

Dothan City Schools Data Governance Policy

Overview

The policy defines how Dothan City Schools (DCS) ensures its data remains accurate, accessible, consistent, and secure during operations and instruction. The document establishes who is responsible for information under various circumstances and specifies the procedures to be used to manage and protect it.

The Superintendent is authorized to establish procedures governing the storage, use, and sharing of data maintained electronically by the school system. Such procedures shall comply with applicable state and federal law and shall include provisions for data security (including physical security measures), access controls, quality control, and data exchange and reporting (including external data requests, and third-party data use). Nothing in this policy or in any procedures authorized hereunder creates or expands any entitlement to confidentiality of records beyond that which is established by law or specific Board policy.

Any unauthorized access, use, transfer, or distribution of Board data by any employee, student, or any other individual may result in disciplinary action (up to and including termination for employees) and other legal action.

Supplemental documents referenced in this policy are administrative implementation documents maintained by the Superintendent or designee and may be revised as needed to address operational, legal, security, or regulatory changes without separate Board approval, provided such revisions do not materially alter the intent of this policy.

POLICY

Protecting the privacy of students' and staff data is an important priority, and Dothan City Schools (DCS) is committed to maintaining strong and meaningful privacy and security protections. The privacy and security of this information are a significant responsibility, and school officials value the trust of students, staff, parents, legal guardians, and the community. For this document "data" and "information" may be used interchangeably and refer to PII, confidential, sensitive and/or other internal information that would require protection against unauthorized access, disclosure, alteration, or destruction to ensure the privacy, integrity, and security of student, staff, and district records in compliance with applicable laws, regulations, and district policies.

It is the policy of Dothan City Schools that data or information in all its forms (written, spoken, electronic, or printed) is protected from accidental or intentional unauthorized modification, destruction, or disclosure throughout its life cycle. This protection includes physical security measures, access controls, quality control, data exchange and reporting, and compliance with all applicable federal, state, and local laws.

The Data Governance Committee and the Technology Director are responsible for reviewing the relevant documents referenced as needed.

Scope

The superintendent and/or his/her designee is authorized to establish, implement, and maintain data and information security measures and procedures. The policy, standards, processes, and procedures apply to all students and employees of the district, contractual third parties and agents of the district, and volunteers who have access to district data systems or data. The terms data and information are used separately, together, and interchangeably throughout the policy. The intent is the same. Dothan City Schools conducts annual training on their data governance policy and documents that training. The data governance policies and procedures are documented and reviewed annually by the data governance committee.

This policy applies to all forms of Dothan City Schools' data and information, including but not limited to:

1. Speech, spoken face to face, or communicated by phone or any current and future technologies
2. hard copy data printed or written
3. communications sent by post/courier, fax
4. electronic mail, text, chat and or any form of social media, etc.
5. data stored and/or processed by servers, PC's, laptops, tablets, mobile devices, etc.
6. data stored on any type of internal, external, or removable media or cloud-based services

Adopted on June 29, 2026

*See Document A. Definitions and Responsibilities

Regulatory Compliance

The Dothan City Schools District will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems. Dothan City Schools complies with all applicable regulatory acts including but not limited to the following:

1. Children's Internet Protection Act (CIPA)
2. Children's Online Privacy Protection Act (COPPA)
3. Family Educational Rights and Privacy Act (FERPA)
4. Health Insurance Portability and Accountability Act (HIPAA)
5. Payment Card Industry Data Security Standard (PCI DSS)
6. Protection of Pupil Rights Amendment (PPRA)
7. Alabama House Bill 166 (FOCUS Act)
8. The Alabama Data Breach Notification Act of 2018

*See Document B. Laws, Statutory, Regulatory, and Contractual Security

Risk Management

A thorough risk analysis of all data networks, systems, policies, and procedures shall be conducted on as need or as requested by the Superintendent. The risk assessment shall be used as a basis for a plan to mitigate identified threats – internal or external, natural or man-made, electronic and non-electronic, and risk to an acceptable level. The Superintendent or designee shall administer periodic risk assessments to identify, quantify, and prioritize risks. Based on the periodic assessment, measures shall be implemented that mitigate the threats by reducing the amount and scope of the vulnerabilities.

*See Document C. Risk Management Practices

Data Classification

Classification is used to promote proper controls for safeguarding the confidentiality of data. Regardless of classification, the integrity and accuracy of all classifications of data are protected. The classification assigned and the related controls applied are dependent on the sensitivity of the data. Data are classified according to the most sensitive detail they include. Data recorded in several formats (e.g., source document, electronic record, report) have the same classification regardless of format.

*See Document D. Data Classification Levels

Systems, Software, Access, and Information Control Systems

Any computer, cloud services, laptop, Chromebook, iPad, mobile device, printing and/or scanning device, network appliance/equipment, security cameras, and other security equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device may be referred to as systems. All involved systems and data are assets of DCS and therefore shall be protected from misuse, unauthorized access, or manipulation, and destruction. These protection measures may be physical and/or software based.

