
Note: For information about use of the District's technology resources and electronic communications by Board members, see BBI(LOCAL). For student use of personal electronic devices, see FNCE. For additional provisions governing employee use of electronic media, see DH(LOCAL) and the District's employee handbook. For information about retention and security of records containing criminal history record information and procedures for reporting related security incidents, see DBAA. For information about District, campus, and classroom websites, see CQA. For intellectual property and copyright compliance, see CY. For the District's cybersecurity plan, see CQB.

**Available
Technology
Resources**

The Superintendent and the Technology Director will oversee the District's technology resources, including electronic communications systems and electronic equipment.

The District makes technology resources available to staff, students, parents or guardians, and members of the public as applicable and in accordance with the District's conditions of use. Available technology resources may include onsite internet access, District-owned hardware and software, District-approved online educational applications for use at school and at home, and digital instructional materials.

Internet Safety Plan

The Superintendent will designate the Technology Director to oversee development and implementation of an internet safety plan, including guidelines for the acceptable use of the District's technology resources in compliance with this plan and related Board policies, if any. All users will be provided copies of acceptable-use guidelines and training in proper use of the District's technology resources that emphasizes ethical and safe use.

Training is provided for students and staff regarding the safe, ethical, legal, and responsible use of the Internet and of the District's Internet system and their rights and responsibilities under this plan.

The District protects against access to materials that are considered inappropriate for users to access through the District Internet system in the following manner:

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information

The District's filtering software limits student internet access as defined by CIPA (Children's Internet Protection Act 2001). Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. At the discretion of the District or school, the filtering software may also be configured to protect against access to other material considered inappropriate. The District recognizes that internet filters are not perfect and some sites with questionable material may not be filtered; however, the District will modify the material once it has been identified and reported. San Felipe Del Rio CISD does not rely on internet filters as a sole protection measure and students and teachers are instructed on procedures to handle inappropriate access. Parents and guardians should report any questionable access to their child's campus.

Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

The District's filtering software is configured tiered access, which allows staff members access to more sites than students.

Requests for website unblocking will be approved through the Technology Director. The determination of whether material is appropriate or inappropriate shall be based on the content of the material, intended use of the material, and content of ads, not on the protection actions of the filtering software.

The school district will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

Inappropriate Network Usage

Utilizing the digital citizenship curriculum, San Felipe Del Rio CISD promotes the safety and security for users of the computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Education, Supervision and Monitoring

It shall be the responsibility of all members of the San Felipe Del Rio CISD staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

The student Responsible Use Policy (RUP) includes provisions that address the following safe and responsible use issues:

- Privacy and communication safety standards for self and others
- Safety and security when using direct electronic communication
- Unacceptable conduct including inappropriate language, bullying, access to inappropriate material, plagiarism and copyright infringement, as well as actions that may disrupt or jeopardize the security or effective performance of the District's network or the Internet
- Illegal activities, including computer security violations, actions taken to disrupt the performance of a computer system, and the use of the Internet to engage in other criminal acts

The employee RUP is provided electronically and posted on the District website. Employees are held accountable for its contents. The employee RUP address information similar to the student RUP and other acceptable use issues specific to employees.

The District follows guidelines for protecting student personal information when accounts are established on third party web sites in accordance with CIPA.

The District has developed regulations addressing the disclosure of student information, posting student-created material, and posting pictures of students on the District web site.

Each school year, parents/guardians are provided information regarding agreements to allow their child to access the Internet and have photos of their child or child's schoolwork on the District web site. Parents have the option to decline all or parts of the above agreement based on need.

Filtering

The Superintendent designates the Technology Director to implement and maintain appropriate technology for filtering material considered inappropriate or harmful to minors.

TECHNOLOGY RESOURCES

CQ
(REGULATION)

The Superintendent designates the Technology to determine appropriate use of filtering devices. All internet access will be filtered for minors and adults on the District's network and computers with internet access provided by the school.

The categories of material considered inappropriate and to which access will be blocked will include, but not be limited to, nudity or pornography; images or descriptions of sexual acts; promotion of violence; illegal use of weapons or drugs; discrimination or participation in hate groups; instructions for performing criminal acts (for example, bomb making); and online gambling.

*Requests to
Disable Filter*

The Technology Director will consider requests from users who wish to use a blocked site for bona fide research or other lawful purposes. The committee will make a recommendation to the Superintendent regarding approval or disapproval of disabling the filter for the requested use.

