Note to administrator: As appropriate, the District may replace the term "Chief Technology Officer" used throughout this regulation with the title of the position that oversees the District's internet safety plan, cybersecurity plan, or any other security network.

Note: For information about 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 development and implementation of an internet safety plan, including guidelines for the acceptable use of the District's technology resources in compliance with this plan and related Board policies, if any. 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.

[See CQ(LEGAL), Internet Safety Plan.]

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 committee, to be chaired by the Chief Technology Officer to determine appropriate use of filtering devices. 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 (for example, bomb making); and online gambling.

Requests to Disable Filter

The committee or designee 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 according to the guidelines below.

General Guidelines

The general guidelines shall include:

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 technology resource users 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 nonschool users, including volunteers and contractors, will be required to sign or accept an acceptable-use agreement before being granted access. [See CQ(EXHIBIT) — E] Access may be limited by the District as appropriate.

6. All passwords for District accounts must meet password complexity and any other requirements, including multi-factor authentication, established by the District. All passwords must remain confidential and should not be shared.

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.

Board Members and All District Employees

The guidelines for Board members and all District employees shall include:

8. 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]

9. Use of personal technology and devices to conduct school business must also comply with all District policies and acceptable use guidelines.

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

11. 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.

12. 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

The guidelines for instructional staff shall include:

13. Students may only be assigned to use resources approved by the District. To view the most updated list of approved resources, go to the District's website.

14. 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.

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

The guidelines for students shall include:

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 and cyberbullying awareness and response.

20. Students in kindergarten-grade 5 may be granted access to the District's technology resources as determined by the campus principal, with parental approval, and in accordance with law and policy.

21. 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.

22. Elementary students may have access to the internet or District-issued email or network accounts only as approved by the campus principal and only with parental permission.

23. With parental approval, students in grades 6-12 will be assigned individual accounts and passwords for use of District-sponsored technology resources, including limited access to the internet, individual email accounts, and District-approved online educational resources.

24. 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.

25. 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.

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

Nonschool Users

The guidelines for nonschool shall include:

27. Nonschool 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.

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

29. 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, 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, the Chief Technology Officer, or 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.

Chief Technology Officer

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

Name : Greg 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:

30. 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]
31. Be responsible for disseminating, implementing, and enforcing applicable District policies and procedures, the internet safety plan, the acceptable-use guidelines for the District's technology resources, and the District's breach-prevention and response plan.
32. Make training available 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 Chief Technology Officer or designee will ensure training is provided to all employees and Board members who are required to receive annual training.
33. Collect and maintain evidence related to incidents involving the District's technology resources, as requested by the administration.
34. Notify the appropriate administrator of incidents requiring District response and disciplinary measures, including incidents of cyberbullying.
35. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed. [See CY]
36. 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.
37. 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]

38. Coordinate with the District webmaster to maintain District, campus, and classroom websites, consistent with the District's policies. [See BBE, CPC, CQA, and CY]

39. Coordinate with the District's cybersecurity coordinator about any known or suspected cybersecurity violations.

40. 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).

41. Proposed projects to distribute devices and equipment to students must be submitted to the campus administrator for initial approval.

42. In loaning devices and equipment to students, the principal will give preference to educationally disadvantaged students, as defined by the Education Code.

43. Before loaning devices and equipment to a student, the campus Chief Technology Officer and principal must have clearly outlined a process that includes:

    a. Criteria to determine eligibility of students;

    b. An application that identifies the responsibility of the student regarding home placement, use, and ownership 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. Documented assessment of any impact on student achievement that use of the device or equipment may provide; and

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

Use of Devices for Instructional Purposes

The District will provide access to graphing calculators. If the District approves, a student may bring a personal graphing calculator to school.

The District is not responsible for damage to or loss of personal graphing calculators brought from home.