

RANCHO SANTIAGO COMMUNITY COLLEGE DISTRICT

[Website: Technology Advisory Group](#)

Agenda for April 2, 2026

2:30 p.m. - 4:00 p.m.

<https://rsccd-edu.zoom.us/j/84722067242>

1. Proposed Self Service changes (10 minutes) – Howard
2. Technology initiatives for next Fiscal Year first reading (10 minutes) – J. Gonzalez
3. First readings (15 minutes) – J. Gonzalez
 - AR 3720 Computer and Network Use
 - Computing Standards: Special use cases for macOS
4. Technology Update – Colleges
 - SACTAC – Steffens (10 minutes)
 - SCCTEC – Rodriguez (10 minutes)
5. Student experience with technology:
 - SAC – Oberschlake (10 minutes)
 - SCC – V. Gonzalez (10 minutes)
6. Approval of TAG Minutes (5 minutes) – **ACTION** – Gonzalez
 - March 5, 2026
7. Technology Project listing, March 2026 (5 minutes) – Howard
8. District Council Minutes – March 2, 2026 (Informational Attachment)

Next TAG Committee Meeting: May 7, 2026

The Rancho Santiago Community College District aspires to provide equitable, exemplary educational programs and services in safe, inclusive, and supportive learning environments that empower our diverse students and communities to achieve their personal, professional, and academic goals.

Districtwide Initiatives 2025 – 2026

<u>Initiative ID #</u>	<u>ITS District Wide Initiatives 2025-2026</u>	<u>Proposal for 2026-2027</u>	<u>Districtwide Goal(s) #</u>
25-26*01	Implement and improve technologies to support enrollment management	Keep	25-27*4C
25-26*02	Support technology solutions that help improve operational efficiencies, provide cost savings, and automate manual processes	Keep	25-27*2D
25-26*03	Support distance education technology and remote delivery of services	Keep	25-27*1A
25-26*04	Improve overall data access and quality for decision making	Keep	25-27*4A, 25-27*4B
25-26*05	Evaluate and enhance computing standards to ensure equitable access to technology resources and support, based on current use, available resources, and funding constraints.	Keep	25-27*6A, 25-27*6B
25-26*06	Implement and manage technology solutions to prevent fraudulent applications, enrollment issues, and unauthorized access to student funding	Keep	25-27*5A, 25-27*5B
25-26*07	Abide by technology replacement cycle for hardware	Keep	25-27*6A
25-26*08	Refresh or replace end of life software. Upgrade to cloud-based applications when possible.	Keep	25-27*5B, 25-27*6A
25-26*09	Develop business process and service documentation. Conduct performance feedback and assessment through surveys and other communication mechanisms.	Keep	25-27*6B, 25-27*6D
25-26*10	Provide documentation and technology resources to support students who take part in participatory and student governance.	Keep	25-27*6C

25-26*11	Research, implement and maintain technology solutions that support campus, off-campus, and community events which enhance the student experience	Keep	25-27*1A
25-26*12	Support, improve and expand usage for single sign on (SSO) authentication solution for better user experience	Keep	25-27*1A, 25-27*5B
25-26*13	Upgrade web Content Management System (CMS) and maintain web platform stability and access for existing systems	Keep	25-27*2E, 25-27*3A
25-26*14	Implement and improve technologies that help ITS provide better support	Keep	25-27*5A, 25-27*5D
25-26*15	Employ data, cloud, web, mobile and infrastructure technologies to support student enrollment, access, persistence, transition, and success	Keep	25-27*1A, 25-27*1B
25-26*16	Implement and maintain security solutions and processes to comply with the Gramm-Leach-Bliley Act (GLBA)	Keep	25-27*5A, 25-27*5B, 25-27*5C
25-26*17	Implement solutions and processes to support Business Continuity (BC) and Disaster Recovery (DR)	Keep	25-27*5A, 25-27*5B
25-26*18	Develop Standard Operating Procedures (SOPs) that define and streamline functions and services across ITS teams and external technical resources	Keep	25-27*2C, 25-27*6D
25-26*19	Support technology solutions that help facility construction projects	Keep	25-27*1A, 25-27*2B
25-26*20	Improve district website experience across all platforms.	Keep	25-27*2E
25-26*21	Research, implement and maintain innovative technology solutions that support teaching and learning.	Keep	25-27*1A, 25-27*2B, 25-27*3B

