



San Carlos Apache College

Information Technology Policies

As approved by the San Carlos Apache College Board of Regents on
XXXX (DATE)

These policies supersede and replace prior Information Technology policies. None of these policies may be amended or altered in any way by oral statements. Only written amendments by authorized management officials and approved by the San Carlos Apache College Board of Regents will constitute changes to the content of this document.

TABLE OF CONTENTS

Table of Contents	1
Introduction	3
1. Definitions and Purpose	
2. General Guidelines	
A. Information Technology Department	4
1. IT Department Responsibilities	
2. Software	
3. Rights of the IT Department	
4. Individual Responsibilities	
5. Rules for Users	
B. Accounts and Passwords	6
1. Accounts	
2. Passwords	
3. Practices to Secure Accounts	
4. Third-Party Vendors	
C. Data Access and Use	7
1. Data Access	
2. Guidelines and Restrictions	
D. Email and Electronic Communication	9
1. Email Guidelines	
2. Conditions for Inspection	
3. Prohibitions	
4. Personal Software	
E. Internet Usage	10
1. Electronic Information Services	
2. Internet Safety	
3. Education, Supervision, and Management	
4. Prohibitions	
F. Social Media	12
1. Guidelines for Posting to Social Media Sites	
2. Monitoring of Social Media	
3. Social Media Site Approval, Administration, and Requirements	
4. Posting to External Social Media Sites	
5. Confidentiality	
G. Bring Your Own Device	16
H. Video Streaming	17
I. Web Publishing	18
J. Copyrighted Materials	18
1. Copyright Protections	
2. Allowable Uses	
3. Fair Use Exception	
K. Violations	19
L. Equipment Circulation Policy	20

1. User Responsibilities	
2. Lost & Damaged Items	
3. Limit on Chromebooks/Laptops	
M. Computer Labs	20
1. Prohibited Use	
2. Access to Computer Labs	
3. Sensitive Materials	
4. General Lab Rules	
5. Operating Hours	
6. Printing	
7. Clean Workspaces	
8. Responsibilities	
Employee Acknowledgement Form	24

INTRODUCTION

The San Carlos Apache College (SCAC and/or College) Information Technology (IT) Department is responsible for ensuring that SCAC students and employees have the electronic equipment and capacity to perform their academic work and employment responsibilities; to ensure that SCAC has adequate internet connectivity; to support programs for instructor online and in classroom instruction connectivity with students; to conduct ongoing maintenance of equipment and systems; and to plan for increased electronic technology capacity. This policy manual documents the policies and procedures for IT staff to administer and for SCAC staff and students to use SCAC electronic equipment, systems, and programs.

1. Definitions and Purpose

- a. “Technology” refers to any internet-based desktop, laptop, tablet, and smartphone applications connected to or associated with SCAC. The Information Technology Department policies encourage internet-based services for SCAC-related purposes for students and staff and on SCAC-related web spaces.
- b. SCAC provides a wide variety of computing and networking resources to students and staff of SCAC. Access to computers, computing systems, and networks owned by SCAC is a privilege that imposes certain responsibilities and obligations and is granted subject to SCAC policies, codes, and tribal and applicable federal laws. All users of these resources must comply with specific policies and guidelines governing their use and act responsibly while using shared computing and network resources, including wireless. This policy aims to promote the efficient, ethical, and lawful use of SCAC’s computer and network resources.
- c. “Social media” refers to Web-based and mobile technologies enabling individuals or entities to disseminate, receive information, communicate, or interact. The term includes email, texting, messaging, social networking, blogging, micro-blogging, bulletin boards, Facebook, LinkedIn, Twitter, YouTube, Instagram, Snapchat, TikTok, and other similar social media platforms and apps.
- d. SCAC recognizes and embraces the power of social media and the opportunity those tools provide to communicate with the SCAC community, including students, faculty, staff, parents, alumni, and other interested parties. However, it is important to recognize that using social media at or concerning SCAC is governed by the same laws, policies, rules of conduct, and etiquette that apply to all other activities at or concerning SCAC.

2. General Guidelines for the Use of Information Technology

- a. Individuals using computer resources belonging to SCAC must act responsibly, comply with law and institutional policies, and respect the rights of others using a shared resource. The right of free expression and academic inquiry is tempered by the rights of others to privacy, freedom from intimidation or harassment, protection of intellectual property, ownership of data, and security of information.
- b. IT policies do not prohibit employees from using social media to discuss among themselves, even in terms that may be critical of the College, any protected activities relating to the terms and conditions of their employment.
- c. Users of SCAC technology implicitly agree not to use technology to engage in harassment or intimidation or use computer and network resources for unlawful acts. Using SCAC’s

computer or network resources for illegal activities is strictly prohibited. Unlawful use of the College's computer and network resources can expose the individual user and the college to damage claims or potential criminal liability and civil liability. Unlawful uses may include, but are not limited to, harassment and intimidation of individuals based on race, sex, religion, ethnicity, sexual orientation, or disability; obscenity; child pornography; threats; theft; attempting unauthorized access to data; attempting to breach security measures on any electronic communications software or system; attempting to intercept electronic communication transmissions without proper authority; and violation of intellectual property or defamation laws. Do not use computer systems to send, post, or display defamatory messages, text, graphics, or images. Using SCAC's computer and network services, each user is responsible for becoming informed about and complying with all applicable laws and policies.

- d. SCAC technology use implies an agreement to use computer and network resources efficiently. Computing resources are finite and must be shared. Users may use the College computer and network resources for incidental personal purposes, provided that such use does not:
- Unreasonably interfere with the use of computing and network resources by other users or with SCAC's operation of computing and network resources;
 - Interfere with the user's employment or other obligations to the college; or
 - Violate this policy or other applicable policy or law. SCAC retains the right to set priorities on the use of the system and to limit recreational or personal uses when such uses could reasonably be expected to cause, directly or indirectly, strain on any computing facilities, to interfere with research, instructional, or administrative computing requirements, or to violate applicable policies or laws. Examples of inappropriate use include circumventing the editor or moderator to post messages to private (closed) list servers, sending "chain letters," engaging in pyramid schemes, or engaging in unauthorized peer-to-peer file sharing. Sending "spam" or posting inappropriate promotional or commercial messages to discussion groups or bulletin boards is prohibited.

