



Education Endpoint Compliance Checklist (FERPA & COPPA)

Practical checklist for aligning K-12 and higher-ed endpoints with FERPA and COPPA using Codeproof UEM.

Note: FERPA and COPPA compliance requires district/institution policies, parental/guardian notices and consents (as applicable), and vendor management. Codeproof provides endpoint and application safeguards that support these programs.

1) Data Access & Authentication (FERPA)

- Require unique accounts for staff and students; apply least-privilege access to student records.
- Enforce device passcodes/biometrics and session lock/idle timeout on shared and 1:1 devices.
- Integrate MFA for staff and privileged roles where feasible.

2) Privacy Notices & Parental Rights (FERPA/COPPA)

- Coordinate parental/guardian notices and obtain consent for online services collecting personal information (COPPA).
- Publish directory information policies and opt-out processes (FERPA).
- Maintain records of disclosures of student education records.

3) Device & App Controls

- Enforce device encryption across Windows, macOS, iOS, and Android endpoints.
- Allowlist district-approved apps; block unapproved/risky apps and third-party stores.
- Use managed configurations to restrict data sharing (copy/paste, AirDrop/Nearby Share, unmanaged apps).

4) Student Data Minimization

- Use per-app VPN and app-level restrictions so only approved apps can reach protected services.
- Separate school data from personal data on BYOD with Work Profile / User Enrollment.
- Limit local storage of student records; prefer secure, centralized systems.

5) Monitoring, Audit & Reporting

- Log device compliance, app installs, configuration changes, and remote actions.
- Export device inventory and compliance reports for audits/board reporting.
- Retain logs according to district/institution policy and state retention schedules.

6) Content & Feature Restrictions (Age-Appropriate/COPPA)

- Apply web/content filters and safe-search controls in cooperation with district tools.
- Restrict cameras, screen capture, Bluetooth/AirDrop, or location sharing in sensitive contexts as policy requires.
- Disable ad tracking/ID where platform supports it; restrict background data collection.

7) Incident Response & Breach Handling

- Enable remote lock, Lost Mode, and selective/full wipe for lost or stolen devices.
- Revoke credentials, certificates, and access tokens immediately.
- Document incidents with activity logs and prepare parent/guardian notifications where required by policy/law.

8) Vendor & Third-Party Management

- Maintain a list of approved educational apps and services with data processing terms.
- Ensure student data handling meets FERPA/COPPA requirements; track DPIAs where applicable.
- Remove access and selectively wipe data when contracts end or apps are decommissioned.

Copyright © Codeproof Technologies Inc. — This checklist supports FERPA/COPPA alignment on endpoints using Codeproof controls. It is not legal advice.
