

**USER AGREEMENT FOR ACCEPTABLE USE OF THE ELECTRONIC  
COMMUNICATION SYSTEMS AND INFORMATION RESOURCES**

The San Angelo Independent School District (the “District”) is pleased to make available to employees (faculty, staff, consultants, contractors, temporary-hires, and others), students, and approved parent users access to the interconnected computer information systems within the District (the “Network”) and to the world-wide network that provides various means of accessing significant and varied materials and opportunities (commonly known as the “Internet”). (This User Agreement applies to employees if and when they are granted access. That access may be granted to the extent that the District determines appropriate, based on the specific employee’s job duties or other factors.)

In order for the District to be able to continue to make its Network and the Internet access available, all users must take responsibility for appropriate and lawful use of this access. Users must understand that one person’s misuse of the District technology hardware or software, Network and/or the Internet access may jeopardize the ability of all to enjoy this access. While the District’s management and Network administrators will make reasonable efforts to administer use of the Network and Internet access, they must have user cooperation in exercising and promoting responsible use of this access.

This document is the Electronic Communication Systems and Information Resources Acceptable Use Policy (the “Policy” or “AUP”) of the District and also relates to Internet and other access or service providers (collectively, the “Provider”) as they provide resources necessary for the District to provide the Network and Internet access. Upon accepting your account information, you are agreeing to follow this Policy, and you will then be given the opportunity to enjoy Network and Internet access. If you have any questions about this Policy, you should contact the Technology or Human Resource departments.

If any user (that is, you or anyone whom you allow to use your account—which itself is a violation) using your account violates this Policy, your access will be denied or withdrawn. Students who violate the policy also will be subject to school discipline; employees will be subject to additional disciplinary action, up to and including, termination

**Personal Responsibility**

By accepting your account password and other information from the District and accessing the Network or the Internet, you are agreeing to follow the rules in this Policy. You are also agreeing to report any misuse of access to the Network or the Internet to your building principal or division head. Misuse means any violations of this Policy, or any other use that, while not included in this Policy, has the effect of harming another or another’s property.

You are responsible for any activity that occurs under the use of your account login. If you leave your device or user account unattended and logged in with the device unlocked, and inappropriate activity occurs, you may be held responsible for that activity. You may not give your login information to another user. (Exception: you may provide it to technical support personnel for tech support purposes but then you are responsible for changing your password after they assist you and resolve your issue.) You may not log into a computer or program and allow another user to utilize your account.

If you utilize school District equipment and/or software outside of the District, you must still follow the SAISD Technology AUP rules while utilizing the school District’s resources. (example: if you take a laptop home or offsite and access the internet, it is forbidden to surf for porn, gambling, etc.)

**Unauthorized Equipment Installation**

Personal or other purchased equipment not expressly authorized by the Director of Technology or designee will not be installed on the Network. Prohibited equipment is defined as any network attached items including, but not

limited to: hubs, switches, routers, wireless access points, splitters, network printers, key loggers, and personal PCs, laptops. Additions of any type of these items are prohibited. Persons who introduce these devices on the Network will be subject to denial of access, and disciplinary actions, including termination for employees.

## **Term of the Permitted Use**

After you have been granted access and as long as you follow this Policy, you will have Network and Internet access during the term of your enrollment or employment with the District. (Please be aware that the District may suspend access at any time for technical, policy, failure to sign and return the AUP receipt form or student handbook receipt form or other reasons.)

## **Purpose and Use**

SAISD Technology Hardware and Software, Network, Internet Access and any other technology related items are provided to staff and students primarily for official business use. Misuse can result in disciplinary actions and possibly termination. If you have any doubt about whether a contemplated activity is appropriate for District business purposes, you may consult with your building principal or division head to help you decide if a use is appropriate.

Remember, access to San Angelo ISD computer resources is a privilege, not a right. Failure to comply with the guidelines set out in the AUP may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. Student users should refer to the Student Code of Conduct for a detailed description of the consequences of improper use of the computer system.