A. INFORMATION TECHNOLOGY DEPARTMENT

1. Department Responsibilities

The responsibility of the IT Department includes but is not limited to:

- Maintaining and repairing computer systems promptly to ensure business productivity.
- Securing information systems.
- Providing a backup system for data stored on the servers.
- Respecting the Confidentiality of information.
- Using Administrative system passwords on computers designated by the Systems Technician.
- Keeping doors locked in restricted areas.
- Accessing information only if it is necessary to resolve an issue or investigate violations of the computer use policy
- Reporting criminal activity to the appropriate authorities. Based upon video surveillance.

- Notifying users when making system changes that affect them. This will be done so the users have time to prepare and voice any concerns about the changes.
- Approving all requested SCAC software before purchase to ensure compatibility.
- Keeping an inventory of all information technology equipment, including but not limited to computers, monitors, printers, scanners, presentation systems, external drives, servers, software, computer accessories, and telephone communication equipment.
- Preparation of a disaster recovery plan.
- Implement a disaster recovery plan when data cannot be retrieved from servers.

2. Software

The SCAC IT Department supports the following software.

- Microsoft Windows
- Microsoft Office 365
- Google G-Suite
- Jenzabar EX
- Canvas
- Adobe

The IT Department may add other software needed for College operations by request of a staff or faculty member and approval by the appropriate supervisor and IT Department.

3. Rights of the IT Department

To perform its duties, the SCAC IT Department reserves the right to perform the following activities:

- IT may routinely monitor and log computer traffic on the network and inspect files of specific users on their computers for evidence of a violation of policy or law.
- IT can control or refuse access to anyone violating computer use policies.

4. Individual Responsibilities

The following list includes responsibilities for which SCAC users are responsible. They are designed to ensure computing security, efficiency, and respect for other SCAC employees and students.

- Respect the privacy and personal rights of others. Accessing files, directories, or emails of others without authorization is prohibited.
- Respect the needs of others and only use a fair share of computing resources.
- Use printing resources responsibly, using two-sided options when feasible.
- Users shall report any violations of the computer use policy to the SCAC Information and Technology department.
- Users who find security holes in the SCAC system must report them to the IT Department.
- Flash drives, external hard drives, or other media with Confidential Information must be in a secured location.
- Flash drives, external storage drives, or other media that once contained confidential information must be properly erased or destroyed so that others cannot recover their information.

- Screens must be oriented to prevent unauthorized people from reading sensitive information when possible.
- Documents should be saved to “My Documents” on SCAC computers as they are backed up into the Google Drive Backup Sync program. Documents created on the computer desktop should be saved in “My Documents” regularly to ensure they are not lost if a computer malfunctions.

5. Rules

The following is a list of rules relating to IT that SCAC users must follow.

- Theft of Computer Equipment, media, software, or data is prohibited.
- Deliberately attempting to degrade the computing system's performance, damage it, or steal information is prohibited.
- Printers are to be used for College use only.
- All devices on the SCAC network must conform to the computer use policy.
- The SCAC computing system will be used only for SCAC-related work. Personal use of software purchased by SCAC is prohibited unless approved by the appropriate supervisor and the IT department.

B. ACCOUNTS AND PASSWORDS

1. Accounts

Email accounts require a username and password to access resources on the computer network and computers. For those employees hired under contract, an email account will be created on the day the contract is signed. An email account will be established for employees not hired under contract on the first day of employment. Employee accounts will remain active during the term of employment. When there is a separation from employment, the College’s Human Resources Department will notify the IT Department of the date of separation, or in the case of termination, just before the termination meeting, when to disable the email account.

For instructors, including Adjunct instructors, if they do not teach for two terms, excluding summer sessions, the account will be suspended until they resume teaching.

Student email accounts will be created when a student completes a SCAC/TOCC application for enrollment and is accepted as a student. The account will be deleted if a new student has not registered for classes after 60 calendar days. Student accounts will be closed after the student graduates, transfers, or has not registered for classes for 60 days.

Accounts with extensive permissions to the SCAC computing system or access to confidential information through the SCAC computing system are to be used only in performing job duties.

Interception, theft, and/or decryption of system or user passwords is prohibited.

Employees and students leaving SCAC/TOCC shall discontinue the use of SCAC/TOCC technology upon termination of employment. Access to the Electronic Information System (EIS) will be removed.

Partners, affiliates, or other college collaborators may provide access to non-SCAC IT resources or services governed by third-party appropriate use policies, statements, or standards. Authorized Users shall comply with these requirements unless doing so would violate applicable law or policy.

2. Passwords

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of SCAC resources. All users (staff, students, guests, contractors, and vendors) with access to SCAC systems are responsible for selecting and securing their passwords, as outlined below.

3. Securing email accounts

Employees and students must use the following practices to secure accounts:

- Avoid storing passwords around the office area where others can find and use the password for unauthorized access.
- Accounts with extensive privileges to the SCAC computer system shall choose sufficient passwords, meaning a mixture of letters and numbers of no less than eight characters. The use of symbols is also recommended.
- Password Length should be a minimum of 8 characters and a maximum of 20 characters and must contain special characters, all of which may be used but are not required.
- Do not store passwords in unsecured locations.
- Computer security for users must have screens locked upon leaving the workstation. (not in a sleep mode on the computer)
- New passwords are required when the IT Department sets a regular schedule to change passwords.
- Avoid sharing usernames and passwords unless concluded necessary by the IT Department.
- Don't use a password that is the same or similar to one you use on any other websites/systems.
- Don't use a single word, for example, password, or a commonly used phrase like "I Love You."
- Make passwords hard to guess and avoid names and birthdays of self, friends and family, favorite bands, and often-used phrases.
- Avoid personal information, including name, important dates, pets, and context-specific words, such as the name of the service, the username, and derivatives thereof.
- Be aware that the IT Department limits the number of failed login attempts.

