

Dothan City Schools Data Governance Procedure

Committee Members:

Alexis Elston (Media Specialists), Leann Smith (Accounting Specialists), Alyssa Dyer (ESS Director), Cade McCardle (Technology Specialists), Emily Dean (Media Specialists), Jason Thweatt (Network Administrator), Jennifer Peaden (Technology Services Secretary), Jennifer Williams (Assistant Principal), Jeremy Green (Director of Technology), Kacia Thompson (Assistant Superintendent of Curriculum & Instruction), Kimberly Maybin (Media Specialists), Kit Cunningham (Media Specialists), Lori Shaughnessy (Secondary Coordinator), Miranda Brannon (Secretary), Mitzy Martin (Media Specialist), Patrick Pezelj (SIS Data Manager), Ryan Richards (CTE Administrator), Sarahann Odom (ELL Coordinator), Sharla Godwin (Maintenance & Facilities Director), & Sherry Corbitt (Elementary Coordinator).

1. PURPOSE, AUTHORITY, AND ADMINISTRATION

These procedures establish the required administrative, operational, legal, cybersecurity, privacy, AI governance, software approval, access control, retention, disposal, and incident response workflows necessary to implement the Dothan City Schools Data Governance Policy across all district data systems, communications, devices, cloud services, and future technologies.

The Superintendent and/or designee is authorized to establish, implement, maintain, and enforce all supporting standards, processes, and procedures necessary to protect District operations and ensure compliance with Board policy and applicable law.

2. SCOPE

These procedures apply to all students, employees, Board members, vendors, contractors, volunteers, service providers, automated service accounts, and any approved user with access to district systems, services, records, or data.

Covered data includes verbal communications, hard copy records, email, chat, ticketing systems, SIS, LMS, cloud services, backups, exports, screenshots, audio/video recordings, AI prompts, generated outputs, mobile devices, removable media, and printed reports.

3. GOVERNANCE COMMITTEE OVERSIGHT

The Data Governance Committee should operate as a role-based governance body and should review:

- annual policy and procedure revisions
 - software and AI approvals
 - incident findings
 - audit findings
 - risk assessments
 - NDPA workflows
 - access exceptions
 - major system changes
 - legal and regulatory changes
 - disciplinary trends involving unauthorized systems use
-

4. EMPLOYEE ACCOUNTABILITY / APPROVED SOFTWARE / SHADOW IT

Only district-approved software, SaaS platforms, AI systems, browser extensions, websites, mobile applications, cloud services, digital instructional resources, and communication platforms may be used with district accounts, systems, or data.

No employee may independently:

- purchase
- install
- pilot
- create student accounts
- export student rosters
- sync SIS/Clever data
- upload district files
- connect APIs
- deploy AI tools
- use browser extensions
- connect external spreadsheets
- create shadow databases

outside the approved Technology Review Committee workflow.

EMPLOYEE LIABILITY CLAUSE

If an employee uses an unapproved platform, AI tool, application, or online service and that action contributes to:

- cybersecurity incidents
- ransomware or phishing compromise
- FERPA/COPPA/CIPA violations
- licensing violations
- unauthorized disclosure
- data residency violations
- records retention failures
- legal or regulatory exposure
- student safety risks
- financial loss
- reputational harm

the employee may be held individually accountable through disciplinary action up to and including termination, revocation of access, legal review, and referral to law enforcement where appropriate.

The district shall not assume responsibility for unauthorized employee actions that bypass this required workflow.

5. DATA CLASSIFICATION AND HANDLING

All district data should be classified using the current Level 1–4 framework:

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

Controls shall follow the most sensitive element contained within the record regardless of format, including email, print, screenshots, exports, backups, cloud storage, and AI-processed content.

6. ACCESS CONTROL, PASSWORDS, MFA, AND PERMISSIONS

All access shall follow:

- least privilege
- role-based access
- school purpose limitation
- need-to-know authorization
- MFA where supported
- periodic entitlement review
- immediate deprovisioning upon role separation

Password and authentication controls shall comply with District standards, including lockout thresholds, password history, encryption, SSO controls, and prohibition on credential storage.

7. CYBERSECURITY / MALWARE / PHISHING / AI RISK

The District shall maintain a multi-layered defense strategy that may including:

- EDR/XDR
- next-generation firewalls
- DNS filtering
- email security
- cloud file scanning
- ransomware recovery controls
- phishing simulations
- AI risk evaluation
- patching
- immutable backups where supported

Employees shall immediately report suspicious AI outputs, phishing attempts, malicious links, unusual login prompts, or suspected ransomware indicators.

8. RISK MANAGEMENT AND CHANGE CONTROL

Formal risk assessments may occur:

- prior to major implementations
 - after significant incidents
 - during vendor onboarding
 - after legal or regulatory changes
 - during annual governance review
 - when shadow IT or unauthorized software patterns emerge
-

9. DATA SHARING / NDPA / THIRD-PARTY ACCESS

All third-party student data sharing shall require:

- approved business purpose
- minimum necessary data
- DPA / NDPA execution
- board attorney review where required
- Superintendent execution
- vendor registry update
- retention/destruction terms
- breach notification obligations

No employee may share district data externally outside this workflow.

10. AI USE, REVIEW, AND HUMAN OVERSIGHT

All AI systems must complete the district AI review and approval workflow before use. AI shall supplement—not replace—human instructional judgment, employee decision-making, student evaluation, discipline decisions, or legal determinations.

No student, employee, HR, discipline, health, or confidential records may be uploaded into non-approved generative AI systems.

11. INCIDENT REPORTING, BREACH RESPONSE, AND LEGAL HOLDS

All users shall immediately report:

- lost devices

- phishing interactions
- suspicious vendor requests
- data misdelivery
- improper exports
- privilege misuse
- suspected account compromise
- unauthorized AI use
- records deletion errors
- ransomware indicators
- exposed printed reports

Failure to report promptly may itself constitute a policy violation.