ATLANTA PUBLIC SCHOOLS | Division of Information Technology



APS DATA GOVERNANCE

FREQUENTLY ASKED QUESTIONS (FAQs)

PREPARED BY: APS IT/PMO GOVERNANCE

Last Updated: November 4, 2026

Contents

PURPOSE 3
GENERAL GOVERNANCE OVERVIEW 3
What is IT Governance? 3
What is Data Governance? 3
Why are IT and Data Governance important? 3
RISKS OF IGNORING GOVERNANCE 4
IT COMPONENTS AND PURCHASING 4
What is considered an “IT Component”? 4
What purchases require IT review? 5
What is the new P-Card process for IT-related purchases? 5
Why were some P-Card transactions declined? 6
How does centralized procurement benefit APS? 6
DATA HANDLING AND SECURITY 6
How does data governance protect me and my school? 6
How does data governance support APS systems like ERP? 6
How can I participate in IT governance? 6
COMMUNICATION, TRAINING & SUPPORT 7
Will training be provided? 7
When will the Governance rollout take effect? 7
Who should I contact for questions or approval? 7
Summary 7
IT SECURITY AND DEVICE POLICY UPDATES 8
Data Storage and Use Policy 8
Network-Connected Peripherals Policy 8
Smart Devices and Network Access Policy 8
Glossary | IT Governance Glossary and Acronym Reference 9
A. CORE GOVERNANCE TERMS 9
B. TECHNOLOGY & SECURITY TERMS 9
C. PROCUREMENT & FINANCE TERMS 10
D. DATA, COMPLIANCE & REGULATORY TERMS 10
E. ROLES & RESPONSIBILITIES 10
F. TRAINING & COMMUNICATION TERMS 11
G. ACRONYM QUICK REFERENCE 11

PURPOSE

This FAQ provides guidance for all Atlanta Public Schools (APS) employees on how to make informed technology and data decisions that align with district policy, ensure fiscal responsibility, and protect student and staff information. It explains the principles of **IT Governance** and **Data Governance**, how they work together, and what each employee's role is in safeguarding APS systems and data.

GENERAL GOVERNANCE OVERVIEW

What is IT Governance?

IT Governance establishes policies, procedures, and accountability for all technology decisions across APS. It ensures that every device, application, and system:

- Supports district goals and instructional priorities,
- Meets security and compliance requirements, and
- Is purchased, implemented, and maintained in a coordinated and cost-effective manner.

What is Data Governance?

Data Governance is the framework of **people, processes, policies, and standards** that ensures effective management, integrity, and protection of data within APS.
It defines **who owns data, how it is used, and how it is protected** to support student achievement, informed decision-making, and operational efficiency.

Why are IT and Data Governance important?

Strong governance:

- **Protects student and employee data** under FERPA, COPPA, and HIPAA.
- **Improves decision-making** through consistent, reliable information.
- **Eliminates redundancy** and prevents duplicate or unauthorized systems.
- **Optimizes resources** and ensures equitable access to technology.
- **Promotes accountability** across schools and departments.

RISKS OF IGNORING GOVERNANCE

Ignoring governance policies creates measurable risk to APS operations and reputation:

- **Data Privacy Violations:** Unvetted software may expose confidential data.
- **Financial Waste:** Redundant purchases of applications already owned by the district.
- **Security Gaps:** Unauthorized apps often lack MFA, SSO, and SOC 2/3 compliance.
- **Operational Strain:** IT staff spend valuable time supporting unsupported tools.
- **Regulatory Noncompliance:** Violations of FERPA/COPPA can result in fines, lawsuits, and loss of public trust.

IT COMPONENTS AND PURCHASING

What is considered an "IT Component"?

Any product, service, or software that connects to, stores, processes, or transmits data on the APS network, or that requires technical setup, licensing, or security review.

If it plugs in, connects online, or uses software—it's an IT component.

The Purchase Card Process Board policy states: "**The following types of purchases are strictly prohibited by Atlanta Public Schools:** Data plans, software, or electronics, including, but not limited to, laptop computers, tablets, smartphones, or computer hardware (unless authorized by the IT department)." Our **IT Guidelines** provide a comprehensive list of what is and is not permitted below:

Strictly Prohibited Purchases (Must be handled by our IT Department):

- Laptop, desktop computers, iPad and tablets, Chromebooks, smartphones, and any computer hardware.
- Interactive Panels and Audio-Visual equipment.
- Networked equipment, Routers, Wi-Fi hotspots, modems, wireless access points, or network switches.
- Security cameras, badge systems, servers, and any other security or surveillance hardware.
- Projectors, servers, and other hardware that require network connectivity/integration.
- Uninterrupted Power Supplies (UPS units)
- Software, mobile apps, and cloud-based services (e.g., Grammarly, Slack, Calendly)
- File-sharing tools (Dropbox, ShareFile, Google Workspace)

What purchases require IT review?

