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 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.

The Superintendent or Chief Information Officer, will oversee the District's technology resources, meaning electronic communications systems and electronic equipment.

Available Technology Resources

The District will make technology resources available to staff, students, parents, and 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 approved for use by staff, students, and parents that meet the District's access, data privacy, and security standards.

Cybersecurity Plan

The District will develop and implement a plan to increase cybersecurity and lessen the District's vulnerability to unauthorized efforts to access District data. These efforts will include both technological safeguards, such as password complexity requirements and regular data backups, and training for users in recognizing and reporting activity aimed at gaining unauthorized access, such as phishing and spoofing.

Note: For further information on cybersecurity for Texas school districts, see the Texas Education Agency's Cybersecurity Tips and Tools.[1]

Internet Safety Plan

The District will develop and implement an internet safety plan, including guidelines for the responsible 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 intellectual property, copyright, ethical and safe use.

Filtering

The Superintendent or designee will appoint a committee, to be chaired by the Executive Director, Cybersecurity and IT Operations, to determine the appropriate technology for filtering material considered inappropriate or harmful to minors.

The committee will be comprised of teachers, campus and District administrators, members of the Technology Services department, parents and community member.

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, drug use, discrimination, or participation in hate groups; instructions for performing criminal acts (e.g., bomb making); and online gambling.

Requests to Change 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 regarding approval or disapproval of disabling the filter for the re- quested use.

Access

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

1. All students, employees, and Board members will be required to complete annual cybersecurity training and sign an acceptable-use agreement annually for issuance or renewal of an account. [See CQ(EXHIBIT)]
2. All non-school 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 meet password complexity requirements. Passwords must be changed every 180 days. All passwords must remain confidential and should not be shared.

General *Guidelines*

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

5. District-owned devices will be regularly updated with security patches to meet current cybersecurity standards.

6. District data and devices will be protected by encryption technology that meets current cybersecurity standards.

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, be subject to disciplinary action and criminal prosecution.

8. Resources are to be used mainly for educational and administrative purposes, but some limited personal use is permitted in accordance with District policy.

Students

9. Students in kindergarten–grade 5 will be granted access to the District's technology resources as determined by the cam- pus 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 K-grade 5 may have access to District-issued email (restricted to internal communication), District-approved digital educational resources that may be accessible via the internet or network accounts only as approved by the campus principal and only with parental permission.

   With parental approval, students in grades 6–12 will be as signed individual accounts and passwords for use of District-sponsored technology resources, including individual email accounts and District-approved digital educational resources that may be accessible via the internet.

10. Students granted access to the District's technology resources must complete any applicable user training, including training on cyberbullying awareness and response, cybersecurity, and appropriate online behavior and interactions with other individuals on social media networking websites. Students must complete digital citizenship prior to using a district-owned device away from school.

11. Parental notice and approval will be required annually before a student may use a District-provided device away from school, District-sponsored social media, District-approved digital educational resources, or other online educational applications, including video sharing for classroom even if public access is blocked.

District Employees and Board Members

12. Upon signature of the acceptable use agreement District employees and Board members will be granted access to the District’s technology resources, as appropriate.

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

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

14. Teachers and other professional staff may request to use additional digital resources for instructional and administrative use as described below at Approval of Technology Resources.

Non-school Users

15. Upon signature of the acceptable use agreement non-school users, such as contractors, 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 Technology Services department.

16. 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, email, web logs (blogs), electronic forums (chat rooms), video-sharing web- sites (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 aboutthem selves 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' ownpersonal 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]

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 and FLA]

Approval of Technology Resources

Before use in the classroom, use with students, or administrative use, professional staff wanting to use a digital resource, online application, digital subscription service, extension 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 the resource for approval via a technology support ticket (e.g. KACE).

As applicable, 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.

Technology Services will not approve requests for generic accounts.

Reporting Violations

Students, employees, and Board members must immediately report any known violation of the District's applicable policies, cybersecurity plan, internet safety plan, or responsible-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 Associate Superintendent, Technology or designee 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]

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 that 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:

Name *(print)*: Troy Neal

Position: Executive Director, Cybersecurity & IT Operations

Phone Number: 713-251-2249

The technology coordinator for the District's technology resources 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.
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 will provide training to all employees within 90 days of hire and will provide annual training to all employees and Board Members.

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. 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

1. The District allows student the privilege to borrow technology equipment upon the campus receipt of parent permission, completion of Digital Citizenship and payment of the annual Technology Fee (see FN series).

2. In loaning devices and equipment to students, the principal will give preference to students requesting equipment as part of the annual registration\verification processes.

3. Before loaning devices and equipment to a student, principal and campus designee must have clearly outlined:

a. A process to determine eligibility of students;

b. A process to distribute and initially train students in the

c. 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 for retrieval of the device or equipment from a student as necessary.

4. Students are expected to bring the devices to school fully charged.

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 purposes:

1. The District provides the privilege for students to bring their own personal device (e.g. BYOD) for instructional purposes.
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. District staff shall not troubleshoot or attempting to re-pair a student’s personal electronic device.
6. The District is not responsible for damages of personal devices. 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

[1] Texas Education Agency's Cybersecurity Tips and Tools: https://www.texasgateway.org/resource/cybersecurity-tips-and-tools.