Policy 2030: Technology Resource Standards
Original Adopted Date: August 20th 2025   Status: Approved

PURPOSE
The Santa Cruz County Provisional Community College District (SCCPCCD) provides its students, employees, District Governing Board members and the public with access to information resources and technologies. SCCPCCD recognizes that the free exchange of opinions and ideas is essential to academic freedom, and the advancement of educational, research, service, operational, and management purposes, is furthered by making these resources accessible.

Arizona constitutional and statutory mandates require that SCCPCCD resources, including technology, be used only for the public's business, and not for private purposes. Those mandates apply to all SCCPCCD public officials – employees of every kind and the District Governing Board. The aim of those laws is to safeguard the use of resources, including technological resources, acquired and maintained with public funds.

This policy establishes standards for the use of SCCPCCD technology resources. They should be seen as supplementing, and not in lieu of, other Governing Board policy or applicable law.

Technology resources (including, but not limited to, desktop and laptop systems, printers, central computing facilities, SCCPCCD-wide or District-wide networks, local-area networks, telephones, facsimile machines, scanners, access to the Internet, electronic mail, and similar electronic devices and information) of the SCCPCCD are available to Governing Board members, employees, students and, in a limited number of cases, SCCPCCD contractors and the public. Use of all those resources is subject to the standards set forth in District policies and procedures.

USE OF NON-SCCPCCD TECHNOLOGY
Under Arizona's public records law, SCCPCCD is required to transact business so that its records are accessible and retrievable. The policy underlying the law is that work done in the name of the public be transparent. Thus, any member of the public may request public records and may be entitled to receive copies of them.

Each individual employee or District Governing Board member is responsible for ensuring that SCCPCCD records or data that he or she initiates or receives are retained for the period of time required by and disposed of according to mandates established by Arizona State Library, Archives and Public Records–the state agency tasked with setting standards for record retention and destruction. Therefore, an employee's or District Governing Board member's use of non-SCCPCCD technology resources for communication or conducting of any type of SCCPCCD business is prohibited because those records are less capable of being managed according to SCCPCCD's processes for ensuring retention, retrieval, and disclosure. If there are questions pertaining to record retention or destruction, department supervisors are encouraged to contact a senior District administrator for assistance.

As stated above, employees or Board members should not use personal technology resources for business/District purposes. Any SCCPCCD employee who receives a communication allegedly from another SCCPCCD employee using a non-SCCPCCD e-mail address should not respond and is to report the email to a supervisor or administrator immediately.

<u>ACCEPTABLE USE</u>
Use of SCCPCCD's technology resources, including websites created by SCCPCCD employees and students, is limited to educational, research, service, operational, and management purposes of the District. Likewise, data, voice, images, and links to external sites posted on or transmitted via SCCPCCD's technology resources are limited to the same purposes.

Frequently, access to SCCPCCD's technology resources can be obtained only through a password known exclusively to SCCPCCD employees, District Governing Board members, authorized affiliates, or students. It is those users' responsibility to keep a password confidential. While SCCPCCD takes reasonable measures to ensure network security, it cannot be held accountable for unauthorized access to its technology resources by other persons, both within and outside the SCCPCCD community. Moreover, it cannot guarantee employees, District Governing Board members, and students' protection against reasonable failures.

The maintenance, operation, and security of SCCPCCD's technology resources, require that network administrators and other authorized personnel have access to those resources and, on occasion, review the content of data and communications stored on or transmitted through those resources. Any other review may be performed exclusively by persons expressly authorized for such purpose and only for cause. All public officer and employee email accounts and correspondences regarding official duties (regardless of where such correspondences originate or are stored) are subject to Arizona's public records laws and other applicable state and federal laws, as well as policies of SCCPCCD, all of which may supersede a user's interests in maintaining privacy of information contained in SCCPCCD's technology resources. Access guidelines and acceptable use directives are further detailed through Procedures 2030.01, Network Resources Guidelines and 2030.02, Information Technology Acceptable Use Directives.

<u>PROHIBITED CONDUCT</u>
The following is prohibited conduct in the use of SCCPCCD's technology resources.

1. Posting to the network, downloading, or transporting any material that would constitute a violation of SCCPCCD policies, procedures, regulations, directives, or contract obligations.

