Note: For information regarding 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 employee handbook. For information regarding District, campus, and classroom websites, see CQA. For information regarding intellectual property and copyright compliance, see CY.

The Superintendent or designee and the technology coordinator will oversee the District's technology resources, meaning electronic communication systems and electronic equipment.

AVAILABLE TECHNOLOGY RESOURCES

The District will make technology resources available to staff, students, parents, and the members of the public, as applicable. Available technology resources 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.

The District will make available a list of technology resources for use by staff, students, parents, and members of the public, with information on access, data privacy, and security.

The District will also make available upon request information regarding outside vendors with which the District contracts for cloud-based (online) technology applications, the nature and type of data provided to the vendors, the intended use of the provided data, and safeguards on use of personally identifiable student and staff information.

ACCEPTING ELECTRONIC SIGNATURES

The District may accept electronically signed documents or digital signatures for any transactions and purposes allowed by law, including contracts for goods and services, student admissions documents, and employment documents.

The District will comply with rules adopted by the Department of Information Resources (DIR), to the extent practicable, to:

- Authenticate a digital signature for a written electronic communication sent to the District;
- Ensure that records are created and maintained in a secure environment;
- Conduct risk assessments for transactions involving digital signatures;

- Implement appropriate nonrepudiation services; and
- Maintain all records as required by law.

Note: For more information, see DIR's "Guidelines for the Management of Electronic Transactions and Signed Records" found at: http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Texas%20Uniform%20Electronic%20Transactions%20Act%20(UETA)%20Guidelines.pdf.

INTERNET SAFETY PLAN

The District will develop and implement an Internet safety plan, including responsible use guidelines for use of the District's technology resources. All users will be provided copies of responsible use guidelines and training in proper use of the District's technology resources. All training in the use of the District's technology resources will emphasize ethical and safe use.

FILTERING

The Superintendent will appoint the technology director to select, implement, and maintain appropriate technology for filtering material considered inappropriate or harmful to minors. 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/pornography; images or descriptions of sexual acts; promotion of violence, illegal use of weapons, drug use, discrimination, or participation in hate groups; instructions for performing criminal acts (e.g., 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 technology director 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 required to sign an acceptable use agreement annually for issuance or renewal of an account. [See CQ(EXHIBIT)]
2. All nonschool users will be required to sign or accept an acceptable use agreement before being granted access.

3. The District will require that all passwords for District accounts be changed every **365 days at a minimum**. All passwords must remain confidential and should not be shared.

4. District-owned devices and personal devices that allow access to District e-mail or potentially sensitive student or employee records must be password protected.

5. 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.

6. Resources are to be used mainly for educational and administrative purposes, but some limited personal use is permitted.

7. Students in pre-kindergarten–grade 5 will be granted access to the District's technology resources as determined by the campus principal.

   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.

   Elementary students in grades pre-kindergarten – grade 5 may have access to District-issued e-mail or network accounts only as approved by the campus principal and only with parent permission.

   With parental approval, students in grades 6–12 will be assigned individual accounts and passwords for use of District-sponsored technology resources, including individual e-mail accounts and District-approved online educational resources.

8. Students granted access to the District's technology resources must complete any applicable user training, including training on cyberbullying awareness and response, and appropriate online behavior and interactions with other individuals on social networking websites.

9. Parental notice and approval will be required before any student may take part in social media, online instructional programs, or other online 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.

DISTRICT EMPLOYEES AND BOARD MEMBERS

10. With written approval of the immediate supervisor or the Superintendent, and upon completion of District network training, District employees and Board members will be granted access to the District's technology resources, as appropriate.

11. Before use in the classroom, use with students, or administrative use, all digital subscriptions, online learning resources, online applications, or any other program requiring the user to accept terms of service or a user agreement must be approved by the technology coordinator.

    District staff and Board members should not accept terms and conditions or sign user agreements on behalf of the District without preapproval.

