Rancho Santiago Community College District
ADMINISTRATIVE REGULATION
Chapter 3
General Institution

AR 3720 Information Resources Acceptable Use

References:

15 U.S. Code Sections 6801 et seq.;
17 U.S. Code Sections 101 et seq.;
Penal Code Section 502, Cal. Const., Art. 1 Section 1;
Government Code Section 3543.1 subdivision (b);
16 Code of Federal Regulations Parts 314.1 et seq.;
Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45

1.0. Purpose and Scope

The objective of this administrative regulation is to outline the acceptable use of information resources at Rancho Santiago Community College District ("District"). Inappropriate use exposes the District to risks including compromise of network systems and services or legal issues.

This procedure applies to all District students, faculty, and staff and to any other individuals granted use of District information resources. These regulations shall be made available to users of District's Information Resources. This procedure shall not be construed as a waiver of any rights of Rancho Santiago Community College District; nor shall the intention be that they conflict with applicable federal, state, and local laws.

2.0. Information Resources Applicability

This procedure refers to all District information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the District. This includes, but is not limited to, personal computers, workstations and associated peripherals, servers, network infrastructure, mobile phones, mobile computing devices, software and all other information resources, regardless of whether used for administration, research, teaching, or other purposes.

3.0. Rights and Privileges

The District information resources are the sole property of Rancho Santiago Community College District. They may not be used by any person without the proper authorization of the District. The District information resources are for District instructional and work-related purposes only.

The District reserves all rights, including termination of all access to information resources that it owns and operates. Access and privileges to District's information resources are assigned and managed by Information Technology Services (ITS) as well as other systems 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.

4.0. **Responsibilities**

Anyone who uses the District's information resources to harass, or make defamatory remarks, shall bear fullresponsibility for his or her actions. District's information resources provide access to external networks, including those of public and private sources, which furnish electronic mail, information services, bulletin boards, websites, social media, 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. District does not assume responsibility for the contents of any external information resource. District'srole in managing these information resources is only as an information carrier. Users of District's information resources must comply with the acceptable use guidelines for external information resources accessed through District's information resources.

Users of District's 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.

Users must not release any individual's (student, faculty, or staff) personal information to anyone without proper authorization.

Users of District's information resources must not use such resources in a way that violates federal, state, local or other law, or in a way that violates any District policies.

Formatted: Right: 0.72", Space Before: 0 pt

Formatted: Right: 0.72", Space Before: 0 pt

5.0. **Copyrights and Licenses**

Users of District's information resources must respect copyrights and licenses to software and other on-line information. Information resources protected by copyright are not to be duplicated in any form, except as permitted by law or by written contract or with permission from the owner or legal holder of the copyright. Protected software may not be copied into, from, or by any District facility or system, except pursuant to a valid license or as otherwise permitted by copyright law. District may require written documentation verifying the user's right to make use of copyrighted materials prior to allowing them to be placed within District's information resources.

In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from information resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is prohibited in the same way that plagiarism of any other protected work is prohibited.

6.0. Number of Simultaneous Users

The number and distribution of copied material must be handled in such a way that the number of simultaneous users in a department does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.

7.0. Integrity of Information Resources

Users of District information resources must respect the integrity of computer-based information resources. No user shall attempt to deliberately degrade the performance of a District information resource.

8.0. Modification or Removal of Equipment

Users of District information resources must not attempt to modify or remove computer equipment, software, or peripherals that are owned by others without proper authorization.

9.0. Unauthorized Use

Users of District information resources must not interfere with others access and use of the District computers. This includes but is not limited to: the sending of chain letters or excessive messages, either locally or off-campus; printing excess copies of documents, files, data, or programs, running grossly inefficient software when efficient alternatives are known by the user to be available; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a District computer or network; and damaging or vandalizing District computing facilities, equipment, software or computer files.

10.0. Unauthorized Programs

Users of District information resources must not intentionally develop or use programs which disrupt other users of District information resources or which access private or restricted portions of the system, or which damage the software or hardware components of the system. Users of District information resources must ensure that they do not use programs or utilities that interfere with other users of District information resources or that modify normally protected or restricted portions of the system or user accounts. If any unauthorized program(s) is(are) discovered on District resources, the District reserves the right to immediately remove or block access from the system in violation. The use of any unauthorized or destructive program will result in disciplinary action as provided in this procedure and may further lead to civil or criminal legal proceedings.

11.0. Unauthorized Access

Users of District information resources must not seek to gain unauthorized access to information resources and must not assist any other persons to gain unauthorized access.

12.0. Abuse of Computing Privileges

Users of District information resources must not access computers, computer software, computer data, or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the District. For example, abuse of the networks to which the District belongs or the computers at other sites connected to those networks will be treated as an abuse of District computing privileges.

13.0. Reporting Problems

Any defects discovered in system accounting or system security must be reported promptly to the Information Technology Services (ITS) Helpdesk so that steps can be taken to investigate and solve the problem.

