

Sonora Independent School District Electronic Communication and Data Management System Acceptable Use Policy

The Sonora Independent School District provides an array of technology resources for faculty and staff use to promote educational excellence in its schools by facilitating resource sharing, innovation, and communication. This agreement outlines appropriate use and prohibited activities when using technology resources at school and all school related functions. Any use of the District's information and communication systems and resources by authorized users must be in furtherance of these limited purposes and conform to the District's expectations for legal, efficient, and ethical use.

Sonora ISD (SISD) provides users access to the District's electronic communications system for educational purposes. The District's computer systems and networks (system) are any configuration of hardware and software. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed. The electronic communications system includes but is not limited to the following:

- Telephones, cellular telephones, and voicemail technologies;
- Email accounts;
- Servers and network equipment;
- Computer hardware (including Chromebooks, mobile devices, tablets, i-devices) and peripherals;
- Software including operating system software and application software;
- Digitized information including stored text, data files, email, digital images, and video and audio files;
- Internally or externally accessed databases, applications, or tools (Online/Internet- or District- server based);
- District-provided filtered Internet access;
- District-provided filtered Wi-Fi;
- Videoconferencing capabilities;
- Message board; and
- New technologies as they become available.

These technologies, when properly used, promote educational excellence in the District by facilitating resource sharing, innovation, and communication. Illegal, unethical or inappropriate use of these technologies can have dramatic consequences, harming the District, its students and its employees. This Acceptable Use Policy is intended to minimize the likelihood of such harm by educating District system users and setting standards, which will serve to protect the District. The District firmly believes that digital resources, information and interaction available on the computer-device/network/Internet far outweigh any disadvantages.

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.

Authorized Users

The District permits individuals in the following categories to become authorized users of its computer network and/or have access to the Internet, subject to administrative regulations developed by the Technology Director and approved by the Superintendent.

- Campus administrators and campus administrative support employees.
- Central office administrators (department or division directors) and their administrative support employees.
- Instructional personnel.
- Instructional support and student services personnel, i.e., librarians, counselors, and school nurses.

- Students in grades Pre-Kindergarten to Twelfth grades.
- School board members.
- Temporary workers (substitute Teacher, Consultants, etc.)

Availability of Access

Acceptable Use. Computer/Device/Network/Internet access will be used to enhance learning consistent with the District's educational goals. The District requires legal, ethical and appropriate computer/device/network/Internet use.

Privilege. Access to the District's computer/device/network/Internet is a privilege, not a right, and administrators and faculty may review files and messages to maintain system integrity to ensure that users are acting responsibly.

Access to Computer/Device/Network/Internet. Access to the District's electronic communications system, including the Internet, shall be made available to staff and students for instructional purposes. Each District computer-device and Wi-Fi has filtering software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act (CIPA). Filtered Internet access is provided to students as defined by CIPA. However, while the District uses filtering technology and protection measures to restrict access to inappropriate material; it is not possible to absolutely prevent such access. It is each user's responsibility to follow the rules for appropriate and responsible use.

Student Access. Computer/Device/Network/Internet access is provided to all students unless parents or guardians request in writing to the campus principal that access be denied. Student Internet access will be under the direction and guidance of a District staff member.

Students 13 or younger. For students under the age of 13, the Children's Online Privacy Protection Act (COPPA) requires additional parental permission for educational software tools. Parents wishing to deny access to these educational tools must do so in writing to the campus principal indicating their child should be denied access to these tools. Examples of these tools are Discovery Education, wikis, blogs, and Edmodo.

Security. A student or staff member who gains access to any inappropriate or harmful material is expected to discontinue the access and to report the incident to the supervising staff member. Any user identified as a security risk or as having violated the Acceptable Use Policy may be subject to suspension of access to school owned devices/computer/network and/or Internet as well as disciplinary action.

A user who knowingly brings prohibited materials into the school's electronic environment will be subject to suspension of access to school-owned devices/computer/network and/or Internet on the District's system. Students will be subject to disciplinary action in accordance with the Board approved Student Handbook and/or Student Code of Conduct. Staff will be subject to disciplinary action in accordance with board policy and the Employee Handbook.

Content/Third-Party Supplied Information. Staff, students and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communication systems in the global electronic network that may contain inaccurate and/or objectionable material.

