USERAUTHGUARD

BLOG COMPLIANCE

FERPA Compliance and Device Management: What Schools Get Wrong

Stef Verleysen | April 08, 2026

> Discover the most common FERPA compliance mistakes schools make with device management, from inadequate data deletion to third-party app sharing, and learn how proper tools help maintain compliance.

Ask most school administrators whether their district is FERPA compliant, and you will get a confident yes. Ask them how student data is handled on shared Chromebooks after a student transfers, or what happens to locally cached data when a device is reassigned, or whether every third-party app on their managed devices has a signed data privacy agreement, and the confidence often evaporates.

FERPA compliance device management is one of those areas where schools think they are doing fine because they have not been caught yet. The Family Educational Rights and Privacy Act has been law since 1974, but its application to modern device management creates compliance challenges that most districts are not fully addressing. The **Student Privacy Policy Office at the U.S. Department of Education** has published extensive guidance specifically addressing digital devices and online services in K-12 settings. And with increasing scrutiny from state attorneys general, parent advocacy groups, and the federal Student Privacy Policy Office, the margin for error is shrinking.

This guide examines the intersection of FERPA requirements and school device management, identifies the most common violations schools do not realize they are making, and provides practical steps to close the gaps.

What FERPA Requires Regarding Student Data on Devices

FERPA protects the privacy of student education records. The law applies to all schools that receive funding from the U.S. Department of Education, which includes virtually every public K-12 district and most private schools that accept federal financial assistance.

In the context of device management, FERPA's requirements boil down to several key principles:

- **Access control:** Only school officials with a legitimate educational interest may access student education records. This includes data stored on, accessed through, or transmitted by school-managed devices.
- **Consent and disclosure:** Student data cannot be disclosed to third parties without prior written parental consent, with certain limited exceptions (directory information, health and safety emergencies, school officials with legitimate educational interest).
- **Record accuracy and access:** Parents have the right to inspect their child's education records and request corrections. This extends to digital records stored in device management systems.
- **Data security:** While FERPA does not prescribe specific security measures, the Department of Education has made clear that schools must use "reasonable methods" to ensure that only authorized individuals access student records. Failing to secure devices that contain student data constitutes a violation.

Common FERPA Violations Schools Do Not Realize They Are Making

Most FERPA violations in device management are not the result of malicious intent. They stem from processes that were never designed with data privacy in mind, or from informal practices that have grown up around the edges of formal policy.

1. Shared Devices with Residual Student Data

In many schools, Chromebooks are shared between students across classes or across school years. When Student A logs out and Student B logs in, is Student A's data truly gone from the device? In many configurations, the answer is no.

Chrome OS caches user data locally for performance. Depending on your device policy settings, this cached data may persist after logout. If Student B accesses the device and encounters Student A's browsing history, cached documents, or saved credentials, that is a disclosure of education records to an unauthorized individual, which is a FERPA violation.

The fix: Configure your Chromebook management policies to wipe local user data on sign-out. In Google Admin, navigate to Device Management, Chrome, Settings, and enable "Erase all local user data" under the Sign-in Settings section. This adds a few seconds to each login but eliminates the risk of data persistence between users.

2. Inadequate Data Deletion When Students Leave

When a student transfers to another district or graduates, what happens to their data? Most districts deactivate the student's Google Workspace account, but deactivation is not deletion. The account and all associated data (Drive files, email, Classroom submissions, Chrome browsing data) persist in your domain until explicitly deleted.

More concerning, the student's data may persist on physical devices that were assigned to them. If a Chromebook is reassigned to a new student without proper deprovisioning, the previous student's data may still be recoverable from the device's local storage.

The fix: Establish a formal data retention and deletion policy that covers both cloud data (Google Workspace accounts) and device data (local storage). When a student leaves, delete their account data after a defined retention period (check your state's records retention requirements) and wipe any device that was assigned to them before reassigning it.

3. Third-Party App Data Sharing Without Agreements

Every Chrome extension and web application that students use on their school Chromebooks potentially collects student data. Under FERPA, schools are responsible for ensuring that any third party that receives student data has agreed to use it only for the purposes for which disclosure was made, and to protect it in accordance with FERPA requirements.

In practice, many districts have dozens or hundreds of Chrome extensions and web apps in use across their schools, and a significant portion of them have no signed data privacy agreement. Teachers install educational apps, students access web-based tools recommended by peers, and browser extensions accumulate over time with no formal review process.

