

Tallapoosa County Schools

Data Governance and Information Security Policy

I. Purpose

The purpose of this policy is to establish a comprehensive, cohesive framework for the governance, protection, and appropriate use of data and information maintained by Tallapoosa County Schools (TCS). This policy ensures that district data are accurate, secure, lawful, and used responsibly to support instruction, operations, accountability, and decision-making.

This policy integrates principles of **data governance**, **student data privacy**, and **information security** and is intended to safeguard data throughout its full lifecycle—collection, use, sharing, retention, and disposal.

II. Authority

The Superintendent is authorized to establish, implement, and enforce data governance and information security measures consistent with this policy. The Superintendent may designate responsibilities to district personnel as necessary to ensure compliance.

III. Scope

This policy applies to:

- All Tallapoosa County Schools employees
- Students
- Volunteers
- Contractors, vendors, and third-party service providers
- Any other individual or entity granted access to district data or information systems

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

- Electronic data stored or transmitted via district systems or cloud-based services
- Paper records

- Oral communications
 - Data transmitted via email, messaging platforms, applications, or other communication tools
-

IV. Governance Structure

A. Data Governance Committee

The Data Governance Committee provides oversight and strategic direction for data governance, privacy, and information security within Tallapoosa County Schools.

Responsibilities include:

- Reviewing and updating this policy annually
- Establishing data governance standards and guidance
- Reviewing data access and data-sharing requests involving sensitive data
- Overseeing compliance with applicable laws and regulations
- Advising the Superintendent on data governance and security matters

The committee shall include representatives from district administration, technology, instruction, student services, and other areas as determined by the Superintendent.

B. Information Security Officer (ISO)

The Information Security Officer is responsible for coordinating the district's information security program and advising the Data Governance Committee and Superintendent on security risks and controls.

V. Legal and Regulatory Compliance

Tallapoosa County Schools shall comply with all applicable federal, state, and local laws and contractual obligations related to data privacy and information security, including but not limited to:

- Family Educational Rights and Privacy Act (FERPA)
- Protection of Pupil Rights Amendment (PPRA)
- Children's Online Privacy Protection Act (COPPA)
- Children's Internet Protection Act (CIPA)
- Alabama Records Disposition Authority requirements
- Payment Card Industry Data Security Standard (PCI DSS), where applicable

FERPA governs most student education records, including student health records maintained by the district. HIPAA applies only in limited circumstances where district services meet the legal definition of a covered entity.

VI. Roles and Responsibilities

A. Data Owners

Data Owners are district administrators responsible for specific data systems or datasets.

Responsibilities include:

- Determining appropriate use and access
- Classifying data
- Approving access requests
- Ensuring compliance with retention and disposal requirements

B. Data Stewards

Data Stewards are responsible for ensuring data quality, accuracy, and appropriate use.

Responsibilities include:

- Monitoring data accuracy and completeness
- Correcting errors promptly
- Supporting training and guidance for users

C. Data Custodians

Data Custodians manage the technical environment in which data are stored and processed.

Responsibilities include:

- Implementing security controls
- Managing user access
- Supporting secure storage, transmission, and disposal

D. Data Users

Data Users are individuals authorized to access district data.

Responsibilities include:

- Accessing data only for legitimate educational or operational purposes
 - Protecting credentials
 - Reporting suspected security incidents immediately
-

VII. Data Classification

All district data shall be classified according to sensitivity:

A. Restricted Data

Includes Personally Identifiable Information (PII) and other highly sensitive data protected by law.

B. Confidential Data

Sensitive operational data not classified as Restricted but requiring controlled access.

C. Internal Data

Information intended for internal district use.

D. Public Data

Information approved for public release.

Data shall be protected according to its highest classification regardless of format.

VIII. Directory Information

Tallapoosa County Schools may designate certain student information as directory information in accordance with FERPA. Parents and eligible students shall receive annual notice of directory information and the right to opt out.

The district shall periodically review directory information categories to ensure alignment with privacy and safety best practices.

IX. Data Access and Use

Access to data shall be granted on a **least-privilege** and **need-to-know** basis. Unauthorized access, use, disclosure, or distribution of district data is prohibited.

Only district-approved systems and accounts may be used for official business.

X. Vendor and Third-Party Data Governance

Third-party vendors with access to district data must:

- Use data only for authorized purposes
 - Implement appropriate security safeguards
 - Comply with FERPA and applicable laws
 - Execute data privacy and security agreements approved by the district
-

XI. Information Security Controls

Tallapoosa County Schools shall implement administrative, technical, and physical safeguards to protect data, including:

- User authentication and access controls
- Secure transmission and storage
- Physical security of facilities and equipment
- Malware and threat protection

Detailed technical controls shall be documented in administrative procedures.

XII. Incident Response and Breach Management

All suspected or confirmed data security incidents shall be reported immediately to the Information Security Officer.

The district shall maintain documented procedures for:

- Incident investigation
- Mitigation and recovery
- Notification as required by law
- Documentation and review

XIII. Data Retention and Disposal

Data shall be retained and disposed of in accordance with Alabama Records Disposition Authority schedules and district procedures. Disposal methods shall ensure data cannot be reconstructed or retrieved.

XIV. Training and Awareness

Annual data governance and information security training is required for all employees and applicable users. Training shall be documented.

XV. Compliance and Enforcement

Failure to comply with this policy may result in disciplinary action in accordance with district procedures and applicable law.

XVI. Policy Review

This policy shall be reviewed annually by the Data Governance Committee and updated as necessary to reflect changes in law, technology, and district operations.