25-26*22	Develop training materials and schedule training sessions for districtwide technology solutions. Facilitate technology demos for innovative technologies	Keep	25-27*1C, 25-27*2A, 25-27*6B, 25-27*6C
25-26*23	Research, implement, maintain and educate on accessible technologies and processes to support ADA and all applicable accessibility regulations	Keep	25-27*3A
25-26*24	Foster base system utilization, expand use of APIs for system integrations, remove or rewrite customizations to be SaaS platform compliant within Ellucian Colleague.	Keep	25-27*2D, 25-27*6A
25-26*25	Improve and deliver consistent user experience on both desktop and mobile environments using Ellucian Experience and Self Service technology.	Keep	25-27*2D, 25-27*2E
	Develop processes, policy, and technology support mechanisms for the responsible implementation and piloting of AI technologies.	Add	

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 3542.1 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 regulation applies to all District students, faculty, and staff and to any other individuals granted use of District information resources. This regulation shall be made available to users of District's Information Resources. This regulation shall not be construed as a waiver of any rights of Rancho Santiago Community College District; nor shall the intention be that it conflicts with applicable federal, state, and local laws.

2.0 Information Resources Applicability

This regulation 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. 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 RSCCD 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 full responsibility 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's role 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.

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.

Telecommunication rooms and facilities, where technology hardware is in operation, are environmentally conditioned to support optimal system performance. Construction activities that generate dust or debris, improper storage of items that affect airflow, or practices that impede access to this hardware are prohibited, as they are detrimental and may cause system failures, reduce system availability, or shorten the lifespan of the equipment. Users with access to these locations must exercise care to prevent damage or disruption to these information resources and must ensure that contractors or other individuals working in these areas understand and abide by these rules. Any construction or activity that may impede the proper functioning of the equipment in these areas must be coordinated with Information Technology Services.

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) Help Desk 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, 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 (Electronic Messaging Systems).

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 (Board Policy 7701), Civility policy (Board Policy 7002), the Standards of Student Conduct (Board Policy 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 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.
- Unauthorized access to others' e-mail accounts is prohibited.
- Personally identifiable information must not be e-mailed 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 e-mail 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 regulation 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 a more specifically defined in: <https://intranet.rscsd.edu/ITS/Pages/EmailMobileDevices.aspx>
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 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.

17.0 Generative Artificial Intelligence

Generative Artificial Intelligence (AI) is technology that can generate text, images, or other media in response to prompts and may be implemented through web applications, chatbot systems and other mechanisms. Users may only use Generative AI in a lawful, ethical manner that complies with all federal, state, or local laws and that does not violate any District policies or standards of academic integrity. To maintain data privacy, users shall not include personally identifiable information or other confidential data in prompts when using Generative AI. If there is a need to share such information through Generative AI, users should first contact the Information Technology Services (ITS) Help Desk to ensure that data privacy policies and other necessary controls are properly assessed. These

policies and controls must be fully evaluated prior to sharing personally identifiable information.

17.1 Use of AI-Based Note Taking Tools for Virtual Meetings

The District has reviewed and recommended specific AI note-taking tools for virtual meetings, whose configurations meet District privacy and security standards. A list of District-recommended tools is available at: <https://XXXXXXXXXXXXXXXXXXXX>.

Many third-party AI note-taking services for virtual meetings automatically store, transmit, or analyze meeting content in a way that may generate public records subject to disclosure under the California Public Records Act (PRA).

Users of District information resources who choose to use non-District recommended AI note-taking tools for virtual meetings should assume that any content captured, processed, or stored by such tools may become publicly available through PRA requests.

Use of non-recommended tools does not relieve users of District information resources of their obligations to protect confidential information, comply with FERPA, applicable privacy regulations, and District policy

Formatted: Underline

Formatted: Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.75" + Indent at: 1.25"

Formatted: Font: (Default) Arial

Formatted: Left, Indent: Left: 1.25", First line: 0"

18.0 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.

19.0 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.

20.0 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.

20.1 Political Use

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

20.2 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.