## **Computing and Software Usage**

Software will be used only in accordance with its license agreement. Unless otherwise provided in the license, any duplication of copyrighted software, except for backup and archival purposes by the Technology Director or designee, is a violation of copyright law. In addition to violating copyright law, unauthorized duplication of software is contrary to the District's standards of conduct. The following points are to be followed to comply with software license agreements:

- All users must use all software in accordance with license agreements and the District's software regulation. All users acknowledge that they do not own this software or its related documentation, and, that unless expressly authorized by the software publisher, may not make additional copies except for archival purposes.
- The District will not tolerate the use of any unauthorized copies of software or fonts in our school system. Any person illegally reproducing software can be subject to civil and criminal penalties including fines and imprisonment. According to the U.S. Copyright Act, illegal reproduction of software is subject to civil damages of as much as U.S. \$100,000 per title infringed, and criminal penalties, including fines of as much as U.S. \$250,000 per title infringed, and imprisonment of up to five years. A District user, who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the circumstances. Such discipline may include termination of employment. The District does not condone the illegal duplication of software and will not tolerate it.
- No user will give software or fonts to any outsiders, including consultants, suppliers, contractors, and others. Under no circumstances will the District use software that has been brought in from any unauthorized location under the District's policy, including, but not limited to, the Internet, home, friends, and colleagues without approval from the Technology Director or designee.
- Any user who determines that there may be a misuse of software within the District will notify the Director of Technology, building principal, and/or division supervisor.
- All software used by the District on District-owned computers will be purchased through appropriate procedures.
- Generally, District-owned software cannot be taken home and loaded on an employee's home computer if it also resides on a District computer. If an employee is required to use software at home, the appropriate cost center manager will purchase a separate package and record it as a District owned asset in the software register with the Technology Department. However, some software companies provide in their license agreements that home use is permitted under certain circumstances. If an employee is required to use software at home, he or she must first consult with the Technology Help Desk, unless allowed under the

software's license agreement, to determine if appropriate licenses allow for home use. The Technology Department will conduct a yearly audit (at least once a year), of all District PCs and servers, including portables, to ensure that the District is in compliance with all software licenses. Random audits may be conducted as well. Audits may be conducted using an auditing software product. The full cooperation of all users is required during audits.

Employee use of handheld computing/communication devices (e.g. personal digital assistants (PDA), smart phones, WAP phones, and other personal communication devices) that use any medium to synchronize, transmit, share, or access files on remote computer or server is permitted with some limitations. Synchronization with Microsoft Outlook calendars, contacts, messages, and notes is permitted. Employees who possess District e-mail accounts may access their account via their handheld computing/communication device. The specific details of this privilege are outlined in the next section.

The District is not responsible for maintaining, repairing, or otherwise troubleshooting an employee's personal cellular or other electronic devices. The District is not responsible for damage, corruption, modification, and/or deletion of any personal data stored on any employee-owned handheld computing/communication device. Furthermore, the District makes no guarantees of service quality or access regarding handheld devices. Modems or wireless broadband wireless devices inside or connected to office desktop computers (PCs) are not permitted, unless specifically authorized by the Director of Technology. Home based, mobile and/or telecommuting computers are an exception to this rule.

Computer equipment supplied by the District must not be altered or added to in any way (e.g., upgraded processor, expanded memory, or extra circuit boards) without prior knowledge and authorization from the Technology and Information Services Department. Unauthorized system changes or components may be removed by Technology Department Staff. On District-supplied computer hardware, workers must not change the operating system configuration or install new software. If such changes are required, they will be performed by Technology Department personnel.

### **Accessing District Internet, E-mail, or Other District Resources via Cellular Phone or other Handheld Communication Device**

Employees who choose to access the District's Internet or their own District e-mail accounts on their personal handheld communication device (e.g., cell phone, Palm Pilot, etc.) may do so subject to the following restrictions and requirements.

The same standards of proper and professional use of the District Internet and District e-mail system apply (including the entirety of this Policy, as well as any provisions applicable from Board Policy (CQ (LEGAL), CQ (LOCAL)), or Employee Handbook, and any other applicable rules or policies) regardless of whether the District services at issue are accessed via District computer or personal device.

Use of personal cell phones or other handheld communication devices for business purposes should be limited. Employees are expected to conduct themselves in a professional manner when corresponding as employees of the District, and failure to do so may result in disciplinary action where the behavior or conduct is school related (example: sending threatening text messages to a coworker from a personal cell phone).

Although employees are permitted to use their cell phones to access District e-mail and for other acceptable business purposes, a cell phone should not be used in place of the employee's District computer or telephone. Personal cell phones may be used for school business calls, including parent contacts, only during planning periods and other off-duty times during the work day. [See Employee Handbook, pg. 52]. Personal cellular phones should be used for school business only when District telephone and computer access is not readily available. Employees who use other functions of personal cell phones for business purposes (e.g., sending text messages to other employees concerning business, or sending text messages or e-mail containing personally identifiable student information), should limit such use to those instances when other forms of communication are not readily available. An employee who allows the use of his or her cell phone to interfere with the performance of job duties may be subject to discipline. [Consult Employee Handbook for consequences of such conduct].

