For purposes of this policy, "technology" and "technology resources" mean electronic communication systems and electronic equipment.

Sec. 1. Applicability

This policy shall govern all students, employees (part-time or full- time), contractors, consultants, temporary employees, vendors, and other individuals affiliated with third parties who access any District-owned information, property, or device.

In addition, this policy shall govern all information systems for which the District has administrative responsibility including all in-formation created, processed, or used in support of the District's business, without respect to form or format.

The term "user" shall refer to all categories of individuals who access any District-owned information, property, or device including, but not limited to, a student, an employee (part-time and full-time), a contractor, a consultant, a temporary employee, a vendor, and any individual affiliated with a third party.

Sec. 2. Security Framework

District information technology (IT) resources, such as, but not limited to computers, networks, network connectivity, information, storage, email accounts, and the like shall only be provided for approved academic and business purposes by the office of the Chief Technology Information Officer (CTIO), IT, and Information Security. The District shall implement the necessary controls over access to data via a combination of adequate physical, system, remote access and application-based security mechanisms.

In an effort to protect the sensitive information under District care, authorized access to District IT resources shall be limited to the access permissions required for an individual to perform assigned duties or academic activities. Access permissions beyond those needed for those duties or activities shall not be granted.

Passwords shall never be shared with anyone, including District IT security administrators.

Users of District IT resources do not have an expectation of privacy. The District shall reserve the right to monitor and/or record any and all use of District IT resources to ensure compliance with prevailing laws, policies, and regulations to identify misuse as well as for general resource management purposes. [See Children's Internet Protection Act (CIPA), Family Education Rights and Privacy Act (FERPA)]. Use of District IT resources constitutes acceptance of this policy. *47 U.S.C. 254(h)(5); 47 C.F.R. 54.520*

As an additional protection measure, District information, including personally identifiable information, shall not be released except through approved processes and in accordance with governing laws.

Adopted by the board on 10/28/2025

Violations for misuse of District IT resources may result in the imposition of administrative, civil, or criminal penalties.

Sec. 3. Technology Resources

The Department of Information and Technology Systems, in coordination with various user departments, shall be responsible for analysis, development, maintenance, and operation of technology resources for both instructional and administrative purposes. These resources shall provide and facilitate instruction to students, as well as gather, process, and report information relating to all administrative functions within the District.

The District shall maintain and support the goals outlined in the Long-Range Plan for Technology. Any purchase of technology shall support the goals of the District as outlined in the Long-Range Plan for Technology.

Sec. 4. Availability of Access

Access to the District's wide-area networks (WANs), local area networks (LANs), and technology resources, including the internet, shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with guidelines set forth in the *Technology and Information Systems Policies and Procedures Manual.*

a) *Limited Personal Use*

Limited personal use of the District's technology resources shall be permitted if the use:

1. Imposes no tangible cost on the District;
2. Does not unduly burden the District's technology resources; and
3. Has no adverse effect on an employee's job performance or on a student's academic performance.

b) *Use by Members of the Public*

Access to the District's technology resources, including the internet, shall be made available to members of the public, in accordance with administrative regulations. Such use shall be permitted so long as the use:

1. Imposes no tangible cost on the District; and
2. Does not unduly burden the District's technology resources.

Sec. 5. Acceptable Use

The Superintendent shall develop and implement administrative regulations, guidelines, and user agreements consistent with the purposes and mission of the District and with law and policy.

Access to the District's technology resources is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the District's technology resources and shall agree to comply with such regulations and guidelines. Noncompliance with applicable regulations may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. Violations of law may result in criminal prosecution as well as disciplinary action by the District.

Sec. 6. Internet Safety

The Superintendent shall develop and implement an internet safety plan to:

1. Control students' access to inappropriate materials, as well as to materials that are harmful to minors;
2. Ensure student safety and security when using electronic communications;
3. Prevent unauthorized access, including hacking and other unlawful activities;
4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students; and
5. Educate students about cyberbullying awareness and response and about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms.

a) ***Filtering***

Access to the internet via the District's network systems shall be filtered to block access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal CIPA and as determined by the Superintendent.

The Superintendent shall enforce the use of such filtering controls. Upon approval from the Superintendent, an administrator, supervisor, or other authorized person may disable the filtering controls for bona fide research or other lawful purpose for adults.

Sec. 7. Monitored Use

Electronic mail transmissions, social media, and other use of the District's technology resources by students, employees, and members of the public shall not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use.

Sec. 8. Disclaimer of Liability

The District shall not be liable for users' inappropriate use of the District's technology resources, violations of copyright restrictions or other laws, users' mistakes or negligence, or costs incurred by users. The District shall not be responsible for ensuring the availability of the District's technology resources or the accuracy or usability of any information found on the internet.

Sec. 9. Record Retention

A District employee shall retain electronic records, whether created or maintained using the District's technology resources or using personal technology resources, in accordance with the District's records management program.

Sec. 10. Electronically Signed Documents

At the District's discretion, the District may make certain transactions available online, including student admissions documents, student grade and performance information, contracts for goods and services, and employment documents.

To the extent the District offers transactions electronically, the District may accept electronic signatures in accordance with this policy.

When accepting electronically signed documents or digital signatures, the District shall comply with rules adopted by the Department of Information Resources, to the extent practicable, to:

- Authenticate a digital signature for a written electronic communication sent to the District;
- Maintain all records as required by law;
- Ensure that records are created and maintained in a secure environment;
- Maintain appropriate internal controls on the use of electronic signatures;
- Implement means of confirming transactions; and
- Train staff on related procedures as necessary.

Gov't Code 2054.060.

Sec. 11. Procurement of Software

The District has an ongoing need for the implementation of major applications to meet business and student data management and reporting requirements. The District shall pursue the acquisition of commercially packaged software to meet these business needs in lieu of developing systems in-house unless the following criteria cannot be met. For a software package to be considered, it should meet 80 percent of the user requirements and be able to be implemented within project cost and time constraints. In addition, any packaged software acquired should not be customized by the District.

Sec. 12. Allocations

Technology resources shall be allocated to meet the requirements of state mandates in accordance with the needs of schools as defined in the school improvement plans and as reflected in the goals of the Long-Range Plan for Technology. All acquisitions of technology resources, both hardware and software, must be reviewed and coordinated by the Department of Information and Technology Systems in accordance with the *Technology and Information Systems Policies and Procedures Manual* and shall meet the requirements described in the *Finance Procedures Manual.*

Adopted by the board on 10/28/2025