12. Teachers and other professional staff may request to use additional online technology resources for instructional and administrative use as described below at APPROVAL OF TECHNOLOGY RESOURCES.

MEMBERS OF THE PUBLIC

13. Members of the public may be given access to District technology resources, 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 administrative department.

14. Use of District technology resources by members of the public should not interrupt instructional activities or burden the District's network.

STUDENT PARTICIPATION IN SOCIAL MEDIA

A student may use District technology resources to participate in social media only as approved by the District in accordance with the student's age, grade-level, and approved instructional objectives. This includes text messaging, instant messaging, e-mail, web logs (blogs), electronic forums (chat rooms), video-sharing websites (e.g., YouTube), editorial comments posted on the Internet, and approved social network sites.

STUDENT TRAINING ON SAFETY AND SECURITY

Students participating in social media using the District's technology resources will receive training to:

- Assume that all content shared, including pictures, is public;
- Not share personally identifiable information about themselves or others;
- Not respond to requests for personally identifiable information or respond to any contact from unknown individuals;
- Not sign up for unauthorized programs or applications using the District's technology resources;

- Understand the risks of disclosing personal information on websites and applications using the students' own personal technology resources; and
- Use appropriate online etiquette and behavior when interacting using social media or other forms of online communication or collaboration.

[See REPORTING VIOLATIONS, below.]

APPROVAL OF TECHNOLOGY RESOURCES

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]

Before use in the classroom, use with students, or administrative use, professional staff wanting to use an online learning resource, online 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]

If approved, additional parental notification or permission may be required before use by students.

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

REPORTING VIOLATIONS

Students and employees must immediately report any known violation of the District's applicable policies, Internet safety plan, or responsible use guidelines to a supervising teacher or the technology coordinator.

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 state 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]

SANCTIONS

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 the principal or District technology coordinator receives notice of withdrawal or of revocation of system privileges or on a future date if so specified in the notice.

TECHNOLOGY COORDINATOR

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

Billy Polasek

Technology Director

830-996-3551

The technology coordinator for the District's technology resources (or campus designee) will:

1. Assist in the development and review of responsible use guidelines, the District's Internet safety plan, and the District's breach prevention and response plan.
2. Be responsible for disseminating, implementing, and enforcing applicable District policies and procedures, the Internet safety plan, the responsible use guidelines for the District's technology resources, and the District's breach prevention and response plan.
3. Each campus with the help of the technology director will provide ongoing training to all users regarding safe and appropriate use of the District's technology resources, including cyberbullying awareness and response and data security measures.
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 and establish a retention schedule for messages that are considered local governmental records.
9. Coordinate with the District webmaster to maintain District websites, including removal of messages from District, campus, and classroom websites that are deemed to be inappropriate, consistent with the District's record management program. [See BBE, CPC, and CQA]
10. 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 **designated administrator** for initial approval.
2. In loaning devices and equipment to students, the principal will give preference to educationally disadvantaged students.
3. Before loaning devices and equipment to a student, the campus technology coordinator and principal must have clearly outlined:
   a. A process to determine eligibility of students;
   b. An application process that identifies the responsibility of the student regarding home placement, use, and ownership of the device or equipment;
   c. A process to distribute and initially train students in the setup and care of the device or equipment;
   d. A process to provide ongoing technical assistance for students using the device or equipment;
   e. A process to determine ongoing student use of the device or equipment;
   f. A process to determine any impact on student achievement the use of the device or equipment may provide; and

g. A process for retrieval of the device or equipment from a student, as necessary.

USE OF PERSONAL ELECTRONIC DEVICES FOR INSTRUCTIONAL PURPOSES

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 **designated administrator** 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. [See CQ(EXHIBIT)]
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 and policy FNCE.
5. Students should bring devices from home fully charged and may not charge their devices at school, unless permission is granted.
6. District staff should avoid troubleshooting or attempting to repair a student's personal electronic device. The District is not responsible for damages.
7. 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.