The District strongly encourages employees who choose to use personal communication devices for business purposes to protect those devices with “password protection”, blocking any unauthorized users access to its contents. An employee who accesses his or her District e-mail from a cell phone should make a report to the District Technology Department immediately if the cell phone is lost or stolen. The possibly delicate and/or confidential information which could be present on the cell phone is of immediate concern to the District.

Electronic mail transmissions and other use of the District’s electronic communications system by students and employees shall not be considered private. The District reserves the right to monitor access to and use of District e-mail, District Internet, or other network or computer-related activity, engage in routine computer maintenance and housekeeping, carry out internal investigations, prepare responses to requests for public records, or disclose messages, data, or files to law enforcement authorities. Monitoring shall occur at any time to ensure appropriate use.

**Reminder: As an employee of a public school district, your communications regarding District business may be subject to public information act requests. Consider this possibility before sending any communication from a cell phone, or other similar device, which contains information or issues of District business.**

## **Networking and Internet Usage**

Employees using District accounts are acting as representatives of San Angelo ISD. As such, employees should act accordingly to avoid damaging the reputation of the school District. The introduction of viruses, spyware, adware, malware, any malicious code or tampering with any computer system, is expressly prohibited. Files that are downloaded from the Internet must be scanned with virus detection software before installing or execution. All appropriate precautions should be taken to detect for a virus and, if necessary, to prevent its spread.

The truth or accuracy of information on the Internet and in e-mail should be considered suspect until confirmed by a separate (reliable) source. Users shall not place SAISD material (copyrighted software, internal correspondences, etc.) on any publicly accessible Internet computer without proper permission. Alternate Internet Service Provider (ISP) connections (such as AOL dial-up) to the District’s internal network are not permitted unless expressly authorized and properly protected by a firewall or other appropriate security device(s).

Unless otherwise noted, all software on the Internet should be considered copyrighted work. Therefore, users are prohibited from downloading software and/or modifying any such files without permission from the copyright holder.

## **Electronic Messaging Communications and Voice Mail Systems**

The District’s voice communications and voice mail systems are designed to assist us in better serving stakeholders, enhancing internal communications, and reducing unnecessary paperwork. These guidelines should govern your use of District equipment, with special attention to unified messaging (email, voice mail, facsimiles and video mail.)

Privacy is not assured in e-mail, facsimiles, video mail, or voice mail messages, whether a password is used or not. The Telecommunications Manager must have access to all program related passwords at all times, to ensure necessary access to the system. Misuse of passwords or the unauthorized use of another employee’s password will result in disciplinary action, up to and including termination. The District may access all employees’ messages at any time.

E-mail messages are like paper documents: Ask yourself whether you would want anyone else knowing about the content, or whether a conversation would be more appropriate.

**Reminder: E-Mail is subject to public information act requests (PIA) and is admissible in court in some cases. Keep in mind when you compose an e-mail message that it could possibly be read by anyone or could appear in the local newspaper if requested via a PIA request.**

Be careful when sending sensitive data via e-mail. It may need to be password protected and possibly encrypted. Review the requirements of HIPAA and FERPA laws which prohibit disclosure of certain student information. Electronic/Voice mail usage must conform to the District’s policies against harassment and discrimination. Messages containing defamatory, obscene, offensive, or harassing information, or messages that disclose personal

information without authorization, are prohibited. If you receive such unsolicited messages, you are to delete them promptly and not forward them.

Chain-type messages and executable graphics also should be deleted and not forwarded---they cause overload on our system. Employees engaging in the transmission of inappropriate electronic messaging, as determined by the District, will be subject to discipline, up to and including termination. For further information regarding the District's policy against sexual and other unlawful harassment, refer to the student code of conduct or the employee manual.

When using e-mail, users should use "e-mail etiquette." For example, avoid the use of all capital letters, as this is considered to be shouting at someone electronically. If you create private mail groups, it is your responsibility to review them periodically so they remain current. The Technology Department will have responsibility for generating and maintaining public mail distribution lists.

Users should be mindful of District regulations regarding e-mail retention periods. It is your responsibility to archive any messages that you do not wish to be automatically deleted.