Access

Access to the District's technology resources will be governed as follows:

*General
Guidelines*

1. All students, employees, and Board members will be provided access to, and be required to adhere to, relevant policies and information concerning use of District technology resources and the District's expectations for acceptable use.
2. Officials and employees will be required to complete cybersecurity awareness training as determined by law and local policy. [See CQB]
3. Access to technology resources may be restricted when required by law or policy or, when permitted by law, upon request for students by their parent or guardian. [See CQB, EF]
4. All District technology resource users must complete required training and sign an acceptable-use agreement annually for issuance or renewal of an account and/or device. [See CQ(EXHIBIT) — B, C, and D]
5. All nonschool users, including volunteers and contractors, will be required to sign or accept an acceptable-use agreement before being granted access. [See CQ(EXHIBIT) — E] Access may be limited by the District as appropriate.
6. All passwords for District accounts must meet password complexity requirements, including multi-factor authentication, established by the District. Passwords must be changed every 90 days. All passwords must remain confidential and should not be shared.

TECHNOLOGY RESOURCES

CQ
(REGULATION)

7. Any user identified as a security risk or as having violated District- and/or campus-use guidelines may be denied access to the District's technology resources.
- Board Members and All District Employees*
1. With written approval of the immediate supervisor or the Superintendent, and upon completion of any required District network training, District employees and Board members will be granted access to the District's technology resources, as appropriate. [See BBI]
 2. Use of personal technology and devices to conduct school business must also comply with all District policies and acceptable use guidelines.
 3. Before using any program requiring the user to accept terms of service or a user agreement, or that requires the user to share confidential or individually identifiable information, including use in the classroom, use with students, administrative use, all digital subscriptions, online learning resources, or online or mobile applications, approval must be obtained from the Technology Director. District staff and Board members should not accept terms and conditions or sign user agreements on behalf of the District without approval.
 4. Teachers and other professional staff must submit a request to use additional online technology resources that have not been approved by the District, as described below at Approval of Technology Resources.
 5. Continued use of District technology resources is conditioned on completion of all required training and compliance with all policies and directives regarding use. Failure to complete required training by applicable deadlines will result in immediate suspension of network access and/or device functions and will require reauthorization from a supervisor.
- Instructional Staff*
1. Students may only be assigned to use resources approved by the District. To view the most updated list of approved resources, go to the Students and Families tab on the District's website.
 2. Parental consent must be obtained before a student may take part in District-sponsored technology, social media, online educational programs or mobile applications, or other cloud-based instructional resources, including video sharing for classroom use or use of a student's photo, image, or voice on a District or classroom website, even if public access is blocked.

TECHNOLOGY RESOURCES

CQ
(REGULATION)

3. The staff member assigning students to use technology resources is responsible for ensuring parents or guardians and/or students have signed the District's acceptable use agreement and that students have received any required technology training. [See CQ(EXHIBIT) — B]
 4. Management of student use of technology is the responsibility of the staff member in the same manner as classroom management or student supervision.
 5. Staff may only record or allow recording of a student's image or voice for the limited purpose of instruction, in compliance with law and policy. [See EHA, FL, FM, and FO]
 6. Disclosure of student directory information may be authorized only in accordance with District policy and requisite parent or guardian notice and consent. [See FL]
- Students*
1. All students will be required to complete training regarding appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.
 2. Students in kindergarten-grade 5 may be granted access to the District's technology resources as determined by the campus principal, with parental approval, and in accordance with law and policy.
 3. Elementary students will have access to District-managed online educational applications and will not be issued or asked to create individual accounts using personally identifiable information.
 4. Elementary students in grades PK-5 may have access to the internet or District-issued email or network accounts only as approved by the campus principal and only with parental permission.
 5. With parental approval, students in grades 6-12 will be assigned individual accounts and passwords for use of District-sponsored technology resources, including limited access to the internet, individual email accounts, and District-approved online educational resources.
 6. Students granted access to the District's technology resources must complete any applicable user training, including training on cyberbullying awareness and response, copyright piracy, cybersecurity, and appropriate online behavior and interactions with other individuals on social media networking websites.