The fix: Implement a formal app vetting process. Use the Chrome Web Store allowlist in Google Admin to control which extensions and apps can be installed on managed Chromebooks. Require a signed Student Data Privacy Agreement (SDPA) or equivalent for every approved app. Organizations like the Student Data Privacy Consortium provide templates and a national registry of signed agreements. Review your **extension privacy practices** regularly to ensure compliance.

4. Overly Broad Access to Device Management Systems

Who has access to your device management system? In many districts, the answer is "everyone in IT." But device management systems contain student data: device assignment records link specific devices to specific students, repair notes may contain information about student behavior, and usage logs reveal individual browsing and activity patterns.

Under FERPA, access to this data must be limited to school officials with a legitimate educational interest. A network administrator who needs access to configure switches does not need to see which student is assigned to which Chromebook.

The fix: Implement role-based access in your device management system. IT staff who manage infrastructure should have a different access level than IT staff who manage student devices. Repair technicians need access to device information but not necessarily to student identity information. Audit access logs regularly to identify and correct over-provisioned access.

5. Unencrypted Device Data in Transit

When Chromebooks are sent to third-party repair vendors, the devices may contain locally cached student data. If the repair vendor is not a FERPA-compliant partner with a signed agreement, sending them a device with student data on it constitutes an unauthorized disclosure.

The fix: Wipe devices before sending them to external repair vendors unless the vendor has signed a FERPA-compliant agreement. For in-district repairs, ensure that repair technicians understand their obligations regarding student data on devices they service. If a device cannot be wiped before repair (because it will not power on, for example), document the situation and ensure the repair vendor's agreement covers data handling for unwiped devices.

6. Insufficient Audit Trails

FERPA requires that schools maintain a record of each request for access to and each disclosure of personally identifiable information from student education records. In the context of device management, this means you need to know who accessed what student data, when, and why.

Many device management systems and Google Admin consoles do maintain access logs, but few districts actively review them. Without regular audit review, unauthorized access can continue undetected for months or years.

The fix: Enable and regularly review audit logs in your device management system and Google Admin console. Establish a quarterly review cadence where a designated staff member examines access logs for anomalies: unusual access patterns, access by staff who should not have it, or bulk data exports that were not authorized.

How Device Management Intersects with Student Privacy

The relationship between device management and student privacy is bidirectional. Proper device management is essential for maintaining FERPA compliance, and FERPA requirements should inform how you configure and use your device management tools.

Device Assignment Records Are Education Records

A record that links a specific device (with its serial number, usage history, and location data) to a specific student is an education record under FERPA. This means device assignment databases, check-out logs, and repair records that identify students by name or ID are protected data that must be handled accordingly.

Monitoring Data Is Sensitive

If you use screen monitoring, keyword alerts, or browsing history tools on student Chromebooks, the data generated by these tools is education record data. It reveals information about individual students' online behavior, academic activity, and potentially their physical and mental health. This data must be protected, access-controlled, and retained according to your data governance policies.

Deprovisioning Is a Privacy Event

When a device is reassigned, decommissioned, or sent for repair, the handling of any student data on that device is a privacy-relevant action. Your deprovisioning procedures should include explicit steps for data handling at every stage of the device lifecycle.

Data Minimization Practices

One of the most effective strategies for reducing FERPA risk is to minimize the amount of student data you collect and retain in the first place. You cannot have a breach of data you never collected.

- **Collect only what you need.** If your device management system asks for student home address, phone number, or social security number, ask whether you genuinely need that data for device management purposes. In most cases, a student ID number and school assignment are sufficient.
- **Retain only as long as necessary.** Establish retention schedules for device management data. Browsing logs older than 90 days are rarely useful for operational purposes. Assignment histories for graduated students should be archived and eventually deleted according to your records retention policy.
- **Anonymize where possible.** If you are generating reports on device damage rates by grade level or building, you do not need individual student names in the report. Use aggregated, anonymized data for analytics and reserve identified data for operational needs.

COPPA Considerations for Younger Students

For students under 13, the **Children's Online Privacy Protection Act (COPPA)** adds another layer of compliance requirements. COPPA, enforced by the FTC, regulates the collection of personal information from children under 13 by websites and online services.

When a school provides a Chromebook to an elementary student and directs them to use online services, the school is effectively consenting to data collection on behalf of the child's parents. This is permissible under COPPA, but only when:

- The service is used for an educational purpose.
- The school has reviewed the service's privacy practices and determined they are appropriate.
- The school does not allow the service to use the collected data for commercial purposes.