4. Third-Party Vendors

Third-Party vendors are only allowed access to production data to resolve problems with their software or hardware. These parties are subject to the SCAC computer use policies where applicable.

C. DATA ACCESS AND USE

1. Guidelines for Data Usage

- The President's Office and the Finance Department must be consulted to ensure that appropriate contract language regarding data protection is incorporated into any agreement.

- The IT Department will work with Operations to ensure appropriate facilities are provided to protect data equipment.
- Legally Restricted Information in paper form must be stored in locked or otherwise secured areas when not in active use. Legally Restricted Information in electronic form must be stored in secure designated data centers or, if authorized to be stored elsewhere, only in encrypted (or similarly protected) form. It must not be stored on a desktop, laptop, or other portable devices or media without encryption or similar protection.
- Reports and communications should only include Legally Restricted Information that is essential to perform the function for which the communication is made. Transmission of Legally Restricted Data must be by secure methods. If Legally Restricted Data is transmitted by e-mail or other electronic transmission, it must be encrypted or otherwise adequately protected. Contact the Information Technology Department for advice and assistance.
- When a record containing Legally Restricted Information is no longer needed, it must be disposed of in a manner that makes it no longer readable or recoverable. Paper records containing Legally Restricted Data must be shredded. Electronic records containing Legally Restricted Data must be deleted from their storage location.

2. Restrictions

Access to information owned by SCAC is generally consistent with the concept of academic freedom and the open nature of the institution. However, there are types of information where access must be restricted, and caution in handling and storing the information is necessary.

The disclosure and use of the following types of information is restricted by law.

- Social Security Numbers (SSN)
- Patient Protected Health Information (HIPAA)
- Student Information (FERPA)
- Financial Account, Credit, and Debit Card Information
- Employee Personnel Records

Legally Restricted Information must be stored, used, and disclosed to others only on a need-to-know basis to permit the individual faculty or staff member to perform the SCAC functions for which the information was acquired and for which it is maintained. Access to legally restricted information is carefully safeguarded. Protection of Legally Restricted Information from disclosure to or unauthorized access by anyone who does not have a legitimate need to access the information is a primary responsibility of the staff person supervising the SCAC Division or Department that houses the information.

Alternatives to using Legally Restricted Information should be identified and used whenever possible. Disclosure of Legally Restricted Information to a third-party agent or vendor is permitted only if the agent or vendor assumes a legally binding obligation to safeguard the use and disclosure of the information. The electronic exchange of Legally Restricted Information outside of SCAC must have proper approval. In addition, the appropriate Administrators must be consulted to ensure appropriate security controls are employed. The Administrators include the SCAC President, Dean for Sustainability, and IT Manager.

D. EMAIL AND ELECTRONIC COMMUNICATION

1. Email Guidelines

When using SCAC/TOCC email accounts, employees and students must conform to the following policies:

- Clearly and rightfully identify the user who sent it.
- Emails must be written professionally and may not be used to send rude, obscene, harassing, or illegal materials.
- Mass mailings may only be used for business and SCAC/TOCC student activities. Chain letters and other types of non-business mailings are strictly prohibited.
- Users shall not use any means to alter, conceal, or misinform their true identity.
- Use of SCAC computing resources to obtain unauthorized access or intent to damage or disturb external computing systems is prohibited.
- Downloads from untrustworthy sources are prohibited. This includes “Freeware” such as games, organizer utilities, clock utilities, etc. If these programs are found on the computer of an employee or a student, they will be removed by the IT Department. Only programs needed for productivity will be supported (see supported software section).
- The IT Department is the only SCAC entity authorized to repair or contract to repair computers and technology systems. Individuals authorized by the SCAC IT Department may perform basic troubleshooting.
- Authorized IT personnel may see the contents of emails while troubleshooting or performing maintenance work on the email system.

2. Conditions for Permitting Inspection, Monitoring, or Disclosure

SCAC may permit the inspection, monitoring, or disclosure of email, computer files, and network connections when:

- Required or permitted by law, including public records law, or by a subpoena or court order.
- SCAC or its designated agent has reason to believe that a violation of law or policy has occurred.
- Monitoring and preserving the functioning and integrity of the e-mail or related computer systems or facilities is necessary.

All computer users agree to cooperate and comply with SCAC requests for access to and copies of email messages or data when access or disclosure is authorized by this policy or required or allowed by law or other applicable policies.

3. Prohibition Against Activities Placing Strain on Facilities

Activities that may strain the e-mail or network facilities more than can be reasonably expected are not allowed. These activities include but are not limited to sending chain letters; “spam,” or the widespread dissemination of unsolicited e-mail; and “letter bombs” to resend the same email repeatedly to one or more recipients.

4. Personal Software

Software can only be installed on SCAC devices by the IT Department.

Personal software is only installed on SCAC devices if approved by the employee's supervisor and IT Manager for a work-related project. If it is approved, the software must be installed by the IT

Department. This policy is not intended to restrict the downloading of files from Internet sources or online services authorized by Instructors for courses and employees in performing their job duties.

E. INTERNET USAGE

This policy and related regulations and exhibits define the acceptable uses of technology and technological education efforts. SCAC provides Electronic Information Services (EIS) to staff, instructors, students, and other users who acquire access privileges through association with SCAC. These services shall support the college's instructional, informational, communication, research, administrative, and educational goals.

Electronic Information Services include but are not limited to networks (e.g., LAN, WAN, Internet), telephone systems/voice mail, electronic mail, databases, hardware, software, Google Apps for G Suite, Microsoft 365, additional services, and any computer-accessible source of information. These include but are not limited to, hard drives, external drives, or other electronic sources/media (e.g., Universal Serial Bus [USB] flash drives, iPads), and similar equipment as it may become available.

