

Definitions and Responsibilities

1. Authority and Administration

The Superintendent and/or his or her designee is authorized to establish, implement, maintain, and enforce District data and information security measures, standards, processes, and procedures necessary to protect District operations and ensure compliance with applicable law, Board policy, and administrative procedures.

These requirements apply to all:

- Students
- Employees
- Board members
- Contractual third parties
- Vendors and service providers
- Agents of the District
- Volunteers
- Any other approved user with access to District systems, services, or data

For purposes of this policy and all supporting documents, the terms **data** and **information** may be used separately, together, or interchangeably. The intent and meaning remain the same and refer to any record, communication, file, system content, metadata, or other information asset created, received, stored, transmitted, processed, or maintained by the District.

2. Annual Review and Governance Oversight

Dothan City Schools shall maintain documented data governance policies, standards, procedures, and administrative controls that are reviewed **at least annually**.

The **Data Governance Committee** shall:

- Review all governance policies and supporting documents annually
- Recommend revisions based on legal, regulatory, operational, or cybersecurity changes
- Review incidents, audit findings, and risk assessments for policy implications
- Ensure alignment with FERPA, COPPA, CIPA, state records requirements, and Board policy
- Maintain documentation of annual reviews and adopted revisions

The Superintendent or designee may direct interim updates whenever significant legal, technical, or operational changes occur.

3. Training Requirements

Dothan City Schools shall conduct **annual data governance and information security training** for all employees and other authorized users as appropriate to their role.

Training shall include, at minimum:

- Data privacy and confidentiality requirements
- FERPA and student records protections
- Password, MFA, and account security practices
- Phishing, social engineering, and cyber awareness
- Acceptable use and prohibited activities
- Approved software and Shadow IT restrictions
- Data handling, sharing, and retention requirements
- Incident reporting procedures
- Records management and secure destruction

The District shall maintain documentation demonstrating completion of required training, including attendance records, digital acknowledgements, or platform-generated completion reports.

Role-specific supplemental training may be required for administrators, finance, HR, student services, technology staff, school administrators, and any employee with elevated access to protected information.

4. Scope of Data and Information Covered

This policy applies to **all forms of Dothan City Schools data and information**, regardless of format, transmission method, storage location, or technology platform, including but not limited to:

1. **Verbal communications** — speech communicated face-to-face, by telephone, radio, conferencing systems, voicemail, or future communication technologies
2. **Hard copy records** — printed, handwritten, copied, scanned, or faxed materials
3. **Physical communications** — mail, courier, records transfer, and document delivery services
4. **Electronic communications** — email, text messaging, chat platforms, ticketing systems, collaboration tools, and social media
5. **Endpoint and processing systems** — servers, virtual systems, desktops, laptops, Chromebooks, tablets, classroom displays, mobile devices, telephony systems, and future endpoint technologies
6. **Storage media and hosted systems** — internal drives, external drives, removable media, backup repositories, cloud services, SaaS platforms, and any hosted data environments

This includes structured and unstructured data in active use, archived storage, backups, exports, logs, metadata, screenshots, audio/video recordings, surveillance records, and derived reports.

5. Responsibilities

Superintendent

- Provides executive authority for District data governance
- Directs policy implementation and enforcement
- Assigns designees and committees as needed

Superintendent Designee / Director of Technology

- Maintains governance standards and procedures
- Oversees technical and administrative safeguards
- Coordinates annual reviews and required updates
- Maintains training documentation and evidence of compliance

Data Governance Committee

- Reviews policies annually
- Recommends updates and supporting administrative procedures
- Ensures alignment with risk, privacy, security, and operational practices

Employees and Authorized Users

- Complete required annual training
- Follow all data governance procedures
- Protect confidential and protected information
- Report suspected misuse, unauthorized disclosure, or policy violations immediately