E-mail and Internet access should not be overused or misused. Misuse of electronic access (i.e., work time spent online for personal use, copying or downloading copyrighted materials, visiting inappropriate sites, online banking, day trading/stock trading, online dating, online gambling, participating in online auctions, etc.) may result in discipline.

Employees and vendors must not make arrangements for, or actually complete installation of voice or data lines with any carrier, if they have not first obtained approval from the Director of Technology or designee.

## **Information Security and Access**

All users (including third parties) are responsible for the activity performed with their personal user-IDs, whether or not these user-ID's are connecting via external network facilities. User-IDs must never be shared with associates, friends, family members, or others. User-IDs may not be utilized by anyone but the individuals to whom they have been issued. Similarly, users are forbidden from performing any activity with user-IDs belonging to other individuals (excepting authorized anonymous user-IDs like "guest"). With the exception of the District intranet, users must not browse through District computer systems or networks. For example, curious searching for interesting files and /or programs in the directories of other users is prohibited. Steps taken to legitimately locate information needed to perform one's job is not considered browsing. This statement on browsing does not apply to external networks such as the Internet.

Confidential information never should be sent over the Internet without the knowledge that it can be intercepted. This includes the transmission of documents containing District financial information, human resource information, student information, or Social Security Numbers. Use extreme caution to ensure that the correct e-mail address is used for the intended recipient(s). If you are sending a document that contains sensitive information, it is recommended that you secure the document; for example, via password, encryption, use of secure socket transfer, etc.

## **Prohibited Use**

The user is responsible for his/her actions and activities involving District computers, networks, and Internet services, and for his/her computer files, passwords and accounts. General examples of unacceptable uses which are expressly prohibited include, but are not limited to, the following:

- Any use that is illegal or in violation of other board policies, including harassing, discriminatory or threatening communications and behavior; violations of copyright laws, etc.;
- Any use involving materials that are obscene, pornographic, sexually explicit or sexually suggestive;
- Any inappropriate communications with students or minors;
- Any use for private financial gain, or commercial, advertising or solicitation purposes;
- Any use as a forum for communicating by e-mail or any other medium with other school users or outside parties to solicit, proselytize, advocate or communicate the views of an individual or nonschool sponsored

organization; to solicit membership in or support of any non-school sponsored organization; or to raise funds for any non-school sponsored purpose, whether profit or not-for-profit.

- No employee shall knowingly provide school e-mail addresses to outside parties whose intent is to communicate with school employees, students and/or their families for non-school purposes. Employees who are uncertain as to whether particular activities are acceptable should seek further guidance from the building principal or other appropriate administrator.
- Any communication that represents personal views as those of the District or that could be misinterpreted as such;
- Downloading or loading software or applications without permission from the system administrator;
- Opening or forwarding any e-mail attachments (executable, batch, and/or script files) from unknown sources and/or that may contain viruses or malicious software;
- Sending mass e-mails to District users or outside parties for school or non-school purposes without the permission of the system administrator [or other designated administrator].
- Any malicious use or disruption of the District's computers, networks, and Internet services or breach of security features;
- Any misuse or damage to the District's computer equipment;
- Misuse of the computer passwords or accounts (employees, students, or other users);
- Any communications that are in violation of generally accepted rules of network etiquette and/or professional conduct, including the use of profanity or vulgar, obscene or sexually explicit language;
- Any attempt to access inappropriate/unauthorized sites (i.e. Internet/Websites, intranet websites, and/or application servers);
- Failing to report a known breach of computer security to the system administrator;
- Executing, using, or viewing any application or website that is resource intensive, resulting in excessive network saturation and denial-of-service for other users;
- *Users* using District computer networks are prohibited from gaining unauthorized access to any information system or network to which they have not been expressly granted access. *Users* using District computer networks are also prohibited from in any way damaging, disrupting, or interfering with the operations of multi-user information systems to which they are connected. Likewise, *users* are prohibited from capturing or otherwise being in possession of passwords, encryption keys, or any other access control mechanism that has not been expressly assigned to them. *Users* are furthermore prohibited from possessing or using software tools which could provide unauthorized access to system resources (these include password dictionary attack programs, encryption key brute-force discovery programs, and software for defeating copy-protection mechanisms).
- Using school computers, networks, and Internet services after such access has been denied or revoked;
- Any attempt to delete, erase, or otherwise conceal any information stored on a school computer that violates these rules;
- Use that violates this Policy, the student code of conduct or the employee standards of conduct;
- Unauthorized disclosure, use, or distribution of personally identifiable information or personal identification regarding students or employees;
- Personal or political use to advocate for or against a candidate, office-holder, political party, or political position. Research or electronic communications regarding political issues or candidates shall not be a violation when the activity is to fulfill an assignment for class credit;
- Participating in chat rooms other than those approved, sponsored and/or overseen by the District; and/or
- The use of personal devices such as PDA's (Palms, Visors, cell phones with web capability, etc.) and laptops (either wireless or Ethernet) or any device used to access SAISD Networks is prohibited unless this Policy provides otherwise.

