
Technology Use

Policy 3-500

Purpose

The Governing Board is committed to ensuring that technology is used safely, ethically, and effectively to support learning and District operations.

The use of District technology must also protect students, staff, and District data as required by law.

Scope:

Technology resources are available to enhance learning, support educational goals, improve communication, and facilitate efficient district operations. All staff, students, Board Members or any other authorized user must use technology resources in a safe, responsible, ethical, and lawful manner consistent with the educational mission of the District.

1. Technology Resources

District technology resource includes, but is not limited to, computers, the District's computer network including servers and wireless computer networking technology (wi-fi), the Internet, electronic communications (including email), USB drives, wireless access points (routers), tablet computers, cellular telephones (including smartphones, smart devices, or, personal digital assistants), pagers, or any other wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through district-owned or personally owned equipment or devices.

Supplemental instructional materials may also include relevant technology that further engages interactive learning in the classroom and beyond.

Adopted on: June 17, 2026
Revised on: N/A

Page 1 of 8

2. Authorized Use

District technology shall be used to support educational programs, school activities, professional responsibilities, and District operations. Including, educational, instructional, research, communication and administrative activities that directly support District programs and goals.

All users shall comply with applicable laws, Board policies, regulations, user agreements, and any other District security requirements. Access is a privilege, not a right, and may be suspended or revoked for misuse, or refusal to agree to the applicable technology use agreement.

Electronic communications (including email) using District technology resources shall be conducted in a professional, respectful, and lawful manner. Employees shall maintain appropriate professional boundaries in electronic communications with students and shall comply with all District policies governing employee conduct and interactions with students.

3. Prohibited Uses

Users shall not:

- Access, create, or distribute material that is obscene, discriminatory, harassing, or illegal.
- Use District systems for personal profit, political campaigning, or non-District business.
- Circumvent network security or install unapproved software or hardware.
- Share passwords, impersonate another user, or attempt to access restricted data.
- Upload, post, or transmit personally identifiable student or staff information to unapproved platforms.
- Violate copyright, intellectual property, or licensing agreements. Users shall respect the legal ownership of software, digital content, and media, including restrictions on reproduction, distribution, and installation of copyrighted material.
- Disrupt District operations or network performance.
- Introduce any malicious software.

4. Technology Privacy and Security

Adopted on: June 17, 2026

Revised on: N/A

Page 2 of 8

The District shall maintain technology protection measures and internet safety procedures consistent with applicable federal and state law.

The Superintendent or designee shall implement safeguards designed to protect students from access to material that is obscene, constitutes child pornography, or is harmful to minors and shall promote safe and responsible online behavior.

- Privacy and Monitoring

Electronic communications, files, and records created or stored on District technology are District property. To the extent permitted by law, the District reserves the right to monitor, access, review, inspect, copy, store, disclose, and delete communications, files, data, and usage associated with District technology resources in order to:

- Maintain system integrity;
- Protect student and employee safety;
- Investigate misconduct;
- Protect confidential information;
- Comply with legal obligations; and
- Ensure proper use of District technology or other related resources.

Users should not expect privacy in information created, transmitted, received, or stored using District technology resources except as otherwise provided by law.

- Protection of Confidential Information

All users must protect confidential information and comply with the Family Educational Rights and Privacy Act (FERPA), the Student Online Personal Information Protection Act (SOPIPA), and the California Consumer Privacy Act (CCPA).

- Cybersecurity

All users share responsibility for protecting District technology resources and data.

Users shall comply with cybersecurity requirements established by the District, including requirements related to passwords, account security, authentication procedures, data protection, and reporting of suspected security incidents.

5. Digital Citizenship and Education

Adopted on: June 17, 2026

Revised on: N/A

Page 3 of 8

The District shall promote responsible digital citizenship and appropriate use of technology resources. Student shall receive age-appropriate instruction regarding online safety, cybersecurity awareness, protection of personal information, prevention of cyberbullying, and responsible use of digital resources.

Staff shall model positive digital behavior and guide students in understanding online ethics and safety.

6. Personal Devices

Only those personal devices authorized by the District for use on District property are permitted. The District assumes no responsibility for loss, theft, damage, maintenance, or security of personally owned devices except as required by law.