20.3 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.

21.0 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 regulation regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

22.0 **Computing Standards**

The District maintains a list of approved computing standards, which is located here: <https://rscdd.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 applicable to technology procured by the District and not to personally owned devices.

23.0 **Disclosure**

23.1 **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 regulation and the integrity and security of its systems or as allowed by law.

23.2 **Possibility of Disclosure**

Users must be aware of the possibility of unintended disclosure of communications.

23.3 **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.

23.4 **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.

23.5 **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 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).

24.0 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 adopted Board Policy 3730 Information Security – Logging and Monitoring 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.

25.0 Violations

Users' information resources privileges may be suspended upon the discovery of violation of this regulation. Violations of this regulation 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) Help Desk and/or Human Resources and/or Admissions and Records, as appropriate.

26.0 Dissemination and User Acknowledgement

All users of District information resources shall be provided copies of the procedures and be directed to familiarize themselves with them. All users must review and acknowledge their understanding of these procedures on a regular basis. Human Resources (HR) will provide the Administrative Regulation and acknowledgement links to new staff upon hire. Admissions and Records will provide the Administrative Regulation and acknowledgement links to new students. Vendors and contractors will be provided a copy of these procedures in Purchase Orders and/or contract clauses.

A "pop-up" screen addressing appropriate portions of these procedures shall be installed on all applicable systems to inform existing students and staff, vendors, guests and other users. The "pop-up" screen shall appear prior to accessing applicable systems. Continued usage of these systems shall constitute users' continued acknowledgement and acceptance of compliance with these procedures. Students and staff shall sign and date the acknowledgement and waiver included in this in this regulation stating that they have read and understood this regulation and will comply with it. This acknowledgement and waiver shall be in the form as follows:

Information Resources Acceptable Use Agreement (sample language)

I have received and read a copy of AR 3720 Information Resources Acceptable Use on (_____) and recognize and understand the guidelines. I agree to abide by the standards set in the procedures established in AR 3720 for the duration of my employment or enrollment. I am aware that violations of this Information Resources Acceptable Use AR 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 violations of State or Federal law.

Name: _____

Employee or Student ID: _____

Signature: _____

Date: _____

Responsible Manager: Assistant Vice Chancellor, Information Technology Services

Adopted: August 11, 2014 (Previously AR 7000)

Revised: June 6, 2022

Revised: October 2, 2023

Revised: February 3, 2025

Computing Standards

Special Use Cases for MacOS

While RSCCD primarily supports PCs within its standards, we recognize that certain situations may require the use of Mac computers due to their unique capabilities in specific areas. These special use cases are built to ensure that all students, faculty, and staff have access to the tools they need to perform their duties effectively and efficiently.

MacOS Special Use Cases for Instructional locations:

Instructional locations are defined as facilities with student facing computing technology. This includes computer labs and classrooms equipped with computer equipment used for instruction.

There are multiple academic disciplines where it is critical to expose students to Mac computers to prepare them for the real world, where they may encounter these devices in the industry. As such, Mac computers are a supported computing standard in Instructional locations within the following use cases:

- Graphic Design and Digital Arts Instruction
- Multimedia and Video Production and Editing Instruction
- Marketing, Communications, and Publishing Instruction
- Photography Instruction
- Music Production and Audio Engineering Instruction
- Macs are also supported when required to provide accessibility accommodations for individuals with disabilities who require the MacOS platform to have equitable access to technology.

MacOS Special Use Cases for Non-instructional locations:

Non-instructional locations are defined as facilities with employee facing computing technology. This includes offices, cubicles, and other areas outside of classrooms equipped with computer equipment that are not used for student instruction. Mac computers are a supported computing standard in Non-Instructional locations within the following use cases:

- For faculty who provide instruction in one of the following:
 - Graphic Design and Digital Arts Instruction
 - Multimedia and Video Production and Editing Instruction
 - Marketing, Communications, and Publishing Instruction
 - Photography Instruction
 - Music Production and Audio Engineering Instruction
- For instances in which there is division/departmental software required that only works on MacOS and no other suitable alternatives exist in the market.

