ADMINISTRATIVE GUIDELINE: THIRD-PARTY APPLICATION ACCESS IN GOOGLE WORKSPACE

Effective Date: October 2026

Issuing Department: Information Technology & District Administration

Applies To: All District Employees, Contractors, and Authorized Account Holders

1. Purpose

This administrative guideline establishes security and privacy controls governing the integration of third-party applications, add-ons, and browser extensions with district-managed Google Workspace accounts. These measures are designed to protect student and staff data from unauthorized disclosure and ensure strict compliance with the Family Educational Rights and Privacy Act (FERPA) and applicable state data privacy regulations.

2. Scope

This guideline applies to all individuals utilizing a district-issued Google Workspace account (`spartaschools.org`) across any district-owned or personal device.

3. Access Controls and Authorization Standards

To prevent unvetted vendors from accessing sensitive district records, the district enforces the following access tiers for third-party applications:

- **Basic Authentication (Permitted):** Users may utilize their district Google credentials to log into external websites and applications that request only basic profile information required for **"Sign in with Google"** (specifically: name, district email address, and profile image).
- **District Data Scopes (Restricted by Default):** Third-party applications that request permission to view, create, edit, transmit, or manage district data—including files in Google Drive, messages in Gmail, Google Calendar events, Contacts, or Google Classroom rosters—are blocked by default.
- **Requirement for District-Level Agreements:** Data-level access will be granted exclusively to applications supported by an active, district-authorized subscription,

contract, or executed Data Privacy Agreement (DPA) on file with the Information Technology department.

- **Prohibition of Personal and Private Subscriptions:** The district will not authorize or whitelist third-party applications tied to individual user accounts, personal credit card purchases, free trials, or unvetted "click-wrap" terms of service. This restriction applies even if the application is intended solely for classroom instruction or district business.

4. Application Request and Vetting Procedure

Staff members seeking to use a restricted third-party application that requires access to district Google Workspace data must follow this process prior to purchasing a license or onboarding students:

1. **Submit a Vetting Request:** Complete and submit a software review ticket via General Tech Request.
2. **Privacy and Security Evaluation:** The Information Technology department (in coordination with Curriculum/Administration, as applicable) will review the vendor's privacy policy, data encryption standards, and willingness to sign a district Data Privacy Agreement.
3. **Authorization or Denial:**
    - **Approved:** Once a formal district agreement or subscription is executed, IT will configure Google Workspace to allow access for authorized users.
    - **Denied:** If the vendor fails to meet FERPA or district security standards, access will remain blocked, and staff must select an approved district alternative.

5. Compliance and Data Handling

Staff members are prohibited from circumventing third-party access restrictions by manually downloading, exporting, or copying student records or confidential district files from Google Drive or Gmail and uploading them into unapproved third-party platforms. Adherence to this guideline is mandatory under the Sparta Area Schools **Acceptable Use Policy (AUP)** and Board Policy **7540**.