14.0. **Accounts and Password Protection**

Users of District information resources are responsible for the proper use of individual

accounts, including but not limited to, proper password protection. A computer user who has been authorized to use a password-protected account may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the system administrator.

Any user account that has been identified as compromised (meaning that an unauthorized individual has gained access to the user account) is subject to temporary suspension or deletion until the assigned account user can be validated and appropriate security remediation has been completed.

15.0. Usage

Computer users must respect the rights of other computer users. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of District procedure and may violate applicable law.

16.0. Electronic Messaging Systems

The District has multiple electronic messaging systems, including but not limited to, an electronic mail (e-mail) system, ~~and provides~~ instant messaging (IM) and text messaging platforms, messaging utilities within its Learning Management System and multiple other systems that allow messages to be delivered electronically ~~services~~ (Electronic Messaging Systems). ~~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.~~

Users are responsible for using these technologies responsibly and within the following policies:

- The District's Electronic Messaging Systems are not to be used to send defamatory, fraudulent, harassing, obscene, threatening, or other messages that intentionally embarrass, disparage or disrespect others and their opinions, violate applicable federal, state or other law, violate the District Code of Ethics (BP 7001), Civility policy (BP 7002), the Standards of Student Conduct (BP 5500) or any other District policy, or which constitute the unauthorized release of confidential information.

- The District's Electronic Messaging Systems may not be used to transmit commercial or personal advertisements, solicitations or promotions.

- Sending unsolicited ~~e-mail~~ messages is prohibited, including the sending of junk mail or other advertising material to individuals who did not specifically request such material.

- Creating or forwarding chain letters or pyramid schemes of any type is prohibited.

- The District's Electronic Messaging Systems must not be used to create any messages that may be considered offensive or disruptive. Examples of messages deemed to be offensive are any which contain sexual implications, racial slurs, gender-specific comments or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin, gender, gender identity, gender expression, race or ethnicity, color, medical condition, genetic information, ancestry, marital status, physical or mental disability, pregnancy, or military and veteran status.

- Falsifying e-mail headers or routing information so as to obscure the origins of the e-mail or identity of the sender is a violation of this Administrative Regulation.

Formatted: Indent: Left: 1", No bullets or numbering

Formatted: Indent: Left: 0"

- Unauthorized access to others' e-mail accounts is prohibited.
- Personally identifiable information must not be e-mailed ~~or stored on portable devices~~ without encryption.
- Caution must be used when opening e-mail attachments or following hypertext links received from unknown senders, which may contain malware or viral code.
- Any email or message found to contain malware, viral code or categorized as a phishing type message is subject to administrative removal without the consent of the user.
- While every reasonable attempt will be made to ensure the privacy of user accounts and electronic mail, users understand that 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.
- Users understand that the District email system contains a set of technical tools to protect the security of its data. These tools allow technical staff to manage and secure smart phones and tablets when an email app is used to synchronize District issued email from them. The District uses these technical tools as required to protect the security of its information resources, in accordance with this procedure and as required by District policies and governing law. Users who choose to use an email app to synchronize their District issued email from a personally owned mobile smart phone or tablet may receive a "remote security administration" notification, a request to "allow my organization to manage my device," or a similar message prior to connecting to the District email system. These notifications indicate the presence of the technical tools previously mentioned and how they can potentially be used. However, the District only uses a limited set of standards to ensure basic email security on personally owned devices as more specifically defined in https://XXXXXXX.edu. The District is not able to see phone records, text messages, pictures, browsing history or any personal data stored or sent on personally owned devices and the District will not perform a remote device wipe on personally owned devices unless requested by the device owner. Users agree to allow these technical controls to be implemented on their personally owned devices by their choice to synchronize email on them. Users understand that this type of usage is completely voluntary and not required by the District
-

Formatted: List Paragraph, No bullets or numbering

Formatted: Font color: Auto

Formatted: List Paragraph, No bullets or numbering

Formatted: Normal, Indent: Left: 0.75", Hanging: 0.25", Outline numbered + Level: 1 + Numbering Style: Bullet + Aligned at: 0.75" + Indent at: 0.5"

17.0. Information Belonging to Others

Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users, without the permission of those other users.

18.0. User identification

Users shall not send communications or messages anonymously or without accurately identifying the originating account or station. However, systems that allow anonymous messaging to protect the identity of the sender are excluded from this provision.

19.0. Political, Personal, and Commercial Use

The District is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state and local laws regarding sources of income, political activities, use of property and similar matters.

19.1. Political Use

District information resources must not be used for partisan political activities where prohibited by federal, state, or other applicable laws.

19.2. Personal Use

District information resources given to users are provided to assist district employees and volunteers in the performance of their jobs and are intended for business and instructional use. Users are expected to exercise good judgment regarding the reasonableness of personal use of District information resources and assets. Personal use of District information resources and assets should be purely incidental. Incidental personal use should not conflict in any way with business objectives or interests, organizational values, or standards of business conduct.