- For certain departments where, under certain circumstances, employees may have more expertise in utilizing the Mac platform, given that it is widely used within their disciplines:
 - Marketing and Communications Departments
 - Departments that have responsibility for multimedia and video production
- For employees that need to develop and test User Experience (UX) and User Interface (UI) Design on the MacOS platform as part of their job duties.
- Macs are also supported when required to provide accessibility accommodations for individuals with disabilities who require the MacOS platform to have equitable access to technology.

Important: Given that PCs are the main computing standard, not all software applications and enterprise technology used within the District will be compatible with MacOS. ITS maintains a list of known incompatible applications and technology at <https://XXXXXXXXXX>. In addition to meeting the use cases above, employees need to ensure that their work will not be negatively impacted by being unable to use any incompatible technology before a Mac computer is issued to them.

MacOS Support Requirements:

Important: For Mac computers to be supported, they need to meet the same processes, technological standards and security controls that are established for PCs. All the following is required for any Mac computers that are added to any Instructional or Non-Instructional locations:

- Appropriate ongoing funding is approved and available to the requesting area to fund MacOS devices as part of computing replacement cycles.
- Devices must receive ongoing security updates from the manufacturer. End of support devices that no longer receive security updates cannot be added to the district network due to security concerns.
- Standard Hardware:
 - Hardware must be tested for compatibility and accessibility to confirm fitness for its intended use.
 - Only specific hardware models will be approved for purchase, in accordance with TAG approved computing standards.
- Standard Software:
 - Operating Systems/MacOS releases must be tested and validated before they can be deployed at large.
 - Standard Endpoint Protection Software (e.g. Microsoft Defender ATP) must be installed.
 - No local administrative rights will be given to end users.
 - Standard MacOS Baseline Configuration installed
- Must login with a Domain account and the computer must be joined to the appropriate RSCCD AD Domain through an established standardized process for all MacOS devices.
- Must use an established standardized process to support network printing.

- Centralized Computer Management is required:
 - MacOS computers must be added to a centralized management console and/or MDM, such as JAMF.
 - MacOS computers must be able to be remotely supported on prem and off network through tools such as JAMF Remote Assist
 - Application deployment must be centrally managed.
 - OS Updates including major releases, patches and other updates must be centrally controlled and managed.
- Mac computers must be added and tracked through centralized inventory repositories.
- Employees requesting the use of Macs will be referred to the list of known incompatible applications and technology here <https://XXXXXXXXXX>. Employees need to confirm that their work will not be negatively impacted by being unable to use any incompatible technology before a Mac computer is issued to them.
- Four-year AppleCare for Enterprise Service support is mandatory for any MacOS device purchased.
- MacOS Replacement Cycle: Mac computers should be replaced in accordance with the cycle established by TAG to ensure proper function and data security.

Technology Advisory Group
Zoom Meeting (Invitation shared via Outlook)
2:30 p.m. – 4:00 p.m.

Meeting Minutes for March 5, 2026

Voting Members Present: Song Graham, Jesse Gonzalez, Veni Herrera, Jennifer McAdam, Alex Natale, Sergio Rodriguez, John Steffens, Vangee Oberschlake – SAC Student

Voting Members Absent: Robert Bustamante, Jimmy Nguyen, SCC Student

Supporting Members: Dane Clacken, Marvin Gabut, Ron Gonzalves, Adam Howard, Scotty James, Kimberly Perna

Call to Order:

- The meeting was called to order by Mr. Gonzalez at 2:32 PM.
1. Update on work of Artificial Intelligence Taskforce:
 - Mr. Gonzalez provided an update. The task force is in the early planning stages of creating a district-wide AI strategy, focusing on teaching and learning, student support, operations, and community relations. They are working on defining membership, reporting structure, and responsibilities, and are making steady progress through weekly meetings. Mr. Steffens expressed concern about excluding existing technology committees, while Mr. James clarified the group is a work group reporting to academic senates, not part of the formal governance structure.
 - Discussions ensued noting on the challenges of maintaining consistent representation and the need to balance existing structures with new initiatives.
 2. Technology Update – Colleges:
 - SACTAC: Mr. Steffens provided an update.
 - SAC Website: Ms. Perna provided helpful guidance on setting up the necessary redirects, in response to a couple of public comments.
 - The committee discussed website redirects and approved new branding standards that incorporate accessibility improvements (i.e. updated colors and font size). Discussions on restricting AI agents in meetings but tabled the motion to allow time for developing a comprehensive framework based on data sensitivity levels. Further discussions have ensued among TAG members.
 - SAC Technology Plan: Mr. Steffens shared that recent poll results showed strong hesitation around AI especially from students. Final draft in progress incorporating structured frameworks, emphasizing governance, training/safeguards and to be presented at the next meeting.
 - Student Services shared informational update on ProcessMaker, an AI powered transfer evaluation tool; designed to automate the intake of roughly 15K transcripts annually to support Financial Aid.
 - Reviewed budget-related action items as part of a new integrated resource allocation process, where technology funding requests tied to program review are now brought to SACTAC.