In practice, this means your app vetting process for devices used by students under 13 needs to be even more rigorous than for older students. Review each app's COPPA compliance statement and ensure it is documented in your records.

Proper Device Deprovisioning and Data Wiping

Deprovisioning is where compliance rubber meets the road. Every device transition, whether from student to student, school to school, or active service to retirement, requires deliberate data handling.

Standard Deprovisioning Workflow

1. **Unassign the device** from the current user in your management system.
2. **Powerwash the device** to remove all local user data. A powerwash resets Chrome OS to factory settings and removes all local accounts, cached data, and downloaded files.
3. **Verify the wipe.** Boot the device after powerwash and confirm it presents the enrollment or login screen with no residual user data.
4. **Update the management system** to reflect the device's new status (available, in repair, retired).
5. **For retired devices:** Perform a full device wipe (not just powerwash) and deprovision the device from Google Admin before disposal or recycling.

Handling Devices That Cannot Be Wiped

Sometimes a device is too damaged to powerwash normally (will not boot, screen is destroyed). In these cases:

- Document the device's condition and the reason it cannot be wiped.

- If the device will be sent for repair, ensure the repair vendor has a signed data handling agreement.
- If the device will be recycled or disposed of, ensure the disposal vendor provides a certificate of data destruction.
- Update your records to reflect the data handling disposition for audit purposes.

Audit Trails and Documentation Requirements

FERPA compliance is not just about doing the right thing. It is about being able to prove you did the right thing. Documentation is your defense in the event of a complaint, audit, or legal action.

What to Document

- **Device assignment history:** Who was assigned which device, when, and by whom.
- **Deprovisioning records:** When devices were wiped, by whom, and what method was used.
- **Access logs:** Who accessed the device management system, what data they viewed or modified, and when.
- **Third-party agreements:** Signed data privacy agreements for every vendor, app, and extension that handles student data.
- **Training records:** Documentation that staff received FERPA training and when.
- **Incident records:** Any data breach or unauthorized access incidents, including your investigation and remediation actions.

UserAuthGuard's **compliance reporting tools** automatically maintain audit trails for device assignments, status changes, and user actions within the system, reducing the manual documentation burden on IT staff.

Training Staff on FERPA Compliance with Devices

Technical controls are only as strong as the people using them. Staff training is a non-negotiable component of FERPA compliance.

Who Needs Training

- **IT staff:** Comprehensive training on FERPA requirements as they relate to device management, data handling, and system configuration. This is your most critical audience.
- **Teachers:** Awareness training on what constitutes student data, how to handle it on devices, and when to report potential issues.

- **Administrators:** Understanding of their responsibilities as school officials with access to education records, and their role in ensuring building-level compliance.
- **Repair technicians:** Specific training on handling student data on devices being serviced, including proper deprovisioning procedures and data confidentiality obligations.

Training Content

- What FERPA is and why it matters.
- What constitutes an education record in the context of devices (hint: more than most people think).
- Who is authorized to access student data and under what circumstances.
- How to handle devices during assignment, reassignment, repair, and disposal.
- What to do if you suspect an unauthorized disclosure or data breach.
- How your district's specific policies and tools implement FERPA requirements.

Train annually at minimum, and provide refresher training whenever significant changes are made to your device management procedures or policies.

How Proper Device Management Tools Help Maintain Compliance

The right device management platform does not just make IT operations more efficient. It makes FERPA compliance structurally embedded in your daily workflows rather than a separate compliance exercise layered on top.

- **Role-based access** ensures that only authorized personnel can view student-device associations.
- **Automated audit trails** document every device assignment, transfer, and status change without requiring manual logging.
- **Standardized deprovisioning workflows** ensure that data handling steps are not skipped when devices change hands.
- **Centralized records** provide a single source of truth for device history, eliminating the risk of uncontrolled spreadsheets containing student data scattered across the district.
- **Compliance reporting** generates the documentation you need for audits, board presentations, and incident response without hours of manual compilation.

Take Control of Your FERPA Compliance

FERPA compliance is not a one-time project. It is an ongoing practice that requires the right policies, the right training, and the right tools. UserAuthGuard provides the device management foundation that makes compliance manageable, with **built-in compliance reporting**, role-based access controls, automated audit trails, and **extension privacy management** designed specifically for K-12 environments.

Request a demo to see how UserAuthGuard can help your district close FERPA compliance gaps and build a device management program that protects student privacy by design.