Subject to Monitoring. All District computer/device/network/Internet usage shall not be considered confidential and is subject to monitoring by designated staff at any time to ensure appropriate use. Users should not use the computer system to send, receive or store any information, including email messages, that they consider personal or confidential and wish to keep private. All electronic files, including email messages, transmitted through or stored in the computer system will be treated no differently than any other electronic file. The District reserves the right to access, review, and copy, modify, delete or disclose such files for any purpose. Users should treat the computer system like a shared or common file system with the expectation that electronic files, sent, received or stored anywhere in the computer system, will be available for review by any authorized representative of the District for any purpose.

Student Computer-Device/Network/Internet Responsibilities

District users are bound by all portions of the Acceptable Use Policy. A student who knowingly violates any portion of the Acceptable Use Policy will be subject to suspension of access to school owned devices/computer/network and/or Internet as well as disciplinary action in accordance with the Board approved Student Handbook and/or Student Code of Conduct. Staff who violates guidelines will be subject to disciplinary action in accordance with board policy and the employee handbook.

Use of Digital Tools. Users may participate in District-approved social media learning environments related to curricular projects or school activities and use digital tools, such as, but not limited to, Google Classroom, blogs, discussion forums, RSS feeds, podcasts, wikis, and on-line meeting sessions. The use of blogs, wikis, podcasts, and other digital tools are considered an extension of the classroom. Verbal or written language that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, wikis, podcasts, and other District-approved digital tools.

Use of System Resources. Users are asked to purge email or outdated files on a regular basis. Users must not waste or abuse school resources through unauthorized system use (e.g. playing games online, downloading music, watching video broadcasts, participating in chat rooms, etc. that are not educational).

Password Confidentiality. Users are required to maintain password confidentiality by not sharing their password with others. Users may not use another person's system account.

Reporting Security Problem. If knowledge of inappropriate material or a security problem on the computer/device/network/Internet is identified, the user should immediately notify the supervising staff member. The security problem should not be shared with others.

Telecommunication Device.

- Non-school network equipment, air-cards, routers, tethering or hotspots is not allowed to be used by student or staff.
- Telecommunication devices are only to be used for educational purposes at the direction of a classroom teacher.
- Campus administrators and staff members have the right to prohibit use of devices at certain times or during designated activities (i.e. campus presentations, theatrical performances, or guest speakers) that occur during the school day.
- An appropriately-trained administrator may examine a student's personal telecommunication device and search its contents, in accordance with the Student Handbook and/or Student Code of Conduct.

Rules of Appropriate Use

- Users are assigned an individual account for hardware and Internet access and are responsible for not sharing the password for that account with others.
 - Users are responsible for any activity that occurs under the use of their login.
 - If users leave their device or user account unattended and logged in with the device unlocked, and inappropriate activity occurs, users may be held responsible for that activity.
 - Users may not give their login information to another user. (Exception: users may provide it to technical support personnel for tech support purposes.)
 - Users may not log into a computer or program and allow another user to utilize their account.

- Users will be held responsible at all times for the proper use of District technology resources, and may be subject to suspension of access to school owned devices/computer/network and/or Internet access if rules are violated.
- The account is to be used primarily for educational purposes, but some limited personal use is permitted. Limited personal use is permitted so long as it imposes no tangible cost on the District; does not unduly burden the District's technology resources; and has no adverse effect on an employee's job performance or on a student's academic performance.
- As applicable, users must comply with the District's record management program, the Texas Open Meetings Act, the Public Information Act, the Family Educational Rights and Privacy Act (FERPA), including retention and confidentiality of student and district records, and campaign laws.
- As applicable, users must maintain the confidentiality of health or personnel information concerning students, district employees and colleagues, unless disclosure serves lawful professional purposes or is required by law.
- Remember that people who receive email from users with a school address might think the message represents the school's point of view.

Inappropriate Use

Inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations in this document, that violate the rules of network etiquette, or that hamper the integrity or security of this computer/device/network/Internet system or any components that are connected to it. The following actions are considered inappropriate uses, are prohibited, and will result in suspension of the student's access to the computer/device/network/Internet.