- Mr. Gonzalves presented both the resource allocation request and technology refresh plan, as well as the updated hardware standards and costs. These were tabled due to time constraints, continuing the discussions at the next meeting.
 - The new ASG representative shared feedback about the website via chat.
 - SCCTEC: Mr. Rodriguez provided an update.
 - Committee discussed creating a tech survey for faculty and staff (similar to ASG's student survey). More information at the next meeting.
 - Email Distribution List and Structure: Reviewed and noted inconsistencies (i.e. part-time faculty are labeled but full-time faculty are not). Made recommendation to relabel "faculty" groups as full-time faculty for clarity. OEC management group is missing from the distribution list structure, raising concern.
 - Outlook Profile & Title Issues: Faculty and managers expressed widespread frustration with incorrect job titles in Outlook, noting unsuccessful attempts to fix them through HR. Concern that the inaccuracies affect professional representation.
 - SCC Website redesign: Ms. Perna shared updates with an April 6 go-live, testing nearly complete and a focus shifting to final updates to include better redirect planning and a new automated faculty profile feature that pulls teaching schedules dynamically.
 - Mr. Clacken provided updates on MFA.
 - Ms. Perna shared an overview noting that the proposal for a new web committee has not yet been reviewed by Academic Senate and is expected to be discussed at the next meeting.
3. Student experience with technology.
- SAC: Ms. Oberschlake: Nothing to report.
 - SCC: No update.
4. Approval of TAG Minutes for February 16, 2026, meeting.
- Mr. Gonzalez requested a motion; moved by Mr. Natale and seconded by Ms. Graham. Abstention: Mr. Steffens. Motion passed with correction.
5. Technology Project listing, February 2026: Mr. Howard provided an update.
- Create process to import noncredit bridge/petition applications from Dynamic forms: Soon to be deployed.
 - Remove Course Families Registration Barrier: Complete.
 - RG542 Visualization for Chancellor: Latest changes in progress. The research team plans to review the data soon after.
 - Ellucian Award implementation: Coordination kickoff scheduled this month after some necessary technical work is completed.
 - Credit and Non-Credit Faculty Assignment Letters: New request from H/R and in progress.
 - CollegeNet Series 25 scheduling system implementation: The team is finalizing data and coordinating with vendor for the build out in our system.
 - Colleague 320 implementation: The new standardized method will take effect in 2026–2027. Transition work is underway.
 - XGENED Data Copy: The development effort is underway.
 - Catalog Hours Cap on WebAtt Batch Uploads: Completed and moved to production.
 - Add Gen Ed Area Filters to Course Search in Self Service: Testing completed, feedback to be presented to the group for final decision.

Informational Handouts

1. District AI Taskforce Document
2. Technology Project listing for February 2026

Next Meeting Reminder: April 2, 2026, via Zoom**Adjournment:** The meeting was adjourned at 4:00 p.m.

