Rancho Santiago Community College District
ADMINISTRATIVE REGULATION
Chapter 3
General Institution

AR 3720 Information Resource Use

These regulations shall be made available to RSCCD information resource users. These procedures shall not be construed as a waiver of any rights of RSCCD; nor shall the intention be that they conflict with applicable federal, state, and local law; nor do these regulations represent an agreement between the district and the users. The administrator responsible for Information Technology Services shall administer these regulations.

Rights and Privleges

RSCCD reserves all rights, including termination of all access to information resources that it owns and operates. Access and privileges to RSCCD information resources are assigned and managed by the administrators of individual information resources. Users may be authorized to use information resources and be granted appropriate access and privileges following the approval steps prescribed for specific information resources. Users may not, under any circumstances, transfer or confer these privileges to other individuals.

Responsibilities

The system administrator of each system sets minimum guidelines within which users must conduct their activities.

RSCCD information resources are for RSCCD related activities. Anyone who uses the RSCCD's information resources to harass, or make defamatory remarks, shall bear full responsibility for his or her actions.

RSCCD information resources provide access to external networks, including those of public and private sources, which furnish electronic mail, information services, bulletin boards, conferences, etc. Users may encounter material that may be considered offensive or objectionable in nature or content. Users shall not transmit or store any illegal, fraudulent, malicious, harassing, or obscene communications and/or content that is encountered. RSCCD does not assume responsibility for the contents of any external information resource. RSCCD's role in managing these information resources is only as an information carrier.

No user shall attempt to deliberately degrade the performance of an RSCCD information resource.

Users of RSCCD information resources must comply with the acceptable use guidelines for external information resources accessed through RSCCD information resources.

Users of RSCCD information resources must never attempt to transmit, or cause to be transmitted, any communication in which the originator's identity is deliberately concealed (except for those external entities lawfully authorized to do so).

Users of RSCCD information resources must never use any information resources to perform an illegal or malicious act. Any user attempting to change in any way the scope of information resource access to which they are authorized shall be regarded as malicious.

Any RSCCD user who becomes aware of a security issue on any information resource is obliged to report the issue to district Information Technology Services. The system must not be used until the system administrator has resolved the security issue.

System administrators may establish more detailed guidelines and responsibilities, as needed.

Accounts and Passwords

Knowledge of information resource passwords or security bypasses shall not be shared.

Users must not use an account not assigned to them without express, written permission from the information resource administrator. Users are responsible for the proper use of individual accounts, including but not limited to, proper password protection.

Knowledge of passwords or bypasses in information resource security shall not be used to damage any information resource, change in any way the authorized scope of information resource access, or otherwise make use of information resources for which proper authorization has not been granted.

Confidentiality

RSCCD reserves the right to access all content stored on RSCCD information resources.

In RSCCD information resources, there are two users who have the ability to access accounts and read individual electronic mail: the user to whom the account was issued, and the information resource administrator. While every reasonable attempt will be made to ensure the privacy of user accounts and electronic mail, there is no guarantee that accounts or electronic mail are private. Electronic mail is not 100% secure, nor is it delivered via a 100% secure information resource.

Student files are considered educational records as covered by the Family Educational Rights and Privacy Act of 1974 (Title 20, Section 1232 (g) of the United States Code). Such records are considered confidential under the law, but student files and electronic mail may be subject to search under court order if such files are suspected of containing information that could be used as evidence in a court of law. In addition, system administrators may monitor network traffic and/or access student files or electronic mail as required to protect the integrity of information resources (e.g., examining files or accounts that are suspected of unauthorized use or misuse, or that have been corrupted or damaged).

Copyright

Information resources protected by copyright are not to be duplicated in any form, except as permitted by law or by written contract with or permission from the owner or legal holder of the copyright. RSCCD may require written documentation verifying the user's right to make use of copyrighted materials prior to allowing them to be placed within RSCCD information resources.

Violations

A user's information resources privileges may be suspended upon the discovery of violation of these regulations. Violations of these regulations will be dealt with in the same manner as violations of other RSCCD policies and regulations and may result in disciplinary review. In such a review, and as specified in the RSCCD Board Policies and Administrative Regulations, the full range of disciplinary actions is available including the permanent loss of information resource use privileges, dismissal from RSCCD, and legal action. Violations of the above policies may constitute a criminal offense and may be prosecuted under applicable federal, state, and local law.

Responsible Manager: Assistant Vice Chancellor, Information Technology Services

August 11, 2014 (Previously AR 7000)