To assure that the SCAC EIS is used appropriately and for the educational purposes intended, SCAC requires anyone who uses the SCAC EIS to follow this policy and related regulations for appropriate use.

The IT Department shall determine steps, including using a firewall and/or proxy, that must be taken to promote the safety and security of using the College's online computer network when using electronic mail, social media hangouts, and other forms of direct electronic communications. Technology protection measures shall protect against Internet access by staff and students to obscene visual depictions, child pornography, or the use of computers by minors harmful to minors. Safety and security mechanisms shall include online monitoring activities.

It is the policy of SCAC to:

- prevent access to or transmission of inappropriate material via the EIS, the Internet, electronic mail, or other forms of direct communication;
- prevent unauthorized access and other unlawful online activity;
- prevent unauthorized online disclosure, use, or dissemination of personal identification information of students.

SCAC may log the use of all systems and monitor all system utilization. Accounts may be closed, and files may be deleted at any time. SCAC is not responsible for any service interruptions, changes, or consequences. SCAC reserves the right to establish rules and regulations to operate electronic information services efficiently.

SCAC does not assume liability for information retrieved via the EIS nor any liability for any information lost, damaged, or unavailable due to technical or other difficulties.

Internet Safety

Focus on the prevention of inappropriate network usage includes unauthorized access, including "hacking" and other unlawful activities; unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Limits, controls, and prohibitions shall be placed on employees and students, including:

- Access to inappropriate matters.
- Safety and security in direct electronic communications.
- Unauthorized online access or activities.
- Unauthorized disclosure, use, and dissemination of personal information.

3. Education, Supervision, and Monitoring

All SCAC employees are responsible for knowing SCAC policies, applicable regulations, and procedures. Further, it is the responsibility of all employees, to the extent prudent to an individual's assignment, to educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet per this policy. The College shall provide appropriate training for employees and students who use the EIS and can access the Internet.

Training provided shall be designed to promote the commitment to:

- The standards and acceptable use of the College network and Internet services as outlined in the policy;
- Student safety regarding the use of the Internet;
- Appropriate behavior while using, but not limited to, such things as social networking websites, online opportunities, and chat rooms; proper use of personal devices; cyberbullying awareness and response.

4. Employees and Students are Strictly Prohibited from the Following Activities and Shall Not:

- Engage in unlawful communications, including threats of violence, obscenity, child pornography, and harassing communications.
- Engage in unlawful communications, including threats of violence, obscenity, child pornography, and harassing communications.
- Use College-owned or leased computer equipment "to access, download, print, or store any information, infrastructure, files, or services that depict nudity, sexual activity, and pornography"
- Make personal use of the Internet and e-mail services in a way that impedes or interferes with the conduct of College business. In general, only incidental amounts of employee time—periods comparable to reasonable coffee breaks during the day—should be used to attend to personal matters.
- Use SCAC computer resources for private business or commercial activities, fundraising, or advertising on behalf of non-SCAC organizations. Nor are they permitted to engage in the unauthorized reselling of SCAC computer resources or the unauthorized use of College trademarks or logos.
- Place links on the College website that generate or have the potential to generate revenue for SCAC or any private business (including click trade or banner advertising) without the approval of the SCAC IT Department. This is not a general prohibition against links to commercial websites.

- Alter addresses, uniform resource locator (URL), or take other action that masks the domain as a host site.
- Intercept or attempt to intercept communications by parties not authorized or intended to receive them or general unauthorized anonymous and anonymous communications. Misrepresent or forge the sender's identity or the source of electronic communication; unauthorized acquisition, attempts to acquire, or use of another person's password or the computer account of others.
- Modify or delete another person's files or account or alter the content of a message from another person or computer with intent to deceive.
- Compromise the privacy or security of electronic information intentionally or recklessly or make SCAC computing resources available to individuals not affiliated with SCAC without the approval of an authorized SCAC administrator.
- Deliberately interfere with or disrupt computer or network accounts, services, or equipment of others, propagate computer "worms" and "viruses," send electronic chain mail, or send "broadcast" messages to large numbers of individuals or hosts that are not College related.
- Disrupt electronic networks through negligent or intentional conduct; attempt to alter any SCAC computing or networking components (including, but not limited to, bridges, routers, and switches).

F. SOCIAL MEDIA

1. Guidelines for posting to social media sites

When posting to any SCAC social media site, or communicating with members of the SCAC community on *any* site, including through an employee's and student's account or when using their own phone, computer, or other device, the lists of Best Practices and Prohibited Practices must be followed.

a. Best Practices:

- Treat past and present co-workers and other individuals respectfully, regardless of different opinions. Avoid posting materials or comments that may be perceived as offensive, demeaning, inappropriate, threatening, abusive, or violating SCAC's policies against discrimination, harassment, or hostility regarding age, race, gender, sexual orientation, and gender preference.
- Without written permission, protect co-workers and students by refraining from sharing confidential or proprietary information, including conversations, statements, photos, or videos. Employees must follow federal requirements such as Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act (HIPAA).
- When posting to social media sites, employees and students must honor the copyright and intellectual property rights of others, including the College.
- Remember that laws and SCAC policies governing inappropriate conduct such as sexual (or other) harassment, bullying, discrimination, defamation, infringement of copyright and trademark rights, and unauthorized disclosure of student records and other confidential and private information apply to communications by SCAC students, faculty and staff through social media.

