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 District's employee handbook. For information regarding retention and security of records containing criminal history record information, as well as procedures for reporting security incidents regarding such information, see DBAA. For information regarding District, campus, and classroom websites, see CQA. For information regarding intellectual property and copyright compliance, see CY. For information regarding the District's cybersecurity plan, see CQB.

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

Available Technology Resources

The District makes technology resources available to staff, students, parents, 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 Director of Digital Learning to oversee development and implementation of an internet safety plan, including guidelines for the Responsible Use of the District's technology resources in compliance with this plan. 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.

Filtering

The Superintendent will appoint a committee, to be chaired by the Director of Digital Learning, to determine appropriate use of filtering devices. The Superintendent will designate the Chief Technology Officer to 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 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 (e.g., bomb making); online gambling; and any material harmful to a child.

Requests to Disable Filter

The committee 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 relevant policies and information concerning use of District technology resources and the District's expectations for acceptable use.
2. All students, employees, and Board members will be required to complete training regarding safe and appropriate use of the District's technology resources, including cyberbullying awareness and response, data security, and cybersecurity measures. [See CQB]
3. All district technology resource users will be required to sign a Responsible Use Agreement annually for issuance or renewal of an account. [See CQ(EXHIBIT)–B–D]
4. All non-school users, including volunteers and contractors, will be required to sign or accept a Responsible Use Agreement before being granted access. [See CQ(EXHIBIT)-E] Access may be limited by the District as appropriate.
5. All passwords for District accounts must comply with the District Cybersecurity Account Management section 2.2.4.3. All passwords must remain confidential and should not be shared.
6. 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 of the Superintendent, and upon completion of district Cybersecurity training, District employees and Board members will be granted access to the District's technology resources, as appropriate. [See BBI]
2. Use of personal devices to conduct school business must also comply with all District policies and responsible use guidelines.
3. Before use in the classroom, use with students, or administrative use, all digital subscriptions, online learning resources, online or mobile applications, or any other 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, must be approved by District Data Governance Committee. 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.

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.

3. The staff member assigning students to use technology resources is responsible for ensuring parents 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 limited purposes of instruction, in compliance with law and policy. [See EHA, FFE, FL, FM, and FO]

6. Disclosure of student directory information for limited school sponsored purposes may be authorized only in accordance to District policy and requisite parent notice and consent. [See FL]

Students

1. Students in Pre-Kindergarten through 12th Grade will be granted access to the District's technology resources as determined by the campus principal.

2. All ECISD 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.

3. Elementary students in grades 3rd to 12th Grade may have access to District-issued individual email or network accounts only as approved by the campus principal and only with parental permission.

4. With parental approval, students in Pre-Kindergarten through 12th Grade will be assigned individual accounts and passwords for use of District-sponsored technology resources and District-approved online educational resources.

5. 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.

6. 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.

7. Upon request from a parent, the District will provide a list of technology resources for use by the student.

Non-school Users0.

1. Non- school 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.

Student Participation in Social Media

A student may use District technology resources to participate in social media with parental consent and 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, email, web logs (blogs), electronic forums (chat rooms), video-sharing websites (e.g., YouTube), editorial comments posted on the internet, and approved social networking 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, 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]

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

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, ECISD Police Department, the Director of Digital Learning or Superintendent, as appropriate.

Students and employees must report to Ector County ISD Police Department 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 Chief Technology Officer 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 Director of Digital Learning receives notice of withdrawal or of revocation of system privileges or on a future date if specified in the notice.

Technology Coordinator

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

Name *(print)*: Lauren Tavarez

Position: Director of Digital Learning

Email: Lauren.tavarez@ectorcountyisd.org

Phone number: (432)-456-8481

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, 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 responsible use guidelines for the District's technology resources, and the District's breach-prevention and response plan.
3. Provide training 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 provide training to all employees within 30 days of hire and will provide annual training to all employees.
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 record 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 Director of Information Technology for initial approval.
2. 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. Procedures for distributing and initially training students in the setup and care of the device or equipment;
    c. Provisions of technical assistance for students using the device or equipment;
    d. Criteria to determine continuation of student use of the device or equipment;
    e. Documented assessment of any impact on student achievement that use of the device or equipment may provide; and
    f. Procedures for retrieval of the device or equipment from a student as necessary.

Use of Student 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 purpose:0.

1. Agreements for responsible 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)-B, Addendum]

2. 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.

3. Physically, personally owned network devices are not permissible.

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.