

Asset Management

This category asks a blunt question: do you know every device, application, cloud service, and data store your district owns or uses — and who is responsible for each? You cannot patch, back up, monitor, or...

Why it matters

- Every other safeguard depends on the inventory. A server, camera controller or old wireless controller that nobody listed is one nobody patches, backs up or monitors, and that is exactly the kind of system attackers look for.
 - When a vendor reports a breach, the superintendent, families and counsel will ask which students and what data were involved. A data inventory with owners and signed data privacy agreements (DPAs) lets you answer from records instead of guessing, and decide on notification with facts.
 - An accurate inventory turns device refresh planning, E-Rate Category Two requests and cyber insurance applications into lookups. Its end-of-support column shows you which systems a carrier may treat as unsupported before the carrier finds them.
- Cyber insurance applications and audits start with inventory counts, and a wrong answer there can jeopardize a claim. A current, owned inventory is the foundation every other rubric category builds on.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	<p>Device, software and data records live in several places (an old spreadsheet, the admin console, purchase orders) and nobody reconciles them. Assets are discovered when something breaks, goes missing or an auditor asks.</p> <p>Moving up: Pick one inventory of record, bring it current, and assign an owner with a set update cadence tied to summer deployment and device collection. Current inventories maintained by a consistent process — not a one-time cleanup — is what Level 2 requires.</p>	<ul style="list-style-type: none"> • No single inventory of record; device counts differ between the admin console, the business office and building lists • Teachers sign up for apps with district accounts and no one can say which ones hold student data • Retired laptops, servers and copier drives sit in a closet or go to surplus with no record of wiping
2 · Repeatable	<p>One inventory of record is kept current by a named owner on a consistent cycle tied to summer deployment, device collection and monthly reconciliation. Controls such as disabling stale devices and an app request form are being added but still respond mostly to problems.</p> <p>Moving up: Document each asset's full life cycle from purchase to wiped disposal, define data classifications that follow your state's standards and legal requirements, and put controls around take-home devices, software installs, and asset transfers.</p>	<ul style="list-style-type: none"> • Inventory spreadsheet or asset system with serial numbers, assigned users and locations, reconciled against the admin console export within the last quarter • Stale-device report run on a set schedule, with missing devices disabled and listed for building follow-up • First version of an approved-apps list and a request form that routes new tools to IT before classroom use
3 · Defined	<p>Every asset is tracked from purchase through assignment, transfer, repair and documented disposal. Data is classified using state standards and legal requirements, and written controls cover take-home devices, software installation and moving equipment between schools.</p> <p>Moving up: Add metrics: spot-audit inventory accuracy on a schedule, report compliance rates, run root-cause analysis when devices turn up missing or unmanaged, and test your protection controls — for example, verify a 'wiped' device really is wiped.</p>	<ul style="list-style-type: none"> • Written life-cycle procedure covering tagging, assignment, transfers between buildings, repair and wipe-and-dispose, with certificates of destruction tied to serial numbers • Data inventory with a classification for each system (for example public, internal, confidential, restricted) that references FERPA, Georgia's student data privacy law and the records-retention schedule • Take-home device agreement plus enforced device policies for off-campus use (content filtering, remote lock and wipe) and standard user accounts that cannot install software without approval

Level	What you would see	Artifacts that show it
4 · Managed	Inventory work is measured. The district samples records against physical devices on a schedule, tracks the accuracy rate over time, finds the root cause when assets turn up missing or unmanaged, and tests whether protection controls actually work. Moving up: Integrate inventory data with refresh budgeting, risk strategy, and system-wide planning so the inventory drives decisions rather than just recording them, and benchmark your process against peer districts and best practice.	<ul style="list-style-type: none"> Spot-audit results each semester comparing a sample of devices on shelves and carts with the inventory, with the match rate tracked from audit to audit Root-cause notes for unmanaged or missing devices (for example a school that skipped the check-in step) and the corrective action taken Test record showing a sample of wiped devices checked for recoverable data before they leave district custody
5 · Optimized	Inventory data drives system-wide decisions. Refresh budgets, end-of-support planning, risk ranking and insurance answers all come from the same automatically maintained records, and the process is benchmarked and improved.	<ul style="list-style-type: none"> Multi-year refresh and end-of-support forecast built from the inventory and used in budget development Automated discovery that reconciles network scans, management consoles and the identity directory into the inventory without manual re-keying Benchmark review against peer districts or the CIS Controls with the resulting process changes recorded