Violations of Law. Using technology resources for any illegal purpose or in violation of district policy. Transmission of any material in violation of any federal or state law is prohibited. This includes, but is not limited to:

- threatening, harassing, defamatory or obscene material;
- copyrighted material;
- plagiarized material;
- material protected by trade secret; or
- blog posts, Web posts, or discussion forum/replies posted to the Internet which violate Federal or state law.

Tampering with or theft of components from District systems may be regarded as criminal activity under applicable state and federal laws. Any attempt to break the law with the use of a District computer/device/network/Internet account may result in prosecution against the offender by the proper authorities. If such an event should occur, the District will fully comply with the authorities to provide any information necessary for legal action.

Modification of District-Owned Devices. Modifying or changing computer settings and/or internal or external configurations without appropriate permission is prohibited.

Transmitting Confidential Information. Users may not redistribute or forward confidential information without proper authorization. Confidential information should never be transmitted, redistributed or forwarded to outside individuals who are not expressly authorized to receive the information. Revealing personal information by students about oneself such as, but not limited to, home addresses, phone numbers, email addresses, or birthdates of others is prohibited.

- Users should not respond to requests for personally identifying information or contact from unknown individuals.
- Making appointments to meet in person with people met online. If a request for such a meeting is received, it should be reported to a teacher or administrator immediately.

Commercial Use. Use of the system for any type of income-generating activity is prohibited. Advertising the sale of products, whether commercial or personal is prohibited.

Marketing by Non-Sonora ISD Organizations. Use of the system for promoting activities or events for individuals or organizations not directly affiliated with or sanctioned by the District is prohibited.

Vandalism/Mischief. Any malicious attempt to harm or destroy District equipment, materials or data, or the malicious attempt to harm or destroy data of another user of the District's system, or any of the agencies or other networks to which the District has access is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above is prohibited and will result in the cancellation of system use privileges. Users committing vandalism will be required to provide restitution for costs associated with system restoration and may be subject to other appropriate consequences.

Intellectual Property. Users must always respect copyrights and trademarks of third-parties and their ownership claims in images, text, video and audio material, software, information and inventions. The copy, use, or transfer of others' materials without appropriate authorization is not allowed.

Copyright Violations. Downloading or using copyrighted information without following approved District procedures is prohibited.

Plagiarism. Fraudulently altering or copying documents or files authored by another individual is prohibited.

Impersonation. Pretending to be someone else when posting, transmitting, or receiving messages. Attempts to log on to the computer/device/network/Internet impersonating a system administrator or District employee, student, or individual other than oneself, will result in suspension of access to school owned devices/computer/network and/or Internet.

Illegally Accessing or Hacking Violations. Intentional or unauthorized access or attempted access of any portion of the District's computer systems, networks, or private databases to view, obtain, manipulate, or transmit information, programs, or codes is prohibited.

File/Data Violations. Deleting, examining, copying, or modifying files and/or data belonging to other users, without their permission, is prohibited.

System Interference/Alteration. Deliberate attempts to exceed, evade or change resource quotas are prohibited. The deliberate causing of network congestion through mass consumption of system resources is prohibited.

- Damaging electronic communication systems or electronic equipment including: a) knowingly or intentionally introducing a virus to a device or network, or not taking proper security steps to prevent a device or network from becoming vulnerable; b) disfiguring or altering equipment, or displaying lack of reasonable care in its use.
- Disabling or attempting to disable any Internet filtering device. Requests to disable a filtering device should be made to the District's Technology Help Desk.
- Accessing sites not authorized under the District's filtering policies. Encrypting communications to avoid security review.
- Attempting to read, delete, copy, modify, or interfere with another user's posting, transmittal, or receipt of electronic media.
- Sending unauthorized broadcasts to official or private distribution lists, regardless of content or recipients.
- Gaining unauthorized access to restricted information or resources.

- The introduction of viruses, spyware, adware, malware, any malicious code or tampering with any computer system, is expressly prohibited.
- Wasting school resources through improper use of the District's technology resources, including creating and distributing chain letters, sending spam, or setting up equipment so that it can act as an "open relay" for third-party spammers, or providing products or services for pay, i.e., outside employment.
- Users may not attach personal network equipment to the Sonora ISD network unless approved by the Sonora ISD Technology Dept. (ex: hubs, routers, switches, wireless access points, etc.)

Harassment, Use of Inappropriate Language and Posting of Pictures without Permission. Using resources to engage in conduct that harasses or bullies others.