*See Document E. Physical and Security Controls

Software

All computer software developed by or used by DCS employees, students or contract personnel on behalf of DCS, licensed or purchased for DCS use shall not be copied for use at home or at any other location, unless otherwise specified by the license agreement and approved by the DCS Data Governance Committee.

All software packages installed on, accessed by, or utilized on DCS technological systems must adhere to relevant licensing agreements and restrictions and comply with DCS's established software acquisition and application (app) vetting procedures.

**See Document F. Software Acquisition Procedures*

Artificial Intelligence (AI) Use Guidelines regarding Data Privacy

Guidelines are established to outline the responsible use, management, and oversight of Artificial Intelligence (AI) within DCS to ensure data privacy, security, ethical use, and compliance with applicable regulations. These guidelines apply to all AI systems, applications, and tools used within DCS, including but not limited to AI-driven analytics, automated decision-making tools, and AI-enhanced educational technologies.

**See Document G. Artificial Intelligence (AI) Use Guidelines Regarding Data Privacy*

Virus, Malware, Spyware, Phishing, Ransomware, and Spam Protection

Virus checking systems approved by the DCS' District Technology Department are deployed using a multi-layered approach (computers, servers, gateways, firewalls, filters, etc.) to ensure all electronic files are appropriately scanned for viruses, malware, spyware, phishing, and spam. DCS trains all employees annually on recognizing phishing attempts and conducts periodic phishing simulations to strengthen staff understanding of the risks associated with phishing and spam attempts.

**See Document H. Virus, Spyware, and Malware Protection*

Cybersecurity Measures

The Superintendent and/or designee is authorized to establish, implement, and maintain data and information security measures and procedures. This includes, but not limited to:

- Next-generation firewalls at both the Board of Education data center and school sites
- Endpoint detection and response on all production servers
- Endpoint virus/malware/ransomware protection on all DCS owned Windows Operating System devices
- Principle of Least Privilege for mission-critical hardware and software
- Automated user provisioning and deprovisioning for enhanced security of accounts
- Annual cybersecurity training including phishing simulations.

Users shall neither turn off, attempt to circumvent, nor disable DCS's protection systems or install other systems.

**See Document H. Virus, Spyware, and Malware Protection*

Access Controls

Physical and electronic access to information systems that contain data are controlled. To ensure appropriate levels of access by internal workers, a variety of security measures are instituted as recommended by the Data Governance Committee and approved by DCS. In particular, the Data Governance Committee shall document roles and rights to the student information system and other like systems. Mechanisms to control access to data and computing resources include, but are not limited to, the following methods:

Adopted on June 29, 2026

- **Authorization.** Access shall be granted on a “need to know” basis. It shall be authorized by the superintendent, principal, immediate supervisor, or Data Governance Committee with the assistance of the Director of Technology or designee. Specifically, on a case-by-case basis, permissions may be added to those already held by an individual user in the student management system, again on a need-to-know basis, and only to fulfill specific job responsibilities, with approval of the Data Governance Committee.
- **Context-based access.** Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The “external” factors might include time of day, location of the user, strength of user authentication, etc.
- **Role-based access.** An alternative to traditional access-control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization’s structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.
- **User-based access.** A security mechanism is used to grant users of a system access based on the identity of the user.

*See Document E. Physical and Security Controls

Identification/Authentication

Unique user identification (User ID) and authentication are required to access any and all systems. Users shall be held accountable for all actions performed on the system with their User ID. User accounts and passwords shall NOT be shared. Strictly controlled passwords, biometric identification, and/or Token, PIN, or MFA are used to secure authentication. Only that user and possibly a designated security manager have access to the authentication controls.

*See Document I. Password and Authentication Control Standards

Data Integrity

DCS provides safeguards so that information is not altered or destroyed in an unauthorized manner. Core data are backed up to a private cloud for disaster recovery. In addition, listed below are methods that are used for data integrity in various circumstances:

- Transaction audit
- Disk redundancy (RAID)
- ECC (Error Correcting Memory)
- Checksums (file integrity)
- Data Encryption
- Data Wipes

Transmission Security

Technical security mechanisms are in place to guard against unauthorized access to data that are transmitted over a communications network, including wireless networks or transferred by any means. The following features are implemented when transferring data electronically.

- Integrity controls and
- Encryption, where deemed appropriate
- Access control lists
- Encrypted and decrypted certificates for authentication
- Secure File Transfer Protocols
- OneRoster v1.2 standard API controls
- Data masking

*See Document J. Data Access Roles and Permissions

*See Document D. Data Classification Levels

Adopted on June 29, 2026

Electronic Mass Data Transfers

Downloading, uploading or transferring data between systems shall be strictly controlled via the use of secure APIs. Requests for mass download of, or individual requests for, information for research or any other purposes that include PII, confidential, and/or sensitive data shall be in accordance with this policy and be approved by the Data Governance Committee. All other mass downloads or uploads of information shall be approved by the committee and/or Systems Administrators and include only the minimum amount of information necessary to fulfill the request. A Memorandum of Understanding (MOU) or National Data Privacy Agreement (NDPA) shall be in place when transferring data to external entities such as software or application vendors, textbook companies, testing companies, or any other web-based application, unless the Data Governance Committee approves the exception.

