// FREE SCHOOL RESOURCE

Student Data Privacy and Education Apps Toolkit

FERPA, COPPA, app approval, contract review, retention, deletion and family communication

// WHAT THIS TOOLKIT PROVIDES

- Plain-language FERPA and COPPA basics for school leaders, staff and app reviewers.
- An app-request workflow, educational-purpose test and vendor due-diligence questions.
- Terms-of-service, contract, advertising, tracking, retention, deletion and security checklists.
- Breach response, parent communication, approved-app inventory and state-law addendum.
- References limited to official U.S. federal and state government sources.

// FOR SCHOOL BOARDS, SUPERINTENDENTS, IT, PRIVACY, PROCUREMENT, CURRICULUM, TEACHERS, RECORDS STAFF AND FAMILIES

// START HERE

How to use this toolkit

A practical privacy and app-vetting resource

Every classroom app is also a data decision.

The U.S. Department of Education warns that online applications can introduce security and privacy vulnerabilities and advises teachers to consult district administration and IT before use. [4]

Use this toolkit as a single approval route

01 **Request.** The educator identifies the educational purpose, users, ages, data and required integrations.

02 **Triage.** Privacy / IT determines whether the service collects student PII, creates education records, serves children under 13 or connects to district systems.

03 **Review.** Evaluate FERPA, COPPA, state law, terms, security, accessibility, advertising, retention, deletion and breach obligations.

04 **Decide.** Approve, approve with conditions, pilot, reject or require a contract.

05 **Publish and monitor.** Add approved apps to a public or staff inventory, train users, review changes and retire tools cleanly.

Small-school approach

Use one form, one named reviewer and a documented escalation route. A simple consistent process is safer than informal teacher-by-teacher sign-up.

Important

This toolkit is not legal advice. FERPA, COPPA, PPRA and state student-data laws apply differently depending on the school, service, age, data, purpose and contract.

// VERSION CONTROL

District / school: _____

Privacy owner: _____

Approved by: _____

Effective date: _____

Next review: _____

// FERPA BASICS

Education records and third-party services

Identify the data, authority, control and records rights

FERPA in plain language

FERPA applies to educational agencies and institutions that receive funds under programs administered by the U.S. Department of Education. It protects education records and gives parents, and later eligible students, rights to inspect, review and seek amendment. [1][2]

Disclosure of personally identifiable information from education records generally requires consent unless a FERPA exception applies.

Under the school-official exception, a contractor may perform a service the school would otherwise use its own employees for, but the contractor must be under the school's direct control for the use and maintenance of the PII and may not use or redisclose it for unauthorized purposes. [3][4]

FERPA questions for an app

Will the app receive PII from education records or create records maintained for the school?

What is the legitimate educational interest and institutional function?

How does the school exercise direct control through contract, configuration and practice?

Can the vendor use, redisclose, sell, profile or train models on the data?

How can parents / eligible students access and correct applicable records?

What happens to records when the user, class or contract ends?

// FERPA IS NOT A PRODUCT CERTIFICATION

Do not rely on: A vendor statement that it is "FERPA compliant," a privacy badge, a free account, a teacher click-through agreement or the fact that another district uses the service.

Do require: A school-specific analysis of purpose, data, authority, direct control, terms, safeguards, records rights, state law and actual configuration.

// FERPA SCREEN

QUESTION	ANSWER / EVIDENCE	OWNER
What education record or PII is disclosed or created?		
What consent or FERPA exception is relied upon?		
How is the provider under direct control?		
How are access, correction, redisclosure and deletion handled?		

// COPPA BASICS

Children under 13 and school consent

School consent is limited to the educational context

COPPA primarily regulates operators, but schools have an important gatekeeping role.

COPPA baseline

COPPA applies to operators of child-directed websites and online services that collect personal information from children under 13, and general-audience services with actual knowledge that they are collecting from a child under 13. [5]

Covered operators must provide notice, obtain verifiable parental consent subject to limited exceptions, provide parent access/deletion rights, use reasonable security, minimize collection and limit retention.

The FTC amended the COPPA Rule in 2025, including separate consent for certain third-party advertising disclosures, retention limits and expanded personal-information definitions. [6]

When a school may consent

A school may act as the parent's agent when personal information is collected for the use and benefit of the school and for no other commercial purpose.

The school cannot consent on behalf of the parent when the provider uses student information for unrelated commercial purposes, including behavioral advertising or commercial profiles.