- Posting, transmitting, or accessing materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
- Using inappropriate language such as swear words, vulgarity, ethnic or racial slurs, and any other inflammatory language.
- Posting or transmitting pictures of students without obtaining prior permission from all individuals depicted or from parents of depicted students who are under the age of 18.

Cyberbullying. The use of any Internet-connected device for the purpose of bullying, harassing, or intimidating another student and is prohibited. This includes, but may not be limited to:

- Sending abusive text messages to cell phones, computers, or Internet-connected game consoles.
- Posting abusive comments on someone's blog or social networking site (e.g., Instagram, Snapchat, or Facebook).
- Creating a social networking site or web page that masquerades as the victim's personal site and using it to embarrass him or her.
- Making it appear that the victim is posting malicious comments about friends to isolate him or her from friends.
- Posting the victim's personally identifiable information on a site to put them at greater risk of contact by predators.
- Sending abusive comments while playing interactive games.
- Recording and distributing media with the intent to manipulate or embarrass others.

Email and Communication Tools

Email and other digital tools such as, but not limited to, blogs and wikis, are tools used to communicate within the District. The use of these communication tools should be limited to instructional, school-related activities, or administrative needs.

Users may be issued email accounts. Users should check email frequently, delete unwanted messages promptly, and stay within the email server space allocations.

Sonora ISD reserves the right to monitor all activity in Sonora ISD electronic resources, included district provided email accounts. Commercial use of Sonora ISD electronic resources is strictly prohibited.

Sonora ISD shall not be liable for a user's inappropriate use of Sonora ISD electronic resources or violation of copyright restrictions or other laws or for any costs incurred by users through the use of SISD electronic resources

Reminder: E-Mail is subject to public information act requests (PIA) and is admissible in court in some cases. Keep in mind when composing 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 any unsolicited messages are received, delete them promptly and not forward them.

Users should keep the following points in mind:

Perceived Representation. Using school-related email addresses, blogs, wikis, and other communication tools might cause some recipients or other readers of the email to assume that the user's comments represent the District or school, whether or not that was the student's intention.

Privacy. Email, blogs, wikis, and other communication within these tools should not be considered a private, personal form of communication. Private information, such as home addresses, phone numbers, last names, pictures, or email addresses, should not be divulged. To avoid disclosing email addresses that are protected, email communications to multiple recipients, who are outside of the district, should be sent using the blind carbon copy (bcc) feature.

Inappropriate Language. Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language in emails blogs, wikis, or other communication tools is prohibited. Sending messages that could cause danger or disruption, personal attacks, including prejudicial or discriminatory attacks are prohibited.

Political Lobbying. Consistent with State ethics laws, District resources and equipment, including, but not limited to, emails, blogs, wikis, or other communication tools must not be used to conduct any political activities, including political advertising or lobbying. This includes using District email, blogs, wikis, or other communication tools to create, distribute, forward, or reply to messages, from either internal or external sources, which expressly or implicitly support or oppose a candidate for nomination or election to either a public office or an office of a political party or support or oppose an officeholder, a political party, or a measure (a ballot proposition). These guidelines prohibit direct communications as well as the transmission or forwarding of emails, hyperlinks, or other external references within emails, blogs, or wikis regarding any political advertising.

Forgery. Forgery or attempted forgery of email messages is prohibited. Attempts to read, delete, copy or modify the email of other system users, deliberate interference with the ability of other system users to send/receive email, or the use of another person's user ID and/or password is prohibited.

Junk Mail/Chain Letters. Generally users should refrain from forwarding emails which do not relate to the educational purposes of the District. Chain letters or other emails intended for forwarding or distributing to others is prohibited. Creating, distributing or forwarding any annoying or unnecessary message to a large number of people (spamming) is also prohibited.

Student Email Accounts and Electronic Communication Tools

Electronic communication is an important skill for 21st Century students. By providing this tool, the District is equipping students with the skills necessary for success in the business world. Students in grades 6 - 12 may be given access to a District student email account. Parents wishing to deny access to District email must do so in writing to the campus principal. As appropriate, project email accounts may be granted for educational activities for students in grades K-5 at the request of the classroom teacher. Student email accounts may be provided directly by the District, through the content management system of an approved online course, or through a District-approved provider.