- If, from a social media post, it is clear that a College employee or student is mentioning the College, or it is reasonably clearly referring to the College or a position taken by the College, and also expresses a political opinion or an opinion regarding the College's positions or actions, the employee or student must specifically note that the opinion expressed is their personal opinion and not the College's position.
- Ensure the information posted is factual and accurate, as the Internet archives everything. Even deleted postings can be searched, copied, and forwarded. It is virtually impossible to eliminate posted comments or pictures from the Internet. Employees and students must not post anything in anger that would deviate from best practices.
- Employees and students must identify their views on personal sites and not suggest that such views are those of SCAC. No one may represent themselves as a spokesperson for the College unless the President or his/her designee gives direct permission to do so.
- Employees and students must accurately disclose their relationship to the College if endorsing it. When using SCAC sites or acting within the scope of College responsibilities, employees may only endorse SCAC, its programs, or its services if authorized by the College.
- Consider the accuracy, clarity, length (brief is better), and tone of written comments before posting them. Posts on social media sites should protect the College's institutional voice by remaining professional in tone and good taste. Posts may last forever, and viewers will take screenshots as evidence.
- Employees and students must sign posts with their real names and indicate their relationship to SCAC. They may not use pseudonyms or post anonymously.
- All users should respect the views of others, even if they disagree.
- Be truthful, accurate, and complete in describing SCAC programs and services.
- Strive to be accountable to SCAC audiences via regular updates and prompt responses when appropriate.
- Employees and students must obey the Terms of Service of any social media site or platform they participate in.
- Share content directly from SCAC's social media pages whenever appropriate rather than duplicating it. When content is directly shared, it is linked to SCAC's social media accounts. This facilitates analyzing social media traffic and engagement (e.g., "likes" and comments). In addition, posts originating from SCAC will have the appropriate links attached to bring the viewer back to the website or coordinating landing page.
- When SCAC faculty use social media as a means of student participation in coursework, they also need to provide a practical and appropriate alternative for students who may need help utilizing that social media platform. For example, some students may not be comfortable with opening a Facebook account.
- SCAC cannot legally prohibit employees from interacting with students on social media. However, SCAC administrators encourage staff and faculty to exercise caution and good judgment if they friend students on social media. Faculty and staff may create a separate professional or course-focused Facebook page to connect with students on social media to encourage discussions and dialogue. It is important for all staff and faculty to exercise sound judgment and to interact with students in a way that a reasonable person would find appropriate.

b. Prohibited Practices:

- Never use social media to harass, threaten, insult, defame, or bully another person

- or entity, and never use social media to engage in any unlawful act, including but not limited to gambling, identity theft, and other types of fraud.
- Never post or store content that is obscene, pornographic, defamatory, racist, excessively violent, harassing, threatening, bullying, or otherwise objectionable or injurious. In addition, do not attempt to compromise the security of any SCAC social media site or use such site to operate an illegal lottery, gambling operation, or other illegal venture.
 - Do not post copyrighted content (such as text, video, graphics, or sound files) without permission from the copyright holder. Even information widely available to the public (such as text, photographs, or other materials posted on the Internet) may be subject to copyright restrictions prohibiting unauthorized duplication or dissemination.
 - Do not post trademarked content (such as logos, names, brands, symbols, and designs) without permission from the trademark owner. The “®” symbol indicates that the mark is federally registered and the owner has the exclusive right to use it. The “TM and SM” symbols indicate that the owner may have common-law rights, but the mark is not federally registered.
 - Do not use the SCAC name, logo, or trademarks for promotional announcements, advertising, product-related press releases, or other commercial use or to promote a product, cause, political party, or candidate.
 - Only disclose confidential College information, non-public strategies, student records, or personal information concerning (past or present) members of the SCAC community with proper authorization.
 - Refrain from making false claims or representations about SCAC programs or services; do not speculate or guess if the information is not verifiable.
 - Do not spread gossip, rumors, or other unverified information. Do not assume that everything posted on a social media site is true.
 - Do not spend excessive time using social media for personal purposes during working hours or use any SCAC social media sites, networks, equipment, or peripherals for unauthorized commercial purposes.
 - Do not transmit chain letters, junk emails, or bulk communications.
 - Never be rude or argumentative or use inappropriate language. [Correct factual inaccuracies but avoid negative exchanges whenever possible.]
 - Do not represent personal opinions as institutionally endorsed by SCAC. If not authorized to post specific content on behalf of the College, then the following disclaimer must appear in a post: “These are my personal opinions and do not reflect the views of San Carlos Apache College or its staff.”
 - Do not expect posted content to remain private or that dissemination will necessarily be limited to the intended audience, even if accessing their private account over the SCAC network or using SCAC equipment or peripherals.
 - Do not insult, disparage, disrespect, or defame the College or members of the SCAC community.
 - Do not discuss legal issues or risks or conclude pending legal or regulatory matters involving the College.
 - Do not post information or conduct any online activity that may violate the San Carlos Apache Tribe’s or applicable federal laws or regulations. Any conduct

impermissible under the law, if expressed in any other form or forum, is also impermissible if expressed through social media.

2. Monitoring of Social Media by SCAC

SCAC is not responsible for monitoring or pre-screening content on its social media sites. Notwithstanding, SCAC reserves the right to monitor its sites and remove, without notice, any content that SCAC determines to be harmful, offensive, commercial, or otherwise in violation of the law or this Policy. If employees and students become aware of objectionable content posted on SCAC social media or of objectionable comments concerning the College posted on an unaffiliated site, they should notify the SCAC IT Department promptly and not reply on behalf of the College. SCAC's IT Department will work with the appropriate department(s) as necessary to address the objectionable content.

3. SCAC Social Media Site Approval, Administration, and Requirements

a. Authorization and Administration.