TECHNOLOGY RESOURCES

CQ
(REGULATION)

	<ol style="list-style-type: none">7. Parental notice and approval will be required before a student may take part in District-sponsored social media, online instructional programs, or other online or mobile educational applications, including video sharing for classroom use or use of a student's photo on a District or classroom website, even if public access is blocked.8. Upon request from a parent or guardian, the District will provide a list of technology resources for use by the student.
<i>Nonschool Users</i>	<ol style="list-style-type: none">1. Nonschool users may be given limited access to District technology resources when available, including computer and internet access, online job applications, and access to the District's wireless internet, in accordance with guidelines established by the campus or the District.2. Use of District technology resources by members of the public may not interrupt instructional activities or burden the District's network.3. In addition to applicable law, Board policies, and District regulations, nonschool users may also be subject to additional requirements related to use or access to District technology that may be covered by written agreements with the District.
Student Participation in Social Media	San Felipe Del Rio CISD does not allow students to participate in social networking.
Approval of Technology Resources	<p>The District will ensure that all technology resources in use in the District meet state, federal, and industry standards for safety and security of District data, including a student's education records and personally identifiable information. [See FL]</p> <p>Before use in the classroom, use with students, or administrative use, any professional staff wanting to use an online learning resource, online or mobile application, digital subscription service, or other program or technology application requiring the user to accept terms of service or a user agreement, other than a District-approved resource, must first submit an application for approval. [See CQ(EXHIBIT) — F]</p> <p>If approved, additional parental notification or permission may be required before use by students.</p> <p>No student 13 years of age or younger will be asked to download or sign up for any application or online account using his or her</p>

TECHNOLOGY RESOURCES

CQ
(REGULATION)

own information. For elementary students, only applications that allow for one classroom or administrator-run account will be approved.

Reporting Violations

All users must immediately report any known or suspected violation of the District's applicable policies, cybersecurity plan, internet safety plan, or acceptable-use guidelines to a supervising teacher, the technology coordinator, or Superintendent, as appropriate.

Students and employees must report to a supervising teacher or the technology coordinator any requests for personally identifiable information or contact from unknown individuals, as well as any content or communication that is abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

The technology coordinator will promptly inform the Superintendent, law enforcement, or other appropriate agency of any suspected illegal activity relating to misuse of the District's technology resources and will cooperate fully with local, state, or federal officials in any investigation or valid subpoena. [See GR series and CQB]

Loss of Privileges

Inappropriate use of the District's technology resources may result in revocation or suspension of the privilege to use these resources, as well as other disciplinary or legal action, in accordance with applicable laws, District policies, the Student Code of Conduct, and District administrative regulations. [See DH, FN series, and FO series]

*Termination /
Revocation of
Use*

Termination of access for violation of District policies or regulations will be effective on the date that the principal or District technology coordinator receives notice of withdrawal or of revocation of system privileges or on a future date if specified in the notice.

Artificial Intelligence

The District supports the use of technology to enhance teaching, learning, and innovation. The District allows the use of artificial intelligence (AI) with a focus on teaching students to use AI ethically.

Teachers may, but are not required to, allow the use of AI for instructional purposes. For example, AI programs may assist students with summarizing text or reframing lessons.

Each staff member and student must follow usage guidelines. Misuse of AI, such as hacking or altering data, is strictly prohibited.

Expectations for
Use of AI

Expectations relating to AI include:

4. Generative AI is not a substitute for human thinking, creating, or decision-making.

5. AI use must be disclosed to the individual's supervisors.
6. The use of AI may implicate privacy interests and intellectual property rights. All users must adhere to laws and District policies relating to these matters.
7. Work prepared by or with AI must be reviewed for accuracy, appropriateness, and bias.
8. Entering passwords or other confidential, proprietary, or sensitive information into any AI system is prohibited. Under no circumstances will student or employee personally identifiable information be used with AI.
9. AI tools will not be integrated with District software without Superintendent permission.
10. AI will not be used to make employment decisions, including hiring, reviewing, or disciplining staff.
11. Any AI tools specifically prohibited by the District or law shall not be used.

Student Use of AI

Expectations for student use of AI include:

1. Students may only use AI with teacher permission.
2. Using any District information or personally identifiable information of students or staff in an AI tool is prohibited.
3. Students must understand that AI is fallible and accuracy must always be checked. AI is not considered a credible source for research.
4. Students are expected to think critically and use primary sources to fact check AI generated content.
5. Some courses (for example, Advanced Placement, International Baccalaureate, Honors, and dual enrollment college and university classes) may have additional rules and limitations on the use of AI.
6. If AI is used in any way to create a work product, the student must cite that they used AI and describe the extent of use. The use of AI could violate rules against cheating and academic dishonesty if used inappropriately.
7. Student access to certain AI tools may be granted by the Technology Director with the approval and recommendation from the campus principal. Privacy issues and the students' ages will be considered when determining if access will be granted.

