

Data Access Roles and Permissions

1. Purpose

This document establishes the District's standards for assigning, approving, reviewing, modifying, and removing access to data, systems, applications, cloud services, and educational platforms based on role, school purpose, least privilege, and legal requirements specific to public K-12 education.

The purpose of these controls is to ensure students, employees, contractors, vendors, volunteers, and automated systems receive only the minimum access necessary to perform their approved educational or business function while protecting student privacy, personnel confidentiality, financial integrity, and District security operations.

2. Scope

These requirements apply to all access permissions involving:

- Student Information Systems (SIS)
- Learning Management Systems (LMS)
- Assessment and state testing platforms
- HR, payroll, finance, and procurement systems
- IEP, special education, nursing, counseling, and student support systems
- Classroom instructional software and digital curriculum
- Security cameras and door access systems
- Network, server, backup, and cloud administration platforms
- Google Workspace, Microsoft 365, and SSO platforms
- Clever, OneRoster, and rostering integrations
- Data dashboards, reporting, and analytics systems
- File shares, records repositories, and board/legal records

These standards apply to permanent, temporary, emergency, delegated, vendor, substitute, and service-account access.

3. Role-Based Access Standards

Technical security mechanisms shall be in place to protect all District data transmitted electronically. The following controls shall be implemented where applicable:

A. Student Access

Student access shall be limited to age-appropriate systems and only the records, coursework, rosters, and digital resources assigned to that student.

Examples:

- Student class schedules

- LMS coursework and grades
- State testing sessions assigned to the student
- District-approved instructional applications
- Student-owned portfolio content

Students shall never be granted administrative, staff, HR, discipline, health, or financial access.

B. Teacher and Instructional Staff Access

Teachers and instructional staff shall have access only to students and classes currently assigned to them through SIS and rostering integrations.

This may include:

- Current class rosters
- Grades and assignments
- Attendance entry
- Instructional intervention data
- Benchmark and classroom assessment results
- Parent communication systems

Access to former students, unrelated grade levels, or districtwide student data is prohibited unless specifically approved.

C. School Administrator Access

Principals, assistant principals, counselors, and designated school leaders may receive broader school-level access based on job duties.

Examples include:

- Schoolwide discipline data
- Attendance trends
- School testing coordination
- Teacher evaluation systems
- School camera access limited to assigned campus
- Student support and intervention systems

D. District Department Access

District leaders shall receive role-based access aligned to their department.

Examples:

- HR: personnel and onboarding systems
- Finance: payroll, purchasing, and budget systems
- Instructional Services: curriculum and assessment analytics
- Technology: infrastructure, SSO, device, backup, and security systems
- Safety: districtwide camera and access control platforms

E. Vendor and Third-Party Access

Vendors, consultants, auditors, and service providers may only receive access when:

- A DPA or contract is fully executed
- Scope is limited to the approved service

- Access duration is time-bound
- MFA and logging are enforced where supported
- Access is removed immediately at contract completion

F. Service Accounts and Integrations

Automated accounts used for Clever, OneRoster, SIS sync, APIs, backups, and other integrations shall use the minimum required permissions.

These accounts must:

- Use unique credentials or certificates
- Be documented with an owner
- Have token/key rotation requirements
- Be reviewed periodically
- Never be used for interactive user access

G. Sensitive Data Segmentation

Where full data values are not required for transfer, data masking, tokenization, truncation, or field suppression shall be used to reduce exposure.

Examples include:

- Partial student identifiers
- Truncated employee IDs
- Hidden financial account values
- Suppression of unnecessary directory attributes
- Limited field exports for vendor integrations

4. Access Approval, Review, and Removal

All access must be approved by the appropriate data owner, supervisor, principal, department director, or Superintendent designee.

The District shall maintain procedures for:

- New hire and student provisioning
- Enrollment-based student access creation
- Teacher schedule changes
- Mid-year transfers and school changes
- Substitute and temporary staff access
- Role changes and promotions
- Immediate termination and offboarding
- Annual entitlement reviews
- Emergency elevated access approvals

Special emphasis shall be placed on rapid access changes during:

- Student withdrawals
- Employee separation
- Long-term substitute assignments
- Discipline or legal holds

- Vendor contract termination
-

5. Logging and Monitoring

All critical data transfers, integrations, and automated synchronization workflows shall be logged where technically feasible.

Logging should include:

- Source and destination
- Date and time
- Authenticated account or service identity
- Records transferred
- Exceptions or failures
- Unauthorized attempts
- Token or certificate issues

Critical failures or repeated unauthorized attempts shall be escalated to the District Technology Department.

6. Prohibited Practices

The following are prohibited:

- Sending protected data through unsecured channels
 - Use of personal email for District data transfer
 - Unencrypted FTP or public file sharing links
 - Excessive data sharing beyond minimum need
 - Long-lived unmanaged API tokens
 - Vendor access without DPA and approved scope
 - Exposing SIS or rostering data without approved standards
-