SCAC social media sites may be administered on behalf of (a) SCAC as an institution; (b) individual programs or departments; (c) members of the faculty in connection with a specific course; or (d) student organizations. The following policies must be followed:

- Any person or organization who seeks authorization for a new site will be expected to articulate an appropriate purpose for the site and a reasonable plan for managing its content. All new sites require approval from the IT Department.
- Institutional sites that represent SCAC as a whole must be authorized by the President of SCAC.
- Sites administered by faculty members in connection with specific courses must be authorized by the Academic Dean or Dean for Sustainability.
- The Academic Dean or Dean for Student Services must authorize sites sponsored by recognized student organizations concerning specific activities.
- When naming pages or accounts, selecting profile pictures or icons, and selecting content to post, authorized SCAC sites that represent only a segment of the SCAC community (for example, an individual College program, department, or course) should take care to avoid the appearance of representing the entire institution. Names, profile images, and posts should all be linked to the program, department, or course.
- Unauthorized use of the San Carlos Apache College name, logo, or trademarks without the express permission of an authorized officer of the College is strictly prohibited.

b. Site Administration

Social media site administration is provided by the IT Manager, the Dean for Student Services, and two staff members designated by the IT Manager.

4. Posting to Social Media Sites Not Administered by San Carlos Apache College

- a. SCAC is aware that members of the SCAC community may wish to express their ideas and opinions through private social media not administered by the College.

- b. Employees must ensure that social media activity does not interfere with their work but may use them to express their thoughts or promote their ideas as long as they do not conflict with SCAC policies. Employees should refrain from sharing confidential or proprietary information about co-workers and students. All personal positions or opinions should be posted specifically as personal views, not those of the College.

5. Confidentiality

Certain College departments possessing unique information, such as personal data, student applications, or employees' medical records or criminal histories, require specific guidelines for releasing information due to legal requirements. Employees should consider any information in these categories as confidential and covered by the College Confidentiality Agreement that the employee signs at the commencement of employment. Confidential information subject to the College's Confidentiality Agreement should be released only with the President's prior approval and only to the requesting individual whose own records are involved or in response to a Court or administrative subpoena or authorized request.

Suppose there is a question as to whether a person's right to know conflicts with maintaining confidentiality. In that case, the President will decide as to whether or not the information should be released.

Financial data regarding the College must be secured and released only as authorized by the designated supervisor. Employees of the College are expected to maintain confidentiality and are prohibited from using confidential financial information available for the benefit of themselves or others.

G. BRING YOUR OWN DEVICE

Bring your own device (BYOD) allows students to use their computers and mobile devices to connect to TOCC-related systems while on a SCAC campus and in class.

The policies do not apply to students using their own devices working remotely in online courses. The following policies apply:

- The devices must be a laptop or a convertible laptop/tablet. The best example of a convertible tablet is a two-in-one device.
- The student is solely responsible for repairing, maintaining, and updating the device. The SCAC technology department will assist students in connecting the device to the wireless network, using the wireless printing system, and connecting to SCAC-related websites.
- SCAC IT Department Staff will be available to verify minimum requirements.
- If a personal device is broken or sent off for repairs, a SCAC computer, Chromebook, and iPad with a keyboard may be available as a loan.
- The following software capabilities must be available for coursework:
 - Ability to run Google Chrome Version 78+
 - Updated virus protection if using a PC or Mac. (SCAC recommends the free Windows Defender for Windows machines)

- Security: You must have a password/passcode (login) to access the device. This is responsible computing. Students will be bound by the SCAC IT Policy related to passwords, security, and appropriate usage.
- SCAC recommends installing the Google Chrome browser, which works well with G Suite. Students collaborate with Google Docs and Microsoft 365 regularly.
- Alternative browsers, including Firefox, Internet Explorer, Opera, and other unlisted browsers, are not supported by the SCAC internet system.
- The Operating System on the student's device is a matter of personal preference. Still, the device needs to be able to run Google Chrome, Microsoft Edge, or Apple Safari Browser. Devices can run Windows, Mac OS, or Chrome OS as long as the minimum requirements are met.
- Operating System:
 - Windows 8.1, 10 or Higher
 - MacOS 10.11 or Higher
 - Chrome Version 78 or Higher
 - Battery life: 5 hours
 - Startup time: No longer than 120 seconds
 - Wireless: Integrated
 - Keyboard: Integrated, but can be wireless
 - Audio: Headphone jack with headphones/earbuds
 - Microphone: Integrated
 - Camera: Integrated
 - Processor: 1.6 GHz or faster 64-bit processor
 - Memory: 4 GB RAM or higher
 - Disk Space: 16GB GB or higher
 - Screen Size: 10 inches or larger
 - Monitor Resolution: 1024 x 768

H. VIDEO AND STREAMING

SCAC recognizes that movies and video content directly related to the instructional program may benefit student viewing. Any movies or video content shown must be directly related to courses being taught and comply with applicable copyright law and licensing agreements. When using movies and video content, the Instructor shall:

- Use approved movies and video content. Video content is typically not rated as described in this regulation. It can be used if the instructor determines, in their reasonable discretion, that all of the content is appropriate for the students to whom it will be shown. If the instructor has questions about the appropriateness of any portion of the video content, the instructor should follow the procedure described below and seek prior administrative approval.
- Do not use a personal video streaming account such as Netflix, Amazon Prime, Hulu, Disney, or others to display movies or video content.
- Not use personally obtained movies and video content licensed for home use only.

- Display only reasonable and limited portions of a copyrighted work in compliance with the fair use exception described below unless licensing fees have been paid. (The larger the portion used, the more likely the copyright violation.)
- Do not use movies and video content for entertainment or rewards.

I. WEB PUBLISHING

SCAC recognizes the value and potential of publishing on the Internet. Faculty and staff are encouraged to create electronic home pages or other pages that seek to carry out official business and communication of SCAC's mission. All such pages must be accessible to the staff and students from an official website within SCAC. All staff publishers must adhere to the policies of the College and must comply with all relevant applicable federal and state laws. Web pages shall not display personally identifiable student information unless the students have granted explicit and verifiable written permission.

Staff publishers will be responsible for maintaining their educational resource sites. Web pages must reflect positively upon SCAC. Web pages must include the e-mail address of the staff maintaining the page. E-mail addresses/links on web pages must be an apachecollege.org address. The SCAC website is maintained under the supervision of the IT Department. The Academic Dean and the IT Department must approve instructor web pages maintained by SCAC.