Digital Citizenship

Sonora ISD users will use information and technology in safe, legal, and responsible ways. Users will embrace the following conditions or facets of being a digital citizen.

- **Respect Yourself:** I will select online names that are appropriate, and I will adhere to District Guidelines when posting information and images online. I will not share inappropriate information or graphics with others.
- **Protect Yourself:** I will not publish my personal details, contact details, or a schedule of my activities.
- **Respect Others:** I will not use technologies to bully or tease other people.
- **Protect Others:** I will protect others by reporting abuse and not forwarding inappropriate materials or communications.
- **Respect Intellectual Property:** I will suitably cite any and all use of websites, books, media, etc.
- **Protect Intellectual Property:** I will request to use the software and media others produce.

Consequences of Agreement Violation

Any attempt to violate the provisions of this agreement may be subject to suspension of access to school owned devices/computer/network and/or Internet, regardless of the outcome of the attempt. In addition, school disciplinary and/or appropriate legal action may be taken.

Denial or Suspension of Access Privileges. With just cause, the Director of Technology and/or building principal, may deny, suspend, or terminated computer/device/network/Internet access as required.

A user whose access has been suspended or terminated may request a conference with the principal and Technology Director to discuss the basis for that action and have an opportunity to respond. A decision by the Technology Director to suspend or terminate system privileges may be appealed to the Superintendent or the Board.

Warning

Sites accessible via the computer/device/network/Internet may contain material that is illegal, defamatory, inaccurate or controversial. Each District computer with Internet access has filtering software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act. The District makes every effort to limit access to objectionable material; however, controlling all such materials on the computer/device/network/Internet is impossible, even with filtering in place. With global access to computers and people, a risk exists that students may access material that may not be of educational value in the school setting.

Disclaimer

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not guarantee that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected. Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.

Acknowledgement of Acceptable Use Policy

User Signature Required

Each user authorized to access the District computers, networks, Internet services, or other resources is required to sign an Acceptable Use Policy Acknowledgement Form or the Employee or Student Code of Conduct and Student/Parent Handbook Acknowledgement Form stating that they have read policy CQ Local, CQ Legal and CQ Exhibit (the Acceptable Use Policy).

As a condition of continued employment, employees, consultants, and contractors must annually sign an Acceptable Use Policy Acknowledgement Form or Sonora ISD Employee Handbook. The acknowledgement form will be retained in the employee’s personnel file or in the Technology Department’s files. Acknowledgement forms from students will be maintained in campus records, as will Acknowledgement forms from parents and volunteers.

I hereby acknowledge that I have received information related to the User Agreement for the Acceptable Use 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 Use Policy by accessing the web sites provided or by requesting, in writing, a paper copy from the appropriate department.

Staff Printed Legal Name

Campus

Staff Signature

Date

STUDENT:

As a user of the Sonora ISD computer network, I hereby agree to comply with the above-stated rules. I will use the network responsibly and will honor all relevant restrictions.

Student Printed Legal Name

Campus

Grade

Student Signature

Date

PARENT OR LEGAL GUARDIAN:

As the parent or legal guardian of the minor student signing above, I grant permission for the student named to access networked computer services such as electronic mail and the Internet. I understand some material on the internet may be objectionable, but that Sonora ISD has systems in place to limit access to this information. Ultimately, I must work with my child to stress the importance of appropriate and responsible behavior and that there are disciplinary and legal consequences for misbehavior.

Acceptance to allow publication of student recognition and/or created work(s) on the district website and associated social media:

Your son or daughter may create artwork or writing which would be suitable for publication on the district website/social media sites or any publicly reproduced document. In addition, there are times when we would like to post your child’s photo on the district website/social media sites or any publicly reproduced document related to awards received, sports and/or club activities, which feature your child, and other celebratory occasions. All postings of work or photos will appear in an educational context with appropriate copyright notice prohibiting the copying of such work without express written permission. No home address or telephone number will appear with such work or photos. If you would not like your child’s artwork, writing, or photos to appear on the Sonora ISD website/social media sites, or any publicly reproduced document, please contact your child’s principal.

Parent/Legal Guardian Signature

Date

To review the Acceptable Use Policy visit the Sonora ISD website at www.sonoraisd.net this document is located beneath the Parents tab.