
Purpose

The Board recognizes that vendors and contractors may require access to district technology resources to perform contracted services. The Board adopts this policy to establish requirements for vendor access that protect district technology resources and data, including student data.

Definitions

District Technology Resources – District computer systems, devices, networks, applications, cloud services, and related technology.

District Data – Data or information created, collected, stored, or maintained by or for the district.

Student Data – Information that identifies or is linkable to a student, including education records protected by FERPA.

Authority

Vendor access to district technology resources is a privilege, not a right. Vendors shall sign a Vendor Network Access and Security Agreement before being granted access to district technology resources. Access is conditioned on compliance with this policy, applicable contracts, district procedures, and applicable law.

Vendors with access to district technology resources shall:

1. Access only systems and data necessary for the contracted service.
2. Comply with applicable background check and clearance requirements.
3. Protect district data and student data from unauthorized access, use, or disclosure.
4. Comply with FERPA, COPPA, and applicable student data and privacy requirements.
5. Not use district data or student data for any unauthorized purpose.
6. Report security incidents promptly in accordance with district procedures and applicable law.

The Board prohibits vendors from using district technology resources for any unauthorized purpose or engaging in any activity that compromises district security.

Failure to comply with this policy may result in termination of access, contractual remedies, and referral to appropriate authorities.

Delegation of Responsibility

The Superintendent or designee shall develop procedures to implement this policy.