SCAC provides computer services and networking to enhance SCAC's educational and administrative processes and to improve communication with the world community. Material that fails to meet established educational objectives or violates a provision of policy and administrative regulations will be removed.

J. COPYRIGHTED MATERIALS

The following summary of copyright law is provided to guide employees and students.

1. Copyright Protections

United States copyright law grants certain rights and protections to the creators and publishers of creative works. Creative works that can be protected by copyright law are numerous and varied and include, but are not limited to, books, magazines, pictures, artwork, sculptures, music, movies, television shows, computer software, and video content. Generally, unless permission is received from the copyright owner, copying, creating derivative works from, and publicly displaying or performing copyrighted materials is prohibited.

Many copyright owners will issue licenses outlining acceptable terms of use for their copyrighted works. If such a license is properly obtained, the copyrighted work may be used according to the terms of the license. For example, colleges can legally show copyrighted entertainment movies for events or activities before or after the instructional day by obtaining a public performance site license.

2. Allowable Unlicensed Uses of Copyrighted Materials

There are exceptions to the general requirement that one must obtain a license to use some or all of a copyrighted work. Subject to various limitations, these exceptions allow instructors and

students to use, without first obtaining a license, some portions and/or some types of copyrighted works in face-to-face teaching activities.

3. The Fair Use Exception

The “fair use” exception allows limited use of copyrighted works without needing permission from the copyright holder. Fair use must be evaluated on a case-by-case basis. The following criteria must be considered in determining the application of the fair use exception:

- The purpose and character of the use, including whether such use is commercial or is for nonprofit educational purposes;
- The nature of the copyrighted work;
- The amount and substantiality of the portion used with the copyrighted work. (The larger the portion used, the more likely the copyright violation); and
- The effect of the use upon the potential market for or value of the copyrighted work. (It is not typically fair use to make educational copies of works intended for educational use.)

K. VIOLATIONS OF IT POLICIES

Upon receiving notice of a violation, SCAC may temporarily suspend a user’s privileges or move or delete the allegedly offending material pending further proceedings. A person accused of a violation will be notified of the charge at the appropriate time and will be able to respond before any SCAC imposes a sanction. In addition to sanctions available under applicable law and SCAC policies, SCAC may impose a temporary or permanent reduction or elimination of access privileges to computing and communication accounts, networks, SCAC-administered computing rooms, and other services or facilities.

SCAC reserves the right, under circumstances it deems appropriate and subject to applicable laws and regulations, to impose disciplinary measures, up to and including dismissal from the College or termination of employment, upon students, faculty, or staff who use private social media sites or communications resources in violation of the Usage Guidelines in this policy or are deemed to interfere with the conduct of College business. Violations of this policy are subject to sanctions prescribed in, but not limited to, the following policies: SCAC Student Handbook, SCAC Personnel Handbook, and the SCAC Faculty Handbook.

Users who misuse SCAC’s computing and network resources or who fail to comply with the college’s written usage policies, regulations, and guidelines are subject to one or more of the following consequences:

- Temporary deactivation of computer/network access;
- Permanent deactivation of computer/network access;
- Disciplinary actions taken by the appropriate Dean or President and including suspension or expulsion from school or termination of employment;
- Subpoena of data files;
- Legal prosecution under applicable federal, tribal, and/or state laws;
- Possible penalties under the law, including fines and imprisonment.

L. EQUIPMENT CIRCULATION POLICY

SCAC is pleased to provide equipment checkout services to SCAC students, faculty, and staff with a current SCAC ID. Equipment and various accessories are available to support student learning

and the academic mission of SCAC and are not available to community patrons. This policy provides guidelines on the equipment's availability, circulation, use, and user responsibilities. The borrower is responsible for returning items by the designated due date and time.

1. User Responsibilities

Individuals are responsible for understanding and adhering to the guidelines stated in this Circulation Policy and following the policies stated in this IT Policies Handbook, including the care and security of the equipment they have checked out.

- Borrowers must fill out the online Equipment Checkout Request Form at <https://www.apachecollege.org>. The equipment is on a first-come, first-served basis.
- A valid SCAC ID is required to check out San Carlos Apache College equipment.
- Users are responsible for all items checked out on their ID cards until the materials are properly checked in and listed "Returned" at SCAC.
- Users are responsible for responding promptly to all notices and for notifying the SCAC IT staff of apparent discrepancies.
- Users are responsible for reimbursement of any items that are lost or damaged while in their possession.
- Users are responsible for paying any fees or fines for damage, late return, or non-return of equipment or components.
- Users are responsible for reporting stolen equipment that they have borrowed to the police.
- Laptops are preloaded with software. Borrowers cannot alter, delete, or copy any of the available software or change its current configuration. Borrowers are prohibited from installing software, unless approved by the SCAC IT Department.

2. Lost & Damaged Items

Items that are considered lost or damaged are assessed a fee equal to the current replacement/repair cost of the item. When items are lost or stolen, students must write a statement detailing the events that lead to their equipment being lost or stolen, and return that statement, along with a police report number (for stolen items), to the SCAC IT Department.

3. Limit on Chromebooks/Laptops

Students are limited to 2 Chromebooks/Laptops as a student at SCAC to check out. Once the student has checked out 2 devices, they are no longer eligible to check out a Chromebook or Laptop.

M. COMPUTER LABS

San Carlos Apache College provides students access to computing technology resources in computer labs. Since the student population on campus is very dynamic and diverse, it is imperative that careful articulation of the policies, expectations, and standards for use of these resources be provided to them, and to the San Carlos Apache College staff and faculty who support those students in their educational endeavors.

This policy is intended to meet and to provide all campus users with guidelines for responsible and

appropriate use of these campus computing and technology resources. The primary purpose of the SCAC computer labs is to provide computing technology resources for students and to facilitate the exchange of information related to, and in furtherance of the education, research and academic missions of the College. The goals of the SCAC computer classrooms are to:

- Provide computer labs across campus that are supportive of the learning environment.
- Help assure the integrity and reliability of the SCAC internal networks, hosts on those networks, and any computing resource connected to them.
- Ensure the security and privacy of the SCAC computer systems and networks.
- Establish appropriate guidelines for the use of SCAC-owned technology.