* See Document K. National Data Privacy Agreement (NDPA)

Other Electronic Data Transfers, Sharing, and Printing

PII, confidential, sensitive, and other internal information shall be stored and or printed in a manner inaccessible to unauthorized individuals. PII and Confidential Information shall not be accessed in an unauthorized manner through the use of malicious code execution, unauthorized use of login credentials, or left unattended and open to compromise. Where possible, PII, confidential, and/or sensitive data that is downloaded for educational purposes shall be de-identified before use.

Subpoenas for Electronic Data

Subpoenas issued by courts of competent jurisdiction will be responded to by the Board in compliance with federal and state law pursuant to the advice and direction of the Board Attorney.

DCS Approved Electronic Communication Services

Only DCS district-supported email accounts and FinalSite shall be used for communications to and from school employees, to and from parents or other community members, to and from other educational agencies, to and from vendors or other associations, and to and from students for school business.

Remote Access

This policy establishes standards for connecting to the DCS network or customer networks where DCS provides managed services. Its purpose is to reduce the risk of data breaches, cyber incidents, or unauthorized access that could lead to loss of sensitive data, damage to DCS systems, or harm to the district's reputation.

This policy applies to all DCS staff, contractors, vendors, and agents using DCS-owned or personal devices to perform work remotely, including accessing email and internal web resources.

Remote access is only permitted through DCS-approved VPN solutions and at the approval of the superintendent or designee. All other methods require explicit approval from the Director of Technology or the Data Governance Committee.

Personally Identifiable Information (PII), confidential, or internal data accessed remotely must be protected to the same standards as on-network data. This data may only be stored in cloud services approved by the Data Governance Committee or its designee.

Physical Security

Access to areas in which information processing is carried out shall be restricted only to appropriately authorized individuals. Technology closets, network racks, and/or any infrastructure equipment is housed in locked areas via keyed access or card access.

It is the user's responsibility to ensure that systems above are not left logged in, unattended, and open to unauthorized use.

No technological systems that may contain information as defined above shall be disposed of or moved without adhering to the appropriate Purchasing and Disposal of Electronic Equipment procedures.

*See Document E. Physical and Security Controls

Adopted on June 29, 2026

*See Document L. Purchasing and Disposal Procedures

IT Disaster Recovery

Dothan City Schools must be able to recover critical systems and data within a reasonable timeframe following emergencies. A Disaster Recovery Plan shall be maintained, tested, and updated regularly.

Compliance and Disciplinary Actions

The Data Governance Policy applies to all users of DCS's information, including employees, staff, volunteers, and outside affiliates. Failure to comply with this policy by employees, staff, volunteers, and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable DCS procedures, or, in the case of outside affiliates, termination of the affiliation.

In the event DCS students attempt actions that violate designated access in accordance with DCS' policies, possible disciplinary/corrective action will be instituted per the Student Code of Conduct. A more comprehensive outline of acceptable student behavior in regard to DCS technologies and their use is included in the DCS Acceptable Use Policy. Depending on the nature and severity of the incident, violations may be escalated for legal action or law enforcement involvement in accordance with applicable laws.

Disciplinary actions may be taken for violations, including but not limited to the following:

1. Unauthorized disclosure of PII (Personally Identifiable Information) or Confidential Information.
2. Unauthorized disclosure of a login code (User ID and password).
3. An attempt to obtain a login code or password that belongs to another person.
4. An attempt to use another person's login code or password.
5. Unauthorized use of an authorized password to invade student or employee privacy by examining records or information for which there has been no request for review.
6. Installation or use of unlicensed software on Dothan City School technological systems.
7. The intentional unauthorized altering, destruction, or disposal of Dothan City Schools' information, data and/or systems. This includes the unauthorized removal from DCS of technological systems such as but not limited to laptops, internal or external storage, computers, servers, backups or other media, copiers, etc. that contain PII or confidential information.
8. An attempt to gain access to login codes for purposes other than for support by authorized technology staff, including the completion of fraudulent documentation to gain access.

Audit Controls

Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PII, sensitive, or confidential data are in use. Further, procedures are in place to regularly review records of information system activity, such as audit logs, access reports, and regular cybersecurity audits.

Evaluation

DCS requires that periodic technical and nontechnical evaluations of access controls, storage, and other systems be performed in response to environmental or operations changes affecting the security of electronic PII to ensure its continued protection.

*See Document E. Physical and Security Controls

Supplemental Documents

- A. Definitions and Responsibilities
- B. Laws, Statutory, Regulatory, and Contractual Security
- C. Risk Management Practices
- D. Data Classification Levels
- E. Physical and Security Controls
- F. Software Acquisition Procedures

Adopted on June 29, 2026

- G. Artificial Intelligence (AI) Guidelines
- H. Virus, Malware, Spyware, Phishing and Spam Protection
- I. Password and Authentication Control Standards
- J. Data Access Roles and Permissions
- K. National Data Privacy Agreement (NDPA)
- L. Purchasing and Disposal Procedures