Quick wins

Quick win and how	Cost	Effort	Usual owner
Export the device list from your MDM and reconcile it against business-office purchase records Export devices from Google Admin (Devices > Chrome > Devices) or Intune (Devices > All devices) and ask the business office for technology purchase records covering the life of your current fleet. Match on serial number and work three lists: in both, purchased but not managed, and managed but not on any purchase record.	Free	Days	Technology director
Disable devices that haven't checked in for 90+ days, collect them, and deprovision only the ones you retire In Google Admin, filter Chrome devices by last sync older than 90 days and disable them, with a disabled-device message that gives your return instructions. Send each principal or media specialist a list for their building, and deprovision only devices you have in hand and are retiring.	Free	Days	Help desk
Start a one-page data inventory: every system with student PII, its owner, and its renewal date List the student information system (SIS), learning management system, Google or Microsoft tenant, special education, nutrition, transportation, assessment and HR/payroll systems, then scan the business office vendor payment list for subscriptions you missed. For each, record what data it holds, who administers it, the renewal date and whether a signed data privacy agreement is on file.	Free	Days	Technology director
Publish an approved-apps list and a simple request form for new tools Start the list from tools that already have signed agreements (check the SDPC registry), mark each as approved, approved with conditions or not approved, and post it where teachers look. Route a simple request form to curriculum and IT, and in Google Admin use Security > Access and data control > API controls to see and restrict which third-party apps can reach district accounts.	Free	Weeks	Curriculum and instruction lead
Record serials and locations for network gear, servers, and other non-1:1 hardware Pull model and serial lists from the firewall, switch and wireless management consoles, then walk each network closet and server room to photograph labels for anything not reported. Record location, firmware version, support contract and end-of-support date; E-Rate rules already require inventory records for Category Two equipment, so start from those.	Free	Days	Network and systems administrator

Free means staff time, existing licenses or free government services. Effort: hours, days or weeks.

Common pitfalls

- Treating the device management console as the whole inventory. Chromebooks appear there, but switches, door-access controllers, cameras, printers, cafeteria point-of-sale terminals and the finance server do not; reconcile the console against purchase records and a network discovery scan.
- Deprovisioning missing Chromebooks before they are found. A deprovisioned device leaves management and can be reset and used without your filtering or policies; disable it so it shows a return-to-district message, and deprovision only when it is retired.
- Running a one-time summer cleanup with no owner. Inventories drift within months as devices are swapped, repaired and moved between schools; name an owner and build the update into deployment, repair and collection steps.
- Counting only hardware. Much of a district's student data exposure sits in apps adopted with a district sign-in; review the third-party app access reports in Google Admin or Microsoft Entra and add what you find to the software and data inventories.
- Sending equipment to surplus, trade-in or lease return without proof of wiping. Copiers, old servers and staff laptops can hold student and payroll records; wipe or destroy the storage first and keep a certificate tied to each serial number.

Evidence that proves it

- MDM or admin-console device export (Google Admin, Intune, Jamf) dated within the last 90 days
- Asset inventory of record with serial numbers, assigned users, and locations
- Data inventory listing every system holding student or staff PII with a named owner
- Approved software list plus the app request and review workflow
- Service provider list with contract dates and signed data privacy agreements
- Certificates of destruction or wipe logs for retired devices
- Network diagram updated within the last year

Who usually owns it

Technology director	Owns the inventory of record for devices, network equipment, software and data systems, sets the update cycle and reports accuracy and end-of-support items to the superintendent.
Business and finance officer	Supplies purchase, surplus and contract records for reconciliation and makes sure disposal and trade-in paperwork includes proof of wiping.
Principals	Account for devices in their buildings at deployment and collection and report lost or stolen equipment to the help desk the same day.
Data privacy officer	Maintains the data inventory and classification and confirms that every system holding student data has a signed data privacy agreement.

Insurance relevance · High

Underwriters treat the inventory as the base for every other answer and ask directly whether any unsupported software or firmware is still in use. Some policies limit coverage for losses that start on end-of-life systems, so this area gets a close look.

- Do you keep a current inventory of all hardware and software connected to your network?
- Is any operating system, application or firmware in use no longer supported by its vendor, and if so, how is it isolated?
- How many workstations, servers and student devices does the district manage?
- Do you know where student and staff personal information is stored?

Tip: Pull device counts and the end-of-support list from your inventory of record before you answer, so the application matches what you could hand an adjuster after an incident.

Funding and free help

CISA K-12 cybersecurity resources and toolkit

Always available

Free federal guidance for K-12: the K-12 cybersecurity report and toolkit, plus access to regional CISA advisors and no-cost services. A resource, not funding.

Programs, eligibility and deadlines change; confirm on the official page before applying.

Learn more

- CIS Critical Security Controls Implementation Group 1 (CIS) <https://www.cisecurity.org/controls/implementation-groups/ig1>
- Cross-Sector Cybersecurity Performance Goals (CISA) <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>
- Student Data Privacy Consortium (SDPC) (Access 4 Learning Community) <https://privacy.a4l.org/>
- Protecting Student Privacy (U.S. Department of Education) <https://studentprivacy.ed.gov/>
- The K12 SIX Essentials Series (K12 SIX) <https://www.k12six.org/essentials-series>