19.3. Commercial Use

District information resources must not be used for commercial purposes. Users also are reminded that the ".cc" and ".edu" domains on the Internet have rules restricting or prohibiting commercial use, and users may not conduct activities not authorized within those domains.

20.0. Nondiscrimination

All users have the right to be free from any conduct connected with the use of Rancho Santiago Community College District information resources which discriminates against any person on the basis of national origin, religion, age, gender, gender identity, gender expression, race or ethnicity, color, medical condition, genetic information, ancestry, sexual orientation, marital status, physical or mental disability, pregnancy, or military and veteran status, or because he or she is perceived to have one or more of the foregoing characteristics, or based on association with a person or group with one or more of these actual or perceived characteristics. No user shall use the District network and computer resources to transmit any message, create any communication of any kind, or store information which violates any District procedure regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

21.0. Computing Standards

The District maintains a list of approved computing standards, which can be located here: https://rsccd.edu/Departments/Educational-Services/Technology-Advisor-Group/Pages/default.aspx

Computing Standards have been vetted to ensure compliance with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C §794d), and its implementing regulations set forth at Title 36, Code of Federal Regulations, Part 1194. Computing standards have also been assessed to ensure information security compliance and software compatibility across District technology platforms. District will only procure information resources within established computing standards. Use of information resources outside of computing standards cannot be guaranteed to satisfy accessibility and information security regulations. As such, exceptions may be prohibited and shall be reviewed by Information Technology Services on a case by case basis. These computing standards are only applicable to technology procured by the District and not to personally owned devices.

22.0. Disclosure

22.1. No Expectation of Privacy

The District reserves the right to monitor all use of the District information resources and access all content stored in its systems to troubleshoot system problems, disruptions or outages and to assure compliance with these policies. Suspected inappropriate use of systems by individuals may also be investigated in order to protect the organization. Users should be aware that they have no expectation of privacy in the use of the District information resources or in anything they store, create, send, or receive on a District information resource. The District will exercise this right only for legitimate District purposes, including but not limited to ensuring

compliance with this procedure and the integrity and security of its systems or as allowed by law.

22.2. Possibility of Disclosure
Users must be aware of the possibility of unintended disclosure of communications.

22.3. Retrieval
It is possible for information entered on or transmitted via computer and communications systems to be retrieved, even if a user has deleted such information.

22.4. Public Records
The California Public Records Act (Government Code Sections 6250 et seq.) includes computer transmissions in the definition of "public record" and nonexempt communications made on the District information resources must be disclosed if requested by a member of the public.

22.5. Litigation
Computer transmissions and electronically stored information may be discoverable in litigation.
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 tosearch under court order if such files are suspected of containing information that could be usedas 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).

23.0. Title IV Information Security Compliance
The Gramm-Leach-Bliley Act requires entities that participate in Title IV Educational Assistance Programs to develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to the entity's size and complexity. As a participating entity, the District has established Board Policy 3730 and associated Administrative Regulations to guide its information security program. Users of District information resources shall become familiar with Board Policy 3730 and its associated Administrative Regulations as they provide further guidance on acceptable use of District information resources.

24.0. **Violations**
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 District policies and regulations and may result in disciplinary review. In such a review, and as specified in the District's Board Policies and Administrative Regulations, the full range of disciplinary actions is available including the permanent loss of information resource use privileges, dismissal from the District, and legal action. Violations of these policies may constitute a criminal offense and may be prosecuted under applicable federal, state, and local law.

Those detecting violations of this Administrative Regulation must report the violation to their direct manager immediately, who will verify the nature of the violation and report it to the Information Technology Services (ITS) Helpdesk and/or Human Resources and/or Admissions and Records, as appropriate.

25.0. Dissemination and User Acknowledgment
All users of District information resources shall be provided copies of these procedures and be directed to familiarize themselves with them. All users must review and acknowledge

their understanding of these procedures on ~~an annual~~regular basis. Human Resources (HR) will provide the Administrative Regulation and acknowledgement links to new staff and contractors upon hire or contract establishment. Admissions and Records will provide the Administrative Regulation and acknowledgement links to new students.

A “pop-up” screen addressing appropriate portions of these procedures shall be installed on all applicable systems. The “pop-up” screen shall appear prior to accessing applicable systems. Users shall sign and date the acknowledgment and waiver included in this procedure stating that they have read and understood this procedure, and will comply with it. This acknowledgment and waiver shall be in the form as follows:

Information Resources Acceptable Use Agreement (Sample Language)

I have received and read a copy of the District Information Resources Acceptable Use Procedures and this Agreement dated, _____, and recognize and understand the guidelines. I agree to abide by the standards set in the Procedures for the duration of my employment or enrollment. I am aware that violations of this Information Resources Acceptable Use Procedure may subject me to disciplinary action, including but not limited to revocation of my network account up to and including termination, expulsion and/or prosecution for violation of State or Federal law.

Responsible Manager: Assistant Vice Chancellor, Information Technology Services

(Previously AR 7000)