2. Unauthorized attempts to monitor another user's password-protected data or electronic communication, or delete another user's password-protected data, electronic communications, or software, without that person's permission.

3. Installing or running any program on any system not approved in advance by the Information Technology Administrator.

4. Performing acts that would unfairly monopolize technology resources to the exclusion of other users, including (but not limited to) unauthorized installation of server system software.

5. Hosting an unauthorized website that violates the .EDU or .ORG domain request.

6. Use of technology resources for non-SCCPCCD commercial purposes or any other private interest not authorized by SCCPCCD, including advertising personal services, whether for financial gain or not.

7. Use of software, graphics, photographs, or any other tangible form of expression that would violate or infringe any copyright or similar legally recognized protection of intellectual property rights.

8. Activities that would constitute a violation of any Board policy, including, but not limited to, SCCPCCD's non-discrimination policy and its policy against sexual harassment.

9. Transmitting, storing, or receiving data, or otherwise using technology resources in a manner that would constitute a violation of state or federal law, or SCCPCCD policy or procedure, including, but not limited to, obscenity, defamation, threats, harassment, and theft.

10. Attempting to gain unauthorized access to a remote network or computer system.

11. Exploiting any technology resources by attempting to prevent or circumvent access or using unauthorized data protection schemes.

12. Performing any act that would disrupt normal operations of computers, workstations, terminals, peripherals, or networks.

13. Using technology resources in such a way as to wrongfully hide the identity of the user or pose as another person.

14. Allowing or engaging in any unauthorized access to or use of SCCPCCD's technology and non-technology resources.

15. Making personal long-distance or other toll calls, except where the charges for the calls are incurred directly by the caller or arrangements are otherwise made at the time of the call to directly bill the caller.

16. Intermittent use of technology resources that interferes with the performance of an employee's main responsibilities.

17. Use of technology resources to market or conduct other activities on behalf of a third-party regarding the "hosting" of an event that is prohibited under SCCPCCD's Facility Use Policy 2050.

18. Conducting District or District-related business using any electronic mail account other than one hosted or provided by SCCPCCD, and approved by the District's Information Technology Services administrator, even when the e-mail account copies all outgoing and incoming messages to the SCCPCCD hosted account.

19. Deleting or altering a technology public record in violation of public records retention requirements, or in anticipation of receiving or after receipt of a public records request, subpoena, or a complaint filed as part of a SCCPCCD grievance, investigation, or review, or another lawful request for the record.

20. Deleting or altering a technology record on a SCCPCCD device in anticipation or after receipt of a public records request, subpoena, or a complaint filed as part of a SCCPCCD grievance, investigation or review, or another lawful request for the records where the record may demonstrate a misuse of technology resources under this regulation.

DISCLAIMER
The home page of a SCCPCCD website must display, or link to, the following disclaimer in a conspicuous manner:

All information published online by SCCPCCD is subject to change without notice. SCCPCCD is not responsible for errors or damages of any kind resulting from access to its internet resources or use of the information contained therein. Every effort has been made to ensure the accuracy of information presented as factual; however, errors may exist. Users are directed to countercheck facts when considering their use in other applications. SCCPCCD is not responsible for the content or functionality of any technology resource not owned by the institution.

The statements, comments, or opinions expressed by users through use of SCCPCCD's technology resources are those of their respective authors, who are solely responsible for them, and do not necessarily represent the views of the Santa Cruz County Provisional Community College District.

INFORMATION ACCURACY AND MARKETING STANDARDS
To ensure that the most accurate information sources are reflected on web pages, information should be cited, sourced, properly attributed, or linked from the official District website or District department responsible for the subject matter. In addition, the design of web pages shall reflect established marketing standards with respect to the imaging and use of SCCPCCD marks as outlined by the District's Marketing and Public Relations Office.

COMPLAINTS AND VIOLATIONS
Complaints or allegations of a violation of these standards will be processed through SCCPCCD's articulated student and/or employee grievance procedures. Upon determination of a violation of these standards, SCCPCCD may unilaterally delete any violative content and terminate the user's access to SCCPCCD's technology resources. It is the user's responsibility to demonstrate and/or establish the relevance of content if a content complaint is made official. Users retain the right to appeal actions through SCCPCCD's grievance procedures.