Procedure 2030-PR(2): Technology Resource Standards - IT Acceptable Use Directives
Original Adopted Date: August 20th 2025 Status: Approved

Santa Cruz County Provisional Community College District (SCCPCCD) seeks to make access to computer technology available to all students, faculty, staff, and guests who use equipment, facilities, and systems appropriately and responsibly. This procedure addresses the use of networked computer technology at SCCPCCD as well as the use of any SCCPCCD computer or equipment containing electronic information. In addition, these directives apply to privately owned computer equipment if connected through SCCPCCD programs or accounts or if used to access network resources.

Network access yields a vast, diverse, and unique educational resource to members of the SCCPCCD community. With the privilege extended to certain SCCPCCD employees, students, and guests to utilize SCCPCCD equipment, programs, or accounts to obtain and exchange information on the network, comes the responsibility to use SCCPCCD computer equipment and resources reasonably, responsibly, and in a manner that promotes the educational goals of the District. Failure to comply with this procedure may be grounds for revocation of that privilege as well as for disciplinary action, up to and including dismissal, or criminal charges, or both. SCCPCCD reserves the right to allocate and restrict access to computing resources for the benefit and protection of the institution.

Users should understand that electronic mail (e-mail) or other information that is electronically transmitted, received, or stored is not private. District networks and technology systems are licensed, maintained, owned, and operated by Santa Cruz County Provisional Community College District. Persons operating and maintaining SCCPCCD's computer systems have access to information transmitted, received, or stored on these systems. A system administrator during routine maintenance may see the content of electronic messages. In addition, electronic messages are stored in files, and these are transferred to various media during system backups. The contents of these files and the copies saved to tape are subject to the same rules outlined in this and other policies governing information technology.

System administrators, while fulfilling their responsibilities, may have to examine files to diagnose or solve problems or gather evidence of violations of SCCPCCD procedure. SCCPCCD reserves the right to examine, edit, or remove any material that violates SCCPCCD policies or procedures and monitor any activity involving District systems, including the Internet or Intranet. SCCPCCD reserves the right to monitor or access all information stored or maintained on its computer systems. If such monitoring reveals possible evidence of criminal, illegal, or other prohibited activity, system personnel may provide the results to the CEO or law enforcement officials.

The user assumes all responsibility for SCCPCCD assigned accounts or computer equipment. This includes assuring that unauthorized persons do not use assigned accounts or systems. Passwords or access codes are the property of SCCPCCD and may not be shared with others. Users may only access data, e-mail, data transmissions, network resources or computer equipment for which they have authorization. Users may not conceal their identity in any electronic communication. All users should save local copies of their work files, including web pages and e-mail, in case of accidental removal.

SCCPCCD makes absolutely no warranties of any kind, neither expressed nor implied, for the services it is providing. The District is not responsible for loss of documents, data, or personal information because of system failure, hardware malfunction, or faults incurred by the network or computing resources, or for any other loss incurred for any reason. The District is not responsible for any damage or loss to personal computing hardware or software incurred while using any District resources, facilities, or services.

While using any such SCCPCCD-owned or maintained computer equipment or resources, a SCCPCCD employee, student, or guest shall not knowingly or intentionally:

a. Transmit, publish, display, retrieve, record, or store any information or material in violation of state or federal law. This includes, but is not limited to, actions that would be in violation of laws protecting copyrights, trademarks, or other intellectual property.

b. Transmit, publish, display, retrieve, record, or store any information or material that is obscene, profane, physically or sexually abusive, sexually explicit, or that describes or displays people engaging in explicit, obscene, or otherwise inappropriate behaviors, or engaging in conduct that would be considered inappropriate for general public viewing or general viewing in the workplace. This prohibition does not impede or contradict Policy 4000, Academic Freedom which allows the legitimate use of various media essential to the fundamental mission of discovering and advancing knowledge and disseminating it to students.

c. Transmit, publish, display, retrieve, record or store information or material that could reasonably be construed to create a hostile or offensive work or educational environment for members of a particular sex, religion, race, or ethnic background. For example, sexually inappropriate screen savers or wallpaper that might create an offensive workplace for others are prohibited on SCCPCCD equipment.

d. Engage in conduct reasonably likely to disrupt use of the Internet or Intranet or use of other SCCPCCD computer equipment or resources by others. This includes conduct known by the employee, student, or guest to be contrary to accepted and reasonable rules of network etiquette when accessing SCCPCCD computer systems. Measures will be taken to protect the quality of service to all users.

e. Use SCCPCCD computer equipment or resources for a commercial or political purpose distinct from the employee's specific job function at SCCPCCD, unless expressly authorized in writing by the appropriate personnel as designated by the CEO.

f. Engage in conduct reasonably likely to compromise any system security device or security program.

g. Engage in conduct reasonably likely to harm or destroy data or software or to harm or destroy computer equipment. Introduction of a virus or other software that will maliciously interfere with the normal operation of the hardware or software is strictly prohibited.

Finally, it is the institution's intention that the above restrictions be applied consistently but reasonably. There is no intention to hamper appropriate educational research and discourse. If an employee, student, or guest has any question about whether a certain activity is or is not prohibited by the above directives, or if the employee, student, or guest believes that an exception to any of the above restrictions is warranted, that employee, student, or guest should seek advice concerning the issue, or request an exception from application of a specific directive, from the appropriate personnel as designated by the CEO.

Requests for unofficial District Internet/Intranet postings via the Web or links to other servers are to be directed to SCCPCCD's IT administrator. Process guidelines governing unofficial District Internet/Intranet postings via the Web or links to other servers include:

District committees, organizations, and groups may be granted the privilege of posting pages that:

are consistent with the public, non-profit educational mission of the District, meet the technical specifications of the system, comply with District procedures and state and federal laws, and are approved in advance by SCCPCCD administration.

Groups and individuals seeking this privilege should contact the IT administrator in writing and provide the following information:

a. An outline of the proposed page(s) including addresses of proposed links and samples of graphics or photos.

b. A justification for why the page is requested or how it might serve the SCCPCCD community.

The IT administrator will seek approval through designated channels if all requested documentation has been provided.

Those groups granted the privilege of posting pages must have designated a District employee to act as a liaison and responsible party to ensure that all District policies, procedures, and applicable laws are understood and followed. Identity of the designated employee will be provided when notification of proper approval is made. Content must be reviewed and approved before an initial link to the page or pages is provided.

The originating party is responsible for maintaining links, updating, and maintaining appropriate and timely content, and ensuring that any changes conform to District policies, procedures, and applicable laws. If the approved page(s) are found at any time to contain inappropriate or outdated content or are in violation of District policy, no advance notice will be given before removing links to the page or groups of pages until the originating party can show compliance to District guidelines and procedure.

Parties granted the privilege of posting pages or links to pages included on District servers may not receive advance warning when the servers are brought down for maintenance, repairs, backups, or any other reason deemed necessary by appropriate District administrators.

SCCPCCD reserves the right to prohibit elements on unofficial pages that it deems inappropriate as outlined in this procedure. This includes text, graphics, or links to third-party pages. Unofficial pages may also be required to display a disclaimer provided by the District.