[Adjust the lists below based on the duties of the District's coordinators of technology and cybersecurity. See CQB]

**Technology
Coordinator**

The District has designated the following staff person as the technology coordinator:

Name (*print*): Manuel Salinas

Position: Technology Director

Email: manuel.salinas@sfd-r-cisd.org

Phone number: (830)778-4016

Campus Principals and Assistant Principals will assist the Technology Director in implementing the following:

1. Assist in the development and review of responsible-use guidelines, the District's internet safety plan, the District's cybersecurity plan, and the District's security breach prevention and response plan. [See CQB]
2. Be responsible for disseminating, implementing, and enforcing applicable District policies and procedures, the internet safety plan, the acceptable-use guidelines for the District's technology resources, and the District's breach-prevention and response plan.
3. Make training available to all users regarding safe and appropriate use of the District's technology resources, including cyberbullying awareness and response, data security, and cybersecurity measures. The technology coordinator or designee will ensure training is provided to all employees and Board members who are required to receive annual training.
4. Collect and maintain evidence related to incidents involving the District's technology resources, as requested by the administration.
5. Notify the appropriate administrator of incidents requiring District response and disciplinary measures, including incidents of cyberbullying.
6. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed. [See CY]
7. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate

to ensure student safety online and proper use of the District's technology resources.

8. Coordinate with the District's records management officer to develop and implement procedures for retention and security of electronically stored records in compliance with the District's records management program. [See CPC]
9. Coordinate with the District webmaster to maintain District, campus, and classroom websites, consistent with the District's policies. [See BBE, CPC, CQA, and CY]
10. Coordinate with the District's cybersecurity coordinator about any known or suspected cybersecurity violations.
11. Set limits for data storage as needed.

**Issuing Equipment
to Students**

The following rules will apply to all campuses and departments regarding loaning technology devices and equipment to students under provisions of law cited at CQ(LEGAL).

1. Proposed projects to distribute devices and equipment to students must be submitted to the Technology Director for initial approval.
2. In loaning devices and equipment to students, the principal will give preference to educationally disadvantaged students, as defined by the Education Code.
3. Before loaning devices and equipment to a student, the campus technology coordinator and principal must have clearly outlined a process that includes:
 - a. Criteria to determine eligibility of students;
 - b. An application that identifies the responsibility of the student regarding home placement, use, and ownership of the device or equipment;
 - c. Procedures for distributing and initially training students in the setup and care of the device or equipment;
 - d. Provision of technical assistance for students using the device or equipment;
 - e. Criteria to determine continuation of student use of the device or equipment;
 - f. Documented assessment of any impact on student achievement that use of the device or equipment may provide; and

- g. Procedures for retrieval of the device or equipment from a student as necessary.

**Use of Student
Personal Electronic
Devices for
Instructional
Purposes**

If the District does not issue graphing calculators for a course requiring their use, a student may use a calculator application with the same functionality as a graphing calculator on a phone, laptop, tablet, or other computing device in place of a graphing calculator.

Otherwise, the following rules will apply to student use of personal telecommunications or other electronic devices for on-campus instructional purposes:

1. Requests to use personal telecommunications or other electronic devices for on-campus instructional purposes must be submitted to the campus principal for initial approval. [See FNCE]
2. Agreements for acceptable use of the District's technology resources and personal telecommunications or other electronic devices for on-campus instructional purposes must be signed annually by both the student and the parent or guardian. [See CQ(EXHIBIT) — B, Addendum]
3. When using devices for instructional purposes while on campus, students must use the District's wireless internet services and are prohibited from using a personal wireless service. Any attempt to bypass the District's filter will result in loss of privileges and disciplinary action as required by the Student Code of Conduct.
4. When not using devices for instructional purposes while on campus, students must follow the rules and guidelines for noninstructional use as published in the student handbook, policy FNCE, and in compliance with applicable user agreements.
5. District staff should avoid troubleshooting or attempting to repair a student's personal electronic device. The District is not responsible for damages.
6. The District is not responsible for damage to or loss of devices brought from home.

Violation of these rules may result in suspension or revocation of system access and/or suspension or revocation of permission to use personal electronic devices for instructional purposes while on campus, as well as other disciplinary action, in accordance with the Student Code of Conduct.