Before purchasing, **staff must confirm with IT** if the product falls into these categories:

- **ALL** software, including student learning/instructional applications, online resources, cloud services, and recurring subscriptions. A ticket must be submitted to the IT department for verification and should be submitted through our IT Marketplace.
- **ALL** printers, copiers, and scanners must be verified by IT to ensure network compatibility and security.
- Flash drives, hard drives, and other portable storage.
- Smart TVs, and specialized sound systems.
- 3D printers, robotics kits, Robots, and any other equipment that may require a network connection or specialized software.

Authorized purchases that **do not** require IT approval:

- Mice, monitors, portable monitors, keyboards, wired headphones, external microphones, and drawing pads that connect via standard USB or Bluetooth and do not require network services.
- VGA, HDMI, basic adapters, and cables.
- Printer toner/ink (for approved printers) and replacement parts.
- Desk pads, mouse pads, desktop covers, and screen protectors
- Photography Cameras requiring network connectivity.

What is the new P-Card process for IT-related purchases?

APS has implemented an **automated P-Card control system** to ensure compliance and prevent unauthorized software or technology purchases

Key details:

1. **Automatic Decline:** If a purchase is made under specific Merchant Category Codes (MCCs) 5734, 7372, or 4816—it will automatically be declined.
2. **Special Authorization Form:** The cardholder must complete a "P-Card Special Authorization Form" and select "Purchase – Has IT Component."
3. **IT Review:** The form routes to the IT Governance team for review and SOC 2 verification, if required.
4. **Approval & Unlock:** If approved, the P-Card is temporarily unlocked for 48 hours to complete the purchase.

This process ensures compliance, data protection, and fiscal accountability.

Why were some P-Card transactions declined?

Declines occur when the purchase:

- Exceeds the $2,000 limit,
- Matches an IT or software merchant category, or
- Violates APS purchasing policy (e.g., unapproved technology).
  To resolve, submit the required **Special Authorization Form** and await IT or Finance approval.

How does centralized procurement benefit APS?

Centralized procurement:

- Prevents redundant software licenses,
- Increases APS buying power with vendors,
- Improves security and compliance monitoring, and
- Ensures equitable access to technology across all schools

DATA HANDLING AND SECURITY

How does data governance protect me and my school?

- It clarifies **data ownership** and **access permissions**.
- Ensures all data is accurate, secure, and compliant.
- Reduces confusion over who maintains records or reports.
- Helps you meet compliance obligations and avoid violations.

How does data governance support APS systems like ERP?

Data governance ensures that data across systems is standardized and interoperable, which is critical for enterprise systems such as ERP, HR, and student information management.
Accurate, structured data enables automation, analytics, and better decision support

How can I participate in IT governance?

Every employee has a role:

- Follow APS data handling and technology policies.
- Use only approved systems and tools.
- Report any data quality or security concerns to IT.
- Attend governance training sessions.
- Collaborate with data stewards and governance teams when working with shared datasets.

COMMUNICATION, TRAINING & SUPPORT

Will training be provided?

Yes. APS will provide:

- **Microlearning modules** and **virtual workshops** on IT Governance.
- **"Governance in Action"** success stories featuring APS schools.
- **Quick reference guides** and **FAQs** via the APS intranet and newsletters.

When will the Governance rollout take effect?

The official rollout begins **November 15, 2025**, with continuous updates through early 2026 as systems, training, and enforcement are phased in

Who should I contact for questions or approval?

Area	Contact	Email
IT Governance	IT Governance Committee	ITGovernance@atlanta.k12.ga.us
Finance & Procurement	APS Finance Division	APSFinance@atlanta.k12.ga.us
PMO & Project Intake	IT Governance & PMO	ITPMO@atlanta.k12.ga.us

Summary

APS's IT Governance program ensures:

- Security of student and staff information
- Accountability in spending
- Compliance with federal regulations
- Alignment with district goals
- Trust and transparency across the APS community

IT SECURITY AND DEVICE POLICY UPDATES

Data Storage and Use Policy

- **Policy Correction:** Data stored externally must primarily contain work-related materials. APS-issued devices are **not intended** for personal use. This includes storing personal files on the device, as well as the use of personal external storage devices (Ex: flash drives).

