of Privileges

A. Inappropriate or unauthorized use or attempted use of the REN.
B. Use or attempted use which is in violation of any applicable College policy or procedure, including Prohibited Use of Redlands Enterprise Network Policy, Specifically Prohibited Activities Policy, and the Standards and Conditions of Use Procedure.
C. Loss of status as an authorized user as defined in the Authorized User Policy for any reason.
D. Account inactivity for longer than one (1) year. Redlands Community College will keep student email accounts indefinitely as long as they show use via login. If the student account is inactive for over one (1) year, the student account will be permanently deleted with no chance of recovery.

507.8:3 Procedure for Suspension or Revocation of Privileges

Any time the College President has reason to believe grounds for suspension or revocation of a user's privileges exist, the President, or his or her designee, is authorized

to suspend the user's privileges, without prior notice. Any such suspension will be followed by notice of the suspension to the user and by a determination of whether the user's privileges should be revoked. If access and use privileges are revoked, the affected user will be notified. If reinstatement of privileges is possible, the affected user will be notified of the conditions and requirements for reinstatement.

507.9:1 Standards and Conditions of Use

The following standards and conditions of use are applicable to all users of the REN, as defined in the Acceptable Use of Redlands Enterprise Network Policy.

A. The REN shall not be used in violation of any College policy or procedure, any city, state or federal law, or any contractual obligation of the College.
B. Use of the REN shall be in compliance with the standards of the Oklahoma Higher Education OneNet Network.
C. Software shall not be installed on, copied or downloaded from the REN, without the express written consent of the management for technology.
D. Hardware shall not be connected to the REN without the express written consent of the management for technology.
E. Personal files and data shall not be saved or stored on the REN.
F. Students will receive emergency and non-emergency notifications to their Redlands email address from the College as needed.
G. Users shall not allow the display on REN computer screens of images, sounds, or messages that could create an atmosphere of discomfort, harassment or intolerance to others in the vicinity.
H. Users shall not use the REN to engage in any conduct that is calculated to harass or to cause embarrassment, shame, or intimidation.
I. Users shall not misuse or damage any component of the REN or take action calculated to cause any such damage.
J. Unauthorized use or attempted unauthorized use of the REN is considered misuse of the REN and is grounds for suspension and/or revocation of a user's access and use privileges.
K. Academic and research activities shall be given priority in the event of a conflict over use of the College's computer lab(s) resources. The priorities for use of the College's computer lab(s) resources are:
    - First: College students, organizations and groups that have reserved exclusive use of the lab(s);
    - Second: College students who are enrolled in classes that require the use of

specific software that is installed on a limited number of computers in the College's computer lab(s);

- Third: Students and faculty who wish to access the lab(s) for educational uses;
- Fourth: Persons who are not students or staff of the College, but have reserved use of the computer lab(s) to access data processing, indexing, or textual information from the REN or the Internet.
- Fifth: Other general users of the College or the Community using the lab(s) for acceptable recreational use.

L. Users shall not rely upon College staff that monitor or supervise the computer lab(s) to provide training in computer or Internet usage.

M. Campus printers require the use of the Campus Card in order to print.

N. Users who are disruptive will be asked to leave the computer lab(s) and, if necessary, will be removed by Security.

O. Users whose conduct is in violation of any standard or condition of use contained in this procedure will be asked to leave the computer lab(s) immediately and, if necessary, will be removed by Security.

P. Users are strongly discouraged from bringing children under twelve (12) years of age into the computer lab and any person under sixteen (16) years of age shall be accompanied by an adult while in the computer lab(s). Children are not authorized users of the REN. If a child is disruptive in the computer lab(s), the child and the adult accompanying the child will be asked to leave and, if necessary, will be removed by Security.

Q. All electronic media, e.g. CD-ROMs, DVD-ROMs, thumb drives, hard drives, solid state drives, etc., used by employees of Redlands Community College shall be turned over to the Redlands Community College Information Technology department for safe disposal upon removal from use.

R. Redlands Community College requires the destruction of data on electronic equipment being disposed, transferred or reused. This includes all forms of electronic media, such as tapes, hard drives, solid-state and flash drives, tapes, and devices with built-in storage. Media that is to be reused must be sanitized in a manner that makes access to previously stored data impossible. Bit by bit erasure at least 3 times is the minimum acceptable (DOD 5520 Standard). Contracting with an electronic disposal company guaranteeing destruction of data before reuse is in accordance with this policy as long as data destruction is performed to the minimum stated standard.

Adopted February 2001
Revised October 2022
Revised February 2023
Revised May 2024