

Data Security

This category asks whether student and staff data is protected wherever it sits, moves, or gets used - and whether you can actually restore it after an incident.

Why it matters

- Special education, health, discipline and counseling records are among the most sensitive information a district holds, and attackers have published stolen student records to pressure districts into paying, which harms students and families long after systems are restored.
- Backups that are complete, protected from deletion and tested are what let a district bring back the SIS, payroll and file shares after ransomware instead of rebuilding by hand during enrollment, report cards or state testing.
- Encrypted laptops and a clear map of where student data lives can turn a lost device into a hardware replacement rather than a possible privacy incident, and they make obligations under FERPA, state law and data privacy agreements easier to meet.

The stakes are concrete: FERPA education-record obligations and separate state-law or contractual breach-notification duties, attackers publishing special education and discipline records for extortion leverage, and multi-week outages when backups turn out to be incomplete or encrypted along with production systems.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	<p>Nobody can say with confidence where student and staff data lives, backups run but no one has tried a restore, and leadership sees data protection as an IT detail.</p> <p>Moving up: Get consistent: document how stored and transmitted data is managed and monitored so the process does not live in one person's head, and brief leadership until they can speak to data protection and risk in their own words.</p>	<ul style="list-style-type: none"> • No data inventory; sensitive spreadsheets sit in personal Drive or OneDrive folders shared by link • Backup jobs with unreviewed failures and no record of a test restore • Staff laptops without BitLocker or other full-disk encryption, and old drives sitting in a storage closet
2 · Repeatable	<p>Stored and shared data is handled consistently, backups run on a schedule and are checked, and formal procedures are being written. Leadership can explain the district's main data risks in plain terms.</p> <p>Moving up: Enforce routinely: apply protections per each system's risk classification, formally manage data records, review every non-encrypted system as a documented exception, and dedicate staff time to monitoring and investigating alerts.</p>	<ul style="list-style-type: none"> • Draft data handling procedure covering storage, sharing, transmission and disposal • Backup schedule covering SIS exports, the finance system and file servers, with success reports reviewed • Cabinet briefing notes on data protection risks and backup status
3 · Defined	<p>Protections are applied according to each system's risk classification, data records are formally managed, systems that cannot encrypt are documented exceptions, and a named technician reviews alerts every week.</p> <p>Moving up: Go beyond checkbox compliance: identify and analyze data risks on a routine cycle, use monitoring results to drive concrete improvements, and build staff depth in managing stored and transmitted data.</p>	<ul style="list-style-type: none"> • Data inventory with risk classification, owner and encryption status for each system • Exception register for systems that cannot encrypt, with compensating controls and review dates • Weekly alert and backup review log with follow-up tickets, plus a dated restore test showing recovery time
4 · Managed	<p>The district looks past minimum compliance to its own data risks, reviews them on a cycle, and uses monitoring and restore-test results to drive specific improvements. Technology staff are skilled at managing stored and transmitted data.</p> <p>Moving up: Adopt stronger tooling and ownership: integrity checking, DLP tuned to your environment, controls that adapt as systems change, and technology staff who proactively hunt for data risks instead of waiting on findings.</p>	<ul style="list-style-type: none"> • Annual data risk review covering items such as bulk SIS exports, third-party integrations and external sharing, with actions tracked • Board or committee report on backup test results and material data risks • Professional development records for technology staff on data protection tools

Level	What you would see	Artifacts that show it
5 · Optimized	Advanced tooling gives visibility into data exposure, integrity checks protect critical systems, controls adapt as systems change, and staff look for data risk before an auditor or attacker finds it.	<ul style="list-style-type: none"> • Data loss prevention (DLP) rules tuned to catch student identifiers leaving the district, with alerts reviewed • Integrity monitoring or automated backup verification for SIS and finance data • Staff-initiated findings logged and fixed, such as an over-shared folder corrected before anyone reported it

