

---

**Note:** For information about the 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.

---

The Superintendent and the Chief Technology Officer 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 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 Chief Technology Officer to oversee the development and implementation of an Acceptable Use Plan and/or Responsible Use Plan. All users will be provided copies of acceptable-use guidelines that emphasize ethical and safe use.

### **Filtering**

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

The Superintendent appoints a Filtering and Software Committee, to be chaired by the Chief Technology Officer to determine the appropriate use of filtering devices. All internet access will be filtered for minors and adults on the District's network.

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.

### **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 employees 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 students and parents must sign a responsible-use agreement annually for issuance or renewal of an account and/or device. [See CQ(EXHIBIT) — B, C, and D]
6. All nonschool users, including volunteers and contractors, will be required to accept an acceptable-use agreement before being granted access. [See CQ(EXHIBIT) — E] Access may be limited by the District as appropriate.
7. All passwords for District accounts must meet password complexity requirements, including multi-factor authentication, established by the District.
8. Any user identified as a security risk or as having violated District- and/or campus-use guidelines may be required to

complete remediation training or be denied access to the District's technology resources.

*Board Members and All District Employees*

9. 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]
10. Use of personal technology and devices to conduct school business must also comply with all District policies and acceptable use guidelines.
11. 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 Filtering and Software Committee. District staff and Board members should not accept terms and conditions or sign user agreements on behalf of the District without approval.
12. Teachers and other professional staff must submit a request to use additional online technology resources by the Filtering and Software Committee, as described below at Approval of Technology Resources.
13. Continued use of District technology resources is conditional 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*

14. Parental consent must be obtained during enrollment 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.

15. 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]
16. Management of student use of technology is the responsibility of the staff member in the same manner as classroom management or student supervision.
17. 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]
18. 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*

19. 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, as outlined in TEKS and cyberbullying awareness and response provided yearly by campus counselors.

#### *Nonschool Users*

20. Nonschool users may be given limited access to District technology resources when available, including the District's wireless internet, in accordance with guidelines established by the campus or the District.
21. Use of District technology resources by members of the public may not interrupt instructional activities or burden the District's network.
22. 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**

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 (for example, 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:

- 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 to the Filtering and Software Committee. [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 non-district-provided application or online account using his or her own information.

### **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 Chief Technology Officer, or the Superintendent, as appropriate.

Students and employees must report to a supervising teacher or the Chief Technology Officer 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 principal or District Chief Technology Officer 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:

23. Generative AI is not a substitute for human thinking, creating, or decision-making.
24. AI use must be disclosed to the individual's supervisors.
25. 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.
26. Work prepared by or with AI must be reviewed for accuracy, appropriateness, and bias.
27. 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.
28. AI will not be used to make employment decisions, including hiring, reviewing, or disciplining staff.
29. 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:

30. Students may only use AI with teacher permission.
31. Using any District information or personally identifiable information of students or staff in an AI tool is prohibited.
32. Students must understand that AI is fallible and accuracy must always be checked. AI is not considered a credible source for research.
33. Students are expected to think critically and use primary sources to fact check AI generated content.
34. 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.

- 35. 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.
- 36. Student access to certain AI tools may be granted by the campus Principal. Privacy issues and the students' ages will be considered when determining if access will be granted.

**Chief Technology Officer**

The District has designated the following staff person as the Chief Technology Officer:

Name (*print*): Gregory Royar  
 Position: Chief Technology Officer  
 Email: gregory.royar@argyleisd.com  
 Phone number: 940-464-7241

The Chief Technology Officer for the District's technology resources (or campus designee) will:

- 37. Assist in the development and review of responsible-use guidelines, the District's cybersecurity plan, and the District's cybersecurity response plan. [See CQB]
- 38. Be responsible for disseminating, implementing, and enforcing applicable District policies and procedures, the acceptable-use guidelines for the District's technology resources, and the District's cybersecurity response plan.
- 39. The Chief Technology Officer or designee will ensure training is provided to all employees and Board members who are required to receive annual training.
- 40. Collect and maintain evidence related to incidents involving the District's technology resources, as requested by the administration.

41. Notify the appropriate administrator of incidents requiring District response and disciplinary measures, including incidents of cyberbullying.
42. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed. [See CY]
43. 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.
44. Coordinate with the District's records management officer to develop and implement procedures for the retention and security of electronically stored records in compliance with the District's records management program. [See CPC]
45. 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 the provisions of law cited at CQ(LEGAL).

46. Proposed projects to distribute devices and equipment to students must be submitted to \_\_\_\_\_ (*insert title of designated administrator*) for initial approval.
47. In loaning devices and equipment to students, the principal will give preference to educationally disadvantaged students, as defined by the Education Code.
48. Before loaning devices and equipment to a student, the Chief Technology Officer and campus principal must have clearly outlined a process that includes:
  - a. Criteria to determine eligibility of students;
  - b. Documentation that identifies the responsibility of the student regarding the use 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. Procedures for retrieval of the device or equipment from a student as necessary.

**Use of Student Personal Electronic Devices for Instructional Purposes is not allowed per HB 1481 and Board Policy.**