DRAFT



Rancho Santiago Community College District District Council Meeting

MINUTES March 2, 2026

Members:	Marvin Martinez	Present
	Enrique Perez	Present
	Iris Ingram	Present
	Kristin Olson	Present
	Annebelle Nery	Present
	Jeannie Kim	Absent
	Jesse Gonzalez	Present
	Alejandro Moreno for Claire Coyne	Present
	Tara Kubicka-Miller	Present
	Steve Bautista	Present
	Sara Gonzalez	Absent
	Tyler Johnson	Present
	Zina Edwards	Absent
	Bridgette Hernandez	Present
	Kimberly Ramirez	Present
	Kayla Lopez	Present
Guests:	Dawn Okinaka, CCCAC	Mark Turner, CCCAC
	Christine Fundell, CCCAC	Elisa Carrillo, CCCAC
	Avi Advani, CCCAC	
	Ron Gonzalves	Linda Melendez
	Kimberly Perna	Adam O'Connor
	Marvin Gabut, SAC	Joseph Alonzo, SCC
	Krystle Taylor, SAC	Scotty James, SCC

1. Call to Order/Update
 - a. Chancellor Martinez convened the meeting via Zoom Conference at 1:32 p.m.

2. State Chancellor's Office Accessibility Center Report
 - a. Dawn Okinaka from the California Community Colleges Accessibility Center presented the RSCCD Accessibility Capability Maturity Model report for the September 2025 districtwide engagement. This report will assist RSCCD in meeting the accessibility compliance deadline of April 24, 2026. A copy of the report will be sent to Jesse Gonzalez who will distribute to appropriate parties.

3. Approval of Minutes

- a. It was moved by Dr. Nery and seconded by Ms. Ingram to approve the minutes of the December 1, 2025 meeting. The motion passed with abstentions from Sara Gonzalez and Kayla Lopez. Mr. Johnson was not present at the vote.

4. Approval of 2026-2027 Tentative Budget Assumptions

- a. Asst. Vice Chancellor Fiscal Services Adam O'Connor presented the 2026-2027 Tentative Budget Assumptions that were approved and recommended by the Fiscal Resources Committee. It was moved by Ms. Ingram and seconded by Ms. Kubicka-Miller to approve the 2026-2027 Tentative Budget Assumptions as presented. The motion carried unanimously.

5. Approval of 2024-2032 Planning Process Manual

- a. Vice Chancellor Enrique Perez requested that this item be moved to the March 30, 2026 meeting. It was moved by Mr. Perez and seconded by Ms. Kubicka-Miller to place the item on the March 30, 2026 District Council meeting agenda. The motion carried unanimously.

6. Approval of Revision to AR 4240 Academic Renewal

- a. It was moved by Mr. Bautista and seconded by Ms. Ingram to approve revision to AR 4240 Academic Renewal as presented. Discussion ensued. It was requested that the following changes be made to the administrative regulation:
 - i. 3rd bullet on page 1: spell out the SAC and SCC acronyms
 - ii. 4th bullet on page 1: will read as follows: "Academic Renewal Without Course Repetition is solely the policy of ~~the Rancho Santiago Community College District~~ Santa Ana College and/or Santiago Canyon College and may not necessarily be followed by other institutions."

The motion carried unanimously with the recommended changes discussed.

7. Committee Reports

- a. Planning and Organizational Effectiveness Committee (POEC)
Vice Chancellor Perez reported on the recent meetings.
- b. Human Resources Committee (HRC)
Vice Chancellor Olson reported on the recent meetings.
- c. Fiscal Resources Committee (FRC)
Vice Chancellor Ingram reported on the recent meetings.
- d. Physical Resources Committee (PRC)
Ms. Ingram reported on the recent meetings.
- e. Technology Advisory Group (TAG)
Asst. Vice Chancellor Gonzalez reported on the recent meetings.

Tyler Johnson joined the meeting during committee reports.

8. Constituent Representative Reports

- a. Academic Senate/SAC: Ms. Coyne reported on the SAC Academic Senate meetings and activities.
- b. Academic Senate/SCC: Ms. Kubicka-Miller reported on the SCC Academic Senate meetings and activities.
- c. CSEA: Mr. Tyler Johnson reported on CSEA 579 activities.
- d. Student Government/SAC: Ms. Ramirez reported on SAC ASG activities.
- e. Student Government/SCC: Ms. Lopez report on SCC ASG activities.

9. Other

- a. Ms. Ingram reported that a districtwide workgroup is being formed under Fiscal Services to plan and work on the statewide TOP to CIP code conversion.

Next Meeting: The next meeting will be held on Monday, March 30, 2026
Meeting Adjourned: 2:43p.m.
Approved: March 30, 2026

DRAFT