1. Prohibited Use

Using SCAC Information Technology Resources for uses and/or communications that are specifically prohibited in the SCAC IT Policy, or which violate any other SCAC policy and/or tribal, applicable state and federal rule or law is strictly forbidden. Those specifically prohibited uses of any SCAC Information Technology Resource include:

- Subverting, attempting to subvert, or assisting others to subvert or breach the security of any SCAC network or other Information Technology Resource, or to facilitate unauthorized access.
- Use of any SCAC Information Technology Resource to create, disseminate or execute self-replicating or destructive programs (e.g., viruses, worms, Trojan horses).
- Viewing, copying, altering or destroying data, software, documentation, or data communications belonging to SCAC, or to another individual without permission.
- Individuals allowing another individual (authorized or not to use the SCAC Information Technology Resource) to use their login account password.
- Disclosing access credentials or masquerading using access granted to another user.
- Using SCAC computing resources for personal or private financial gain without written authorization.
- Unauthorized distribution of copyrighted material.

2. Access to Computing Labs

SCAC computer labs are open for computer use only by authorized faculty, staff, and currently enrolled SCAC students. Non-student adult visitors may be allowed in monitored labs, including the open lab, to assist or tutor currently enrolled students provided they do not personally use or attempt to use the Information Technology Resources for personal use. In the event of a non-student visitor violating any provisions of this policy or the computer labs procedures, the staff, including security, may instruct the visitor to leave. Non-student visitors will not be allowed into any unmonitored lab.

Faculty and staff may only use SCAC computer labs in furtherance of their support of the learning objectives of SCAC students. SCAC computer labs will not be used to perform duties or tasks normally performed in the employee's office environment. Access to any SCAC computing lab is controlled by login and password-secured accounts managed through the SCAC network.

3. Sensitive Materials

All SCAC computer labs are considered shared public places. Users should be aware that some materials accessed on the Internet may be considered controversial, offensive, inappropriate or inaccurate. SCAC asks users, out of consideration for others, to take care not to display, or broadcast in any SCAC-shared public place, any images, sounds, or messages that could create an atmosphere of discomfort, harassment or intimidation for others, and to refrain from transmitting such images, sounds or messages to others using SCAC computing resources.

In some situations, the display or broadcast of such materials is necessary to further a legitimate educational purpose. In these cases, SCAC asks that users be sensitive to the public nature of shared facilities and make arrangements to access these materials in a private environment.

In some situations, the display or broadcast of such materials, if unlawful or otherwise prohibited by this Policy could be grounds for disciplinary action.

4. General Lab Rules

- Prohibited uses
 1. Computing labs will only be used for legitimate academic purposes. Food, drink, smoking, bicycles, skateboards and pets (appropriate guide-animals are exceptions) are not permitted.
- Noise
 1. All SCAC computer labs are intended to be quiet work and study environments, similar to a library. Users are encouraged to:
 - a) Avoid excessive noise, keeping the level of conversational noise at a minimum.
 - b) Turn off or set cell phones to vibrate.
 - c) Take cell phone conversations outside the lab.
 - d) Use headphones any time music is played, either from the computer or from personally-owned devices.

5. Operating Hours

Lab hours will be posted in each lab. All users shall complete their work, including obtaining any printouts, before closing time. Users are not permitted to stay in the computer lab areas after closing time. Refusal to comply may result in sanctions.

6. Printing

Printers are provided in the SCAC computer labs as a privilege for student use only; faculty and staff should refrain from printing in a lab. Users should exercise discretion in the use of printers in computing labs. Most programs have print preview functions which should be used prior to printing any final document. Print usage on the student network may be actively monitored for abuse. Those users identified as printing excessively will be notified and asked to comply with this policy.

7. Clean Workspaces

For safety reasons, it is important that computer lab users make an effort to keep aisles clear of books and backpacks. Additionally, coats or backpacks should not be placed on computers or on tables which have been provided as workspaces in the labs. Any materials brought into a computer lab should be taken out when the user leaves. After classes are held in computer labs, instructors will clean any whiteboard, ensuring that students have cleaned their workspaces.

8. Responsibilities

All users of the SCAC computer labs have a responsibility to know, understand, and comply with this policy, to understand their responsibilities, and to meet all the expectations of this and all other SCAC IT security policies and standards. These responsibilities include assumption of any civil and/or criminal liability which may arise from their individual use or misuse of SCAC technology resources.

ACKNOWLEDGEMENT FORM

This Manual includes the authorized policies for Information Technology for SCAC. The policies provide clear standards for the appropriate use of IT resources, promote institutional efficiency and effectiveness, enhance individual accountability for ethical and lawful use, and help mitigate cyber security risks. The policies apply to all SCAC's IT Resources users, including faculty, staff, student employees, students, alumni, affiliates, contractors, consultants, collaborators, and volunteers wherever located.

All Information Technology users must agree to comply with the IT policies and acknowledge knowledge and understanding of the policies by signing the following form.

Please complete the form and return it to the SCAC Information Technology Department.

ACKNOWLEDGEMENT FORM San Carlos Apache College Information Technology Policies

This is to acknowledge that I have received a copy of the San Carlos Apache College Information Technology Policies. I understand that I must sign a new Acknowledgement Form each time it is updated.

_____ Hard Copy

_____ Electronic version.

I will immediately familiarize myself with the information in this policy. If I have questions or there are parts of these policies that I need help understanding, I will ask for clarification from my supervisor or Human Resources.

Print Name

Signature

Date

NOTE: This page will be provided to employees as a separate document to complete, sign, and return to the SCAC IT Department. It may be submitted electronically or as a hard copy.