Network-Connected Peripherals Policy

- **Policy Update (Printers, Copiers, and Scanners):**
    - To ensure network security and compatibility, all printers, copiers, and scanners must be verified and authorized by the IT Department **prior to installation**.
    - **New Requirement:** New or replacement printing devices must connect **directly to a computer via USB cable** (USB printed only).
    - **Prohibited Connections:** Connection via **Bluetooth or direct wireless network access** is strictly prohibited for these devices.

Smart Devices and Network Access Policy

- **Smart Device Restrictions:**
    - **Smart TVs:** Only **"dumb" or non-network-enabled** displays are permitted. Displays connected to the APS network are strictly prohibited due to potential **open microphone risks and student data privacy concerns**.
    - **Voice-Activated Assistants (Open Mic Risk):** Personal smart devices such as Google Homes, Amazon Alexas, and Apple HomeKit devices are **not permitted** in the APS environment due to inherent open microphone risks and potential student data security concerns.
    - **Specialized Sound Systems:** Specialized sound systems must be reviewed and authorized by IT.
- **Personal Device Network Access:**
    - Personal mobile devices (ex: iPads, phones) are permitted to connect to the dedicated personal Wi-Fi network but **must strictly adhere to all established APS network security best practices and policies**.
    - **Gaming Systems:** Gaming consoles and unauthorized recreational systems are **not allowed** to connect to the APS network or be used within the APS environment.

Glossary | IT Governance Glossary and Acronym Reference

A. CORE GOVERNANCE TERMS

Term	Definition
IT Governance	The framework of policies, processes, and oversight that ensures APS technology decisions align with district goals, regulatory requirements, and fiscal responsibility. It manages the lifecycle of systems, applications, and devices across all schools and departments.
Data Governance	The people, processes, and policies that ensure the quality, security, privacy, and proper use of data across APS. It defines who owns data, how it is accessed, and how it supports decision-making.
Shadow IT	Any system, software, or service used without approval or oversight from the IT Division. Shadow IT increases cybersecurity, compliance, and fiscal risks.
Compliance	Adherence to laws, regulations, and internal APS policies such as FERPA, COPPA, HIPAA, and the district's procurement and data security standards.
Governance Committee	The APS cross-functional group is responsible for reviewing IT-related requests, ensuring proper vetting, security, and alignment with district standards.
Security Posture	The overall strength of APS's cybersecurity controls and readiness against threats such as ransomware, phishing, and unauthorized access.
Centralized Procurement	A purchasing model in which APS negotiates and manages technology contracts at the district level to ensure consistency, compliance, and cost savings.
Decentralized Procurement	School- or department-level technology purchasing without centralized review; often associated with redundant spending and increased risk.
Outcomes-Based Contracting	A funding model that ties vendor payments to measurable improvements (e.g., student outcomes, uptime metrics, performance KPIs).
Adoption	The process of implementing and sustaining use of approved systems across APS. Includes user access management, training, and periodic review.
Governance Rollout	The staged implementation of APS's IT Governance framework, beginning November 15, 2025.

B. TECHNOLOGY & SECURITY TERMS

Term	Definition
IT Component	Any item, software, or service that connects to, stores, processes, or transmits data on the APS network—or requires technical setup, licensing, or security oversight from IT.
SOC 2 / SOC 3 Report	A third-party audit that verifies a vendor's data security, availability, and confidentiality controls. Required for high-risk or cloud vendors.
Single Sign-On (SSO)	A centralized authentication method that allows users to access multiple applications with one set of credentials—reducing password fatigue and improving security.
Multi-Factor Authentication (MFA)	An extra layer of security requiring a second form of verification (such as a code or app) in addition to a password.
Phishing / Spear Phishing	Fraudulent email or communication attempts that trick users into revealing sensitive information or credentials.
Password Spray Attack	A hacking attempt using common passwords across multiple accounts to gain unauthorized access.
Attack Surface	The total number of potential points where unauthorized users can access or compromise APS systems.
Cloud Identity Abuse	Unauthorized access or misuse of cloud-based credentials or accounts.
ERP (Enterprise Resource Planning)	A centralized system that integrates APS business processes such as finance, HR, procurement, and operations, ensuring data consistency and efficiency.
SOC Compliance	Adherence to the Service Organization Controls (SOC) standards for data protection, especially when using third-party cloud vendors.