7. Emerging Technologies

“Emerging Technologies” include new or evolving digital tools—such as Artificial Intelligence (AI), virtual or augmented reality (VR/AR), Internet-of-Things (IoT) devices, robotics, data analytics, and future technologies not yet defined—that have potential educational or administrative applications.

Oversight and Approval

- All Emerging Technology must be reviewed and approved by the Superintendent or designee before use.
- Approval shall include evaluation of educational value, accessibility, data-privacy compliance, and potential bias.

Ethical Use and Human Oversight

- Emerging Technologies must support, not replace, professional judgment or instructional decision-making.
- Any system using personal data must include clear notice, opt-out rights, and human review for decisions affecting students or staff.
- The District shall monitor state and federal guidance on Artificial Intelligence and related tools and revise this policy as laws evolve.

Administrative Regulations

District technology resources include District-owned or District-authorized computers, networks, servers, internet access, email systems, cloud-based services, software applications, mobile devices, telecommunications systems, digital instructional resources, and other electronic resources.

The District shall review technology practices periodically and update procedures as necessary to address evolving technologies, cybersecurity risks, educational needs, and legal requirements.

1. User Agreements

All authorized users shall sign or electronically acknowledge the applicable District Technology Use Agreement, which includes:

- Students;
- Employees/Staff;
- Governing Board Members;
- Contractors and Consultants;
- Volunteers; and
- Other individuals as authorized by the District.

For students under 18, a parent or guardian must also sign. Internet access may be restricted until acknowledgment is received.

2. Network Access and Security

- The Technology Department shall maintain security measures and content filtering required under the **Children's Internet Protection Act (CIPA)**.
- Users shall immediately report suspected breaches, data loss, or misuse to a site administrator or the Technology Department.

3. Device Management

- District-issued devices are to be used for educational and work purposes only.
- Users are responsible for reasonable care and must return devices upon request. Intentional damage or neglect may result in financial liability or disciplinary action.

4. Student Use of Technology

Adopted on: June 17, 2026

Revised on: N/A

Page 5 of 8

Students shall use District technology resources only for educational purposes and authorized school activities.

Students shall:

- Follow teacher and staff directions;
- Use only authorized accounts;
- Respect intellectual property rights;
- Protect personal information;
- Immediately report inappropriate content or security concerns.

The District may restrict or revoke student technology access when misuse occurs.

5. Student Data Privacy

The District shall implement reasonable administrative, technical, and physical safeguards to protect student information.

Employees shall:

- Access student records only for legitimate educational purposes;
- Protect personally identifiable information; and
- Report suspected data breaches immediately.

Technology vendors shall be required to comply with applicable student privacy laws and contractual requirements

6. Personal Technology Devices

The Superintendent or designee may authorize students and employees to use personally owned devices on District property or District networks.

Users of personal devices shall:

- Comply with District security requirements;
- Use approved network access methods;
- Permit installation of required security configurations when authorized by law; and
- Refrain from using personal devices in a manner that disrupts educational activities.

7. Records Retention

Adopted on: June 17, 2026

Revised on: N/A

Page 6 of 8

Electronic communications and digital records may constitute public records or education records and shall be retained, disclosed, or destroyed in accordance with applicable law and District record-retention requirements.

8. Violations

Violations of this regulation may result in:

- Suspension or revocation of technology privileges;
- Student discipline;
- Employee discipline;
- Restitution;
- Referral to law enforcement; and
- Other remedies authorized by law.

Acknowledgment of Acceptable Use Agreement

I have read and understand the District's **Acceptable Use of Technology Policy 3-500**. I understand that access to District technology resources is a privilege that may be revoked if I fail to comply with District rules. Misuse of technology resources may result in disciplinary or legal action.

Student Name (Print) _____

Student Signature _____ **Date** _____

Parent/Guardian Name (Print) _____

Parent/Guardian Signature _____ **Date** _____

(For employees and other users, signature indicates acknowledgment of professional obligations under this policy.)

Adopted on: June 17, 2026
Revised on: N/A

Page 8 of 8

The policies are developed in collaboration with the Small School Districts' Association for general informational, educational and procedural purposes only and are not intended to constitute legal advice for any specific situation.