Quick wins

Quick win and how	Cost	Effort	Usual owner
Change Drive/OneDrive sharing defaults to internal-only with exceptions by request In the Google Admin console (Apps, Google Workspace, Drive and Docs, Sharing settings) or the SharePoint admin center sharing policies, turn off sharing outside the district or limit it to trusted domains, and create an exception group for staff who truly need it. Announce the change a week ahead and give teachers a simple request form.	Free	Days	Network and systems administrator
Run a timed test restore of one critical system this quarter Pick one system, such as a file server, the finance database or a copy of the SIS export, restore it to an isolated location, and record the start time, finish time and anything missing. For a hosted SIS, ask the vendor to show its latest restore test or walk through one with you.	Free	Days	Network and systems administrator
Enforce BitLocker on staff Windows laptops with escrowed keys Create an Intune disk encryption policy or a Group Policy object that requires BitLocker and saves recovery keys to Entra ID or Active Directory, then check the encryption report for devices that did not comply. Confirm the help desk can look up a recovery key before rollout so a locked-out teacher is not stuck.	Free	Days	Network and systems administrator
Write the one-page inventory of your top sensitive-data systems List each system that holds student or staff personal data (SIS, special education, health, meal eligibility, HR and payroll, counseling, assessment platforms) with its owner, where it is hosted, what it holds and how it is backed up. Start with the most sensitive systems and fill in the rest over time.	Free	Hours	Data privacy officer
Wipe or shred drives in surplus equipment and file the certificate Pull drives from surplus computers and returning lease copiers before pickup, then wipe them following NIST SP 800-88 media sanitization guidance or have a vendor shred them. File the certificate of destruction with the board's surplus approval.	Low cost	Days	Technology director

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

Common pitfalls

- Treating the cloud recycle bin as a backup. Deleted-item retention and version history have time limits and can be emptied by an attacker with admin rights, so back up Google Workspace or Microsoft 365 data you cannot afford to lose with a separate service.
- Keeping the backup reachable from the network it protects. A backup server joined to the domain with the same admin credentials can be encrypted along with everything else; keep one copy offline or immutable with separate credentials.
- Never testing a restore until the day it counts. Missing databases, lost encryption passwords and unrealistic restore times only show up in a test, so run one each quarter and write down how long it took.
- Letting bulk student data leave through exports and spreadsheets. Full SIS exports emailed to vendors or saved to personal drives fall outside every control; limit export rights and use the vendor's secure transfer or rostering integration instead.
- Forgetting copier and printer hard drives at lease end. Multifunction copiers can store images of scanned individualized education programs (IEPs), report cards and payroll forms, so require drive wiping or drive retention in every copier lease.

Evidence that proves it

- Data inventory listing systems that hold student and staff PII, with owners
- Backup job success reports plus a dated test-restore log with recovery time
- Device encryption compliance report from Intune or the Google admin console
- Drive/OneDrive external sharing configuration export or screenshot
- Certificates of destruction for retired drives and copiers
- Documented non-encryption exceptions with review dates

Who usually owns it

Technology director

Maintains the data inventory, backup design and restore testing, and approves documented exceptions for systems that cannot encrypt.

Data privacy officer

Classifies sensitive data and keeps sharing, exports and vendor handling consistent with FERPA, state law and data privacy agreements.

Network and systems administrator

Runs backups, encryption policies and sharing settings, and reviews security and backup alerts every week.

Superintendent

Brings data protection status and backup test results to the board and funds gaps such as an offline or immutable backup copy.

Insurance relevance · High

Underwriters treat backups as a deciding factor in ransomware exposure and ask about backup scope, offline or immutable copies and restore testing, along with encryption and how well you know where sensitive records are kept.

- Are critical systems, including the SIS and business office systems, backed up automatically on a regular schedule?
- Is at least one backup copy offline or immutable so an attacker cannot delete or encrypt it?
- When did you last restore a critical system from backup, and is the result documented?
- Are laptops and portable devices encrypted, and do you know where student and staff personal data is stored?

Tip: Answer backup questions from the backup console's immutability settings and your dated restore-test log, and confirm in writing what your hosted SIS and finance vendors back up before you claim those systems are covered.

Funding and free help

AWS K12 Cyber Grant Program

Unclear · last published deadline was 31 Jan 2024

A \$20M pool of AWS promotional credits announced in 2023 for cloud-based security and resilience projects at districts and education agencies. Awards are credits, not cash.

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

- #StopRansomware Guide (CISA) <https://www.cisa.gov/resources-tools/resources/stopransomware-guide>
- Protecting Student Privacy (U.S. Department of Education) <https://studentprivacy.ed.gov/>
- Student Data Privacy Consortium (SDPC) (Access 4 Learning Community) <https://privacy.a4l.org/>
- CIS Critical Security Controls Implementation Group 1 (CIS) <https://www.cisecurity.org/controls/implementation-groups/ig1>