

Software Acquisition Procedures

1. Purpose

This procedure establishes the required process for requesting, reviewing, approving, piloting, purchasing, implementing, and renewing software platforms, digital tools, applications, and hosted services used by Dothan City Schools.

The purpose of this procedure is to ensure all software acquisitions align with instructional goals, operational needs, legal compliance, cybersecurity requirements, student data privacy expectations, budget sustainability, and long-term district technology standards.

No software, application, browser extension, SaaS platform, AI platform, or digital service may be purchased, deployed, piloted, integrated, or used with District data until all requirements in this procedure have been completed.

2. Request Submission and Initial Requirements

A software request may be submitted by a school principal, district director, or department leader for consideration at an upcoming Technology Review Committee (TRC) meeting.

All requests must be submitted using the official request form on the DCS Technology Services website.

All required fields must be completed for the request to be placed on the agenda.

Required Submission Information

Each request must include, at minimum:

- Name of the software, tool, or platform
- Vendor/company name
- Instructional or operational purpose
- Business need and desired outcomes
- Description of how students and/or staff will interact with the tool
- Method of access (Clever, SSO, direct login, SIS rostering, manual accounts, etc.)
- Whether students create profiles or accounts
- Data elements required for use
- Link to vendor website
- Link to privacy policy and terms of service
- Funding source for purchase and renewals
- Estimated cost and license structure
- Requested implementation timeline
- Curriculum or department sponsor

Any request related to curriculum, instruction, assessment, or classroom use must include recommendation from the Instructional Services Department or Director before committee review.

3. Technology Review Committee Process

The Technology Review Committee shall meet quarterly to review submitted requests.

The committee may vote to:

- Approve
- Conditionally approve
- Partially approve
- Deny
- Table for additional information

Conditional approvals may require pilot testing, revised scope, grade-level limitations, contractual changes, privacy clarifications, or additional technical validation.

No software may move forward until formal committee action is documented.

4. Mandatory Approval Standards

All proposed platforms must meet the following minimum standards:

- Compliance with FERPA, COPPA, CIPA, CALEA, applicable Alabama student data privacy requirements, and other relevant law
 - HIPAA alignment where school health, counseling, nursing, or protected health workflows may apply
 - No unauthorized sharing of District data with third parties without prior written District consent
 - No sale, advertising use, profiling, or behavioral tracking of student data
 - Data residency restricted to the continental United States unless explicitly approved in writing
 - Must support integration with Clever, District SSO, and/or the current Student Information System (SIS) where applicable
 - Must support required cybersecurity controls including MFA, secure authentication, encryption, and auditability where applicable
 - Must align with age appropriateness, parental notice, and school-purpose limitations
-

5. Data Privacy and Software Vetting Criteria

The committee shall evaluate all software using a formal privacy and governance review that includes internal review processes and external trusted evaluation resources.

To support consistent and defensible vetting decisions, the committee may use trusted third-party evaluation and standards platforms, including:

- 1EdTech TrustEd Apps
- Access for Learning (A4L)
- Common Sense Privacy and Evaluation resources
- Other recognized K-12 privacy, interoperability, and standards-based review frameworks approved by the District

These resources may be used to validate interoperability, roster standards, data privacy expectations, vendor trust signals, and existing K-12 review history.

The committee shall evaluate all software using a formal privacy and governance review that includes the following topics:

- Data collection
- Data sharing
- Data security
- Data ownership and rights
- Individual user control
- Whether data is sold or monetized
- Student safety and content protections
- Advertising and tracking technologies
- Parental consent requirements
- Legitimate school purpose
- Vendor breach history and incident response practices
- Data deletion and retention procedures
- AI or algorithmic decision-making risks

The District shall practice due diligence by reviewing the vendor's:

- Security track record
- K-12 experience
- Existing client references
- Financial stability and long-term viability
- Integration maturity
- Product roadmap and support model

Where appropriate, the District may request references from similarly sized K-12 districts that have used the platform for at least 12 months.

6. Data Protection Agreement (DPA) Process

If approved by the committee, the requestor shall coordinate with the vendor to complete the required Data Protection Agreement (DPA).

DPA Workflow

1. Vendor completes its required DPA sections
2. DPA is submitted for Board attorney review
3. Following attorney approval, the Superintendent may execute the agreement
4. A fully executed copy must be sent to the Director of Technology for records retention and compliance filing
5. The approved platform and relevant metadata shall be entered into the 1EdTech TrustEd Apps / approved platform registry

No software may be purchased, used, piloted, or integrated prior to full DPA execution.

If the cost exceeds procurement thresholds, Board approval may also be required before purchase.

7. Evaluation and Testing Procedures

During the Evaluate and Test Software Packages phase, software shall be assessed against current District standards and the viability of implementation into the DCS technology environment.

Evaluation activities may include:

- Beta testing or pilot deployments
- Limited user group trials
- Bandwidth and storage impact analysis
- Hardware and endpoint compatibility review
- SIS, Clever, SSO, and rostering validation
- Accessibility and ADA review
- Device age and browser compatibility testing
- Review of classroom and instructional workflow fit
- License structure and renewal analysis
- Vendor maintenance and patching process review
- Backup/export capability validation
- Cybersecurity scanning or secure architecture review
- Training plan development
- Funding sustainability review for initial and recurring costs

The evaluation must determine whether the software can be implemented without negatively affecting:

- Network performance
 - Internet bandwidth
 - Endpoint stability
 - Student data protections
 - Existing classroom workflows
 - State testing environments
 - Device lifecycle standards
-

8. Pilot Program Requirements

Whenever feasible, approved software shall first be deployed as a pilot program before broad district rollout.

Pilot programs should:

- Validate instructional or operational value
- Confirm integration performance
- Minimize business and classroom disruptions
- Provide measurable proof of effectiveness
- Allow vendors to resolve issues before full deployment
- Build leadership and stakeholder confidence
- Support future funding justification

Pilot outcomes must be documented and reviewed before districtwide adoption.

9. Final Implementation Authorization

Only after completion of all required steps may the requestor proceed with:

- Purchase
- Training
- Pilot expansion
- SIS/Clever integration
- Rostering
- Staff rollout
- Student deployment
- Parent communications
- Renewal scheduling

The Director of Technology or designee shall maintain the official approved software inventory.

10. Renewal and Continued Use Review

Prior to renewal, all software platforms shall undergo continued-use review to confirm:

- Ongoing instructional or business value
- Continued legal compliance
- DPA validity
- Security posture remains acceptable
- Vendor viability remains strong
- Licensing remains cost effective
- Redundant functionality does not already exist elsewhere in the District

The cost and disruption of changing platforms is significant; therefore, the District should change providers only when clearly justified by security, compliance, functionality, or operational need.

11. Prohibited Practices

The following are prohibited:

- Use of unapproved software with District accounts or data
 - Teacher or department purchases outside this process
 - Student account creation without approved privacy review
 - Use of software storing data outside approved geographic boundaries
 - Installation of browser extensions or apps not approved by the District
 - Any platform that monetizes student or employee data
-