## **No Expectation of Privacy**

Electronic mail transmissions and other use of the electronic communications system by students and employees shall not be considered private. Employees have no expectation of privacy in their use of District computing and network resources, including electronic messaging (e-mail), online chatting, any stored files, etc.

The District reserves the right to monitor, track, and report access to and use of District e-mail, the Internet, or other network or computer-related activity, engage in routine computer maintenance and housekeeping, carry out internal

investigations, prepare responses to requests for public records, or disclose messages, data, or files to law enforcement authorities. Monitoring by designated District staff shall occur at any time to ensure appropriate use.

### **Confidentiality of Information**

Employees are expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential. When engaging in written communication regarding any student, employees should avoid using the student's name or ID number, and instead should use the student's initials if possible.

### **Staff Responsibilities to Students**

Teachers, staff members, and volunteers who use District computers for instructional purposes with students must supervise such use. Teachers, staff members and volunteers are expected to be familiar with the District's policies and rules concerning student computers and Internet use and to enforce them. When, in the course of their duties, employees/volunteers become aware of student violations, they are expected to stop the activity and inform the building principal [or other appropriate administrator].

### **Compensation for Losses, Costs and/or Damages**

Users shall be responsible for any losses, costs or damages incurred by the District related to violations of policy CQ and/or these rules.

### **District Assumes No Responsibility for Unauthorized Charges, Costs, or Illegal Use**

The District assumes no responsibility for any unauthorized charges made by users, including but not limited to credit card charges, subscriptions, long distance charges, equipment and line costs, online gambling charges or debts, or for any illegal use of its computers such as copyright violations. Therefore, the District will hold the user liable for the user's actions.

### **User Acknowledgement Required**

Each user authorized to access the District computers, networks, telecommunications, and Internet services is required to sign an acknowledgement form (CQ Exhibit D), or the Employee or Student Handbook stating that they have read policy CQ and these rules. As a condition of continued employment, employees, consultants, and contractors must annually sign an acceptable usage policy or SAISD Employee or Student Handbook. The acknowledgement form will be retained in the employee's personnel file or in the Technology Department's files. Agreements from students will be maintained in campus records, as will Agreements from parents and volunteers.

**San Angelo ISD  
226-903**

**ELECTRONIC COMMUNICATION AND DATA MANAGEMENT  
EXHIBIT D**

**CQ  
(EXHIBIT)**

**ACKNOWLEDGEMENT OF USER AGREEMENT FOR ACCEPTABLE USE OF  
THE ELECTRONIC COMMUNICATION SYSTEMS AND INFORMATION RESOURCES**

**User Signature Required**

Each user authorized to access the District computers, networks, telecommunications, Internet services, or other resources is required to sign an acknowledgement form (CQ Exhibit D) or the Employee or Student Handbook stating that they have read policy CQ and these rules. As a condition of continued employment, employees, consultants, and contractors must annually sign an acceptable usage policy or SAISD Employee Handbook. The acknowledgement form will be retained in the employee's personnel file or in the Technology Department's files. Agreements from students will be maintained in campus records, as will Agreements from parents and volunteers.

I hereby acknowledge that I have received information related to the User Agreement for Acceptable Use of the Electronic Communications Systems and Information Resources (commonly known as "Acceptable Usage Policy") as required on Board Policy CQ (LEGAL) and CQ (LOCAL). I further acknowledge that I have been offered the option to receive a paper copy of said agreement or to electronically access them. I agree to review the Acceptable Usage Policy by accessing the web sites provided or by requesting, in writing, a paper copy from the appropriate department.

---

Printed Legal Name

---

Staff or Student ID Number (not applicable if you are not a staff member or a student)

---

Campus/Location or Company Name

---

Role: Student, Volunteer, or Employment Position

---

Date

---

User Signature