C. PROCUREMENT & FINANCE TERMS

Term	Definition
P-Card (Procurement Card)	A district-issued payment card used by APS employees for approved purchases. IT-related transactions are restricted and must follow the governance review process.
Merchant Category Code (MCC)	A four-digit code assigned by credit card companies identifying the type of business. Certain MCCs (e.g., 5734, 7372, 4816) automatically trigger IT review.
Special Authorization Form (P-Card)	A form completed when a transaction is declined or involves IT components. It routes the purchase to IT Governance and Finance for approval.
SPLOST (Special Purpose Local Option Sales Tax)	A local sales tax that funds capital projects in APS, including technology and infrastructure improvements.
Capital Outlay	Funds used for long-term assets such as equipment, buildings, or technology infrastructure. Must align with SPLOST or district goals.
Outcomes-Based Contract	A vendor agreement linking payments to measurable results, ensuring accountability for performance.
Budget Alignment	The process of ensuring technology purchases are tied to strategic outcomes, measurable goals, and available funding models.

D. DATA, COMPLIANCE & REGULATORY TERMS

Term	Definition
FERPA (Family Educational Rights and Privacy Act)	Federal law protecting the privacy of student education records. Governs disclosure and access to student data.
COPPA (Children's Online Privacy Protection Act)	Federal law regulating online collection of personal information from children under 13.
HIPAA (Health Insurance Portability and Accountability Act)	Law that ensures the confidentiality and security of personal health information. Relevant for student and employee health data.
PII (Personally Identifiable Information)	Any data that can identify a student, employee, or parent—such as name, ID number, or date of birth.
Data Steward	A designated staff member responsible for managing and maintaining data accuracy, quality, and compliance within a specific area.
Data Integrity	The accuracy, consistency, and reliability of data throughout its lifecycle.
Data Lifecycle	The process of data creation, use, storage, sharing, and disposal according to APS standards.
Data-Sharing Agreement (DSA)	A formal agreement outlining how data is shared between APS and a third party, including security and compliance terms.

E. ROLES & RESPONSIBILITIES

Role	Description
IT Governance Manager	Leads implementation of APS IT Governance policies and ensures district-wide compliance.
IT Division	Oversees district technology strategy, infrastructure, cybersecurity, and support.
Governance & PMO Team	Manages the project intake, prioritization, and governance review for IT initiatives.
Principals & School Leaders	Ensure school-level purchases and processes align with governance policies.
Bookkeepers / Business Managers	Manage P-card transactions and ensure purchases follow IT review and Finance policy.
IT Governance Team	Oversee data management standards, compliance, and staff training.
End Users (All Staff)	Responsible for using approved systems, maintaining data privacy, and reporting security or data issues.

F. TRAINING & COMMUNICATION TERMS

Term	Definition
Governance Training Modules	Short, required online sessions explaining APS IT Governance policies and purchasing processes.
Governance Campaign	District-wide communication initiative promoting awareness of IT Governance, launching Fall 2025.
Awareness Materials	Flyers, infographics, and videos reminding staff to check IT approval before buying or using new tools ("Stop. Check. Verify before you buy.").
Governance Champions	Staff designated at each school or department to reinforce compliance and serve as local points of contact.
Feedback Loop	Mechanism for collecting staff input to improve policies and user experience in governance processes.

G. ACRONYM QUICK REFERENCE

Acronym	Full Term
APS	Atlanta Public Schools
PMO	Project Management Office
IT	Information Technology
MFA	Multi-Factor Authentication
SSO	Single Sign-On
ERP	Enterprise Resource Planning
SOC	Service Organization Control
DSA	Data-Sharing Agreement
FERPA	Family Educational Rights and Privacy Act
COPPA	Children's Online Privacy Protection Act
HIPAA	Health Insurance Portability and Accountability Act
PII	Personally Identifiable Information
MCC	Merchant Category Code
P-Card	Procurement Card
SPLOST	Special Purpose Local Option Sales Tax
KPI	Key Performance Indicator
PM	Project Manager
SLA	Service Level Agreement
ITSM	IT Service Management