

# Data Classification Levels

## 1. Purpose

This document establishes the District's data classification framework to ensure appropriate safeguards are applied based on the sensitivity, confidentiality, integrity, legal requirements, and operational importance of District data.

Data classification is used to promote proper administrative, physical, and technical controls for protecting the confidentiality of data. Regardless of classification level, the integrity, accuracy, availability, and authenticity of all District data shall be protected.

The classification assigned and the controls applied shall be based on the most sensitive data element contained within the record, system, communication, or dataset.

Data maintained in multiple formats shall retain the same classification regardless of medium, including but not limited to paper, email, database records, reports, screenshots, exports, backups, audio/video recordings, and cloud-hosted content.

---

## 2. Classification Standard

All District data shall be classified into one of the following levels:

- **Level 1 – Public**
- **Level 2 – Internal Use**
- **Level 3 – Confidential**
- **Level 4 – Restricted / Highly Sensitive**

When uncertainty exists, the data owner or Superintendent designee shall assign the **higher classification level** until formal review is completed.

---

## 3. Level 1 — Public

Public data includes information approved for release to the general public where disclosure creates little or no risk to District operations.

### Examples

- Public website content
- Board-approved policies
- Published school calendars
- Public job postings
- Approved press releases
- Public athletic schedules
- School lunch menus
- General district contact information

### Minimum Controls

- Accuracy verification before release
  - Change control for official publications
  - Website access protections against unauthorized alteration
  - Public records retention compliance
- 

## 4. Level 2 — Internal Use

Internal Use data includes operational information intended for authorized District personnel, but not for unrestricted public release.

### Examples

- Internal procedures and work instructions
- Network diagrams without sensitive configurations
- Routine staff communications
- Technology inventory workflows
- Internal reports and draft planning documents
- Work order and ticketing data
- Internal committee notes

### Minimum Controls

- Access limited to authorized users
  - SSO and account-based authentication
  - Share only with legitimate educational or business purpose
  - Storage in approved District systems
  - Retention according to records schedules
- 

## 5. Level 3 — Confidential

Confidential data includes protected information that could cause legal, privacy, operational, financial, or reputational harm if disclosed without authorization.

### Examples

- Student education records protected by FERPA
- Employee personnel files
- Payroll and compensation data
- Purchase and bid information before award
- School safety and emergency response procedures
- Security camera exports and incident footage
- Internal vulnerability assessments
- Vendor contracts and DPAs
- Discipline records
- Student schedules and rosters

### Required Controls

- Least-privilege access
- Role-based permissions

- MFA where supported
  - Encryption in transit and at rest where feasible
  - Approved sharing workflows only
  - Logging and auditability
  - Controlled export and printing
  - Secure disposal requirements
  - DPA/vendor protections when shared externally
- 

## 6. Level 4 — Restricted / Highly Sensitive

Restricted data includes the most sensitive information requiring the highest degree of protection due to legal mandates, safety implications, or severe operational impact.

### Examples

- Social Security numbers
- Driver's license numbers
- Banking and ACH details
- Health, counseling, nursing, and protected student support records
- Authentication credentials, password hashes, MFA seeds, and recovery codes
- Security system configurations and access control credentials
- Encryption keys and backup credentials
- Active cybersecurity incident evidence
- Law enforcement or juvenile justice protected records
- Data protected by court order or attorney-client privilege

### Required Controls

- Strict need-to-know access only
  - Explicit data owner approval
  - MFA required where technically feasible
  - Encryption required in transit and at rest
  - Prohibited local storage unless specifically approved
  - Restricted external sharing
  - Immediate revocation upon role change
  - Detailed audit logging
  - Enhanced retention and destruction procedures
  - Incident escalation for any suspected exposure
- 

## 7. Data Handling Rules

All users shall handle data according to its assigned classification.

This includes controls for:

- Access and permissions
- Email and communication sharing
- Cloud storage and SaaS platforms

- Printing and scanning
- Backup and archival storage
- Data exports and screenshots
- Third-party sharing
- Public records requests
- Secure destruction

Where multiple classifications exist in the same file, communication, or report, the highest classification level governs the entire asset.

---

## 8. Roles and Responsibilities

### **Data Owners**

- Determine initial classification
- Review classification during process changes
- Approve access based on business need

### **Director of Technology / Superintendent Designee**

- Maintains technical controls supporting each level
- Ensures systems support classification requirements
- Reviews exceptions and unresolved conflicts

### **Employees and Authorized Users**

- Protect data according to assigned level
  - Use only approved systems for storage and sharing
  - Report suspected misclassification or exposure
- 

## 9. Review and Reclassification

Data classifications shall be reviewed when:

- New systems are implemented
- Data elements change
- Legal requirements change
- Data is repurposed for a new use
- Public release is requested
- New integrations or vendors are introduced

Reclassification shall be documented where the risk profile materially changes.

---