

TECHNOLOGY RESOURCES

CQ  
(REGULATION)

---

**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.

---

**Available  
Technology  
Resources**

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

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 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.

**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.

**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

TECHNOLOGY RESOURCES

CQ  
(REGULATION)

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

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.

---

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 accept an acceptable-use agreement before being granted access.
3. The District will require that all passwords for District staff and students in grades 7 – 12 meet password complexity requirements. Passwords must be changed every semester. All passwords must remain confidential and should not be shared.
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. 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.
7. Resources are to be used mainly for educational and administrative purposes, but some limited personal use is permitted in accordance with District policy.

TECHNOLOGY RESOURCES

CQ  
(REGULATION)

- |                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Students</i>                                     | <ul style="list-style-type: none"><li>8. Students 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.</li><li>9. 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.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                |
| <i>District<br/>Employees and<br/>Board Members</i> | <ul style="list-style-type: none"><li>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.</li><li>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.<br/><br/>District staff and Board members should not accept terms and conditions or sign user agreements on behalf of the District without approval.</li><li>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</li></ul> |
| <i>Nonschool Users</i>                              | <ul style="list-style-type: none"><li>13. Nonschool users 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.</li><li>14. Use of District technology resources by members of the public should not interrupt instructional activities or burden the District's network.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
-

TECHNOLOGY RESOURCES

CQ  
(REGULATION)

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 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 and FLA]

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

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** 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 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]

**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:

Position: Chief Technology Officer

Phone number: 214-780-3070

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

TECHNOLOGY RESOURCES

CQ  
(REGULATION)

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 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 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. Set limits for data storage as needed.

TECHNOLOGY RESOURCES

CQ  
(REGULATION)

**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. 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(EX-HIBIT)]
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. 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.
4. District staff should avoid troubleshooting or attempting to repair a student's personal electronic device. The District is not responsible for damages.
5. 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.