The school should understand collection, use, disclosure, parent review/deletion, security and retention before authorizing the service. [5]

// COPPA QUESTIONS

QUESTION	APPROVAL STANDARD	EVIDENCE
Is the service directed to children, or will children under 13 use it?	Age and audience analysis documented.	
What personal information is collected?	Only reasonably necessary data for the educational activity.	
Is use limited to a school-authorized educational purpose?	No unrelated commercial use, advertising or profiling.	
Can the school / parent review and delete information?	Practical process and responsible contact identified.	
How long is data retained?	Specific purpose-based period; no indefinite retention.	

// DATA MAPPING

Know what the app collects and creates

Privacy review starts with the actual data flow

Classify the data

PUBLIC Approved public information with no restricted student data.

INTERNAL Routine district information not intended for public release.

SENSITIVE Student identifiers, grades, attendance, behavior, communications, device or usage data.

HIGHLY SENSITIVE Health, disability, counseling, discipline, biometrics, precise location, credentials, safety or exploitation information.

Map the data life cycle

Collect: Who provides the data and is each field necessary?

Use: What exact educational function is performed?

Store: Where, for how long, under whose account and encryption?

Share: Which subprocessors, integrations or public features receive it?

Generate: What scores, profiles, inferences, transcripts or AI output are created?

Delete: How is data removed from production, backups and subprocessors?

// MINIMUM NECESSARY DATA MAP

DATA ELEMENT	SOURCE	PURPOSE	WHO CAN ACCESS	RETENTION	DELETE / EXPORT

Data minimization test: If a field is not necessary for the approved educational purpose, do not collect or share it.

// APPROVAL WORKFLOW

From request to monitored use

A consistent process for every school and classroom

One route for every app.

Teachers should not have to become privacy lawyers, but they should know that unapproved click-through use is not the approval process.

1. Request. Educational purpose, grade, users, cost, account type, data and start date.

2. Quick screen. Student login? Under 13? PII? AI? Ads? Payment? Integration? Sensitive use?

3. Educational review. Standards alignment, evidence, accessibility, age suitability and alternatives.

4. Privacy / legal review. FERPA, COPPA, PPRA, state law, notice, consent and records status.

5. Security review. Authentication, encryption, incident history, logging, subprocessors and configuration.

6. Terms / contract. Data ownership, purpose limits, advertising, retention, deletion, breach and audit.

7. Decision. Approve, conditional approval, limited pilot, reject or request changes.

8. Publish and monitor. Approved-app list, owner, review date, changes, complaints and retirement.

// DECISION LEVELS

LEVEL	EXAMPLE	REVIEW	DECISION AUTHORITY
LOW	No login, no student data, staff-only content reference.	Educational and basic security check.	
MODERATE	Student accounts, assignments, usage analytics or classroom communication.	Full privacy, security, accessibility and terms review.	
HIGH	Grades, IEP/504, health, biometrics, monitoring, AI profiling, safety or district integration.	Contract, counsel/privacy review, impact assessment, pilot and leadership approval.	
REJECT	Targeted ads, sale, unrelated profiling, no deletion, no meaningful security or unacceptable terms.	Do not deploy.	

// REQUEST FORM

Education app approval request

Capture the purpose, users, data and integrations

Education app request

Requester / school / role: _____

App / provider / website: _____

Requested start and duration: _____ Cost / funding: _____

Grade(s), subject and number of users:

_____

Educational purpose and expected benefit:

_____

_____

Why approved tools do not meet the need:

_____

Account method: no login | student login | SSO | teacher roster

Data entered or collected:

_____

_____

Integrations / permissions requested:

_____

Requester confirms

- ☐ I have not asked students to create accounts.
- ☐ I provided current privacy policy and terms links.
- ☐ I identified any AI, advertising, chat, social or public-sharing feature.
- ☐ I will follow approval conditions and report material changes.

Review routing

Curriculum: _____

Privacy / records: _____

IT / security: _____

Accessibility: _____

Procurement / legal: _____

Do not begin a free trial with real student data while review is pending. Use vendor demonstrations, fictional data or an approved sandbox.

// DUE DILIGENCE

Questions before approving an app

Understand the educational value, data and business model

Educational purpose

What specific need does the app meet?

Is there evidence it is effective for the age, subject and intended use?

Can the same goal be met with less data or an approved tool?

Does the app require student social interaction, public posting or direct messaging?

Data and rights

What PII, content, usage, device, location, audio, video or biometric data is collected?

What profiles, scores or inferences are generated?

Can parents / eligible students access and correct applicable records?

Can the district export and delete all data?

Business model

Is there advertising, product promotion, tracking, sale, licensing or commercial profiling?

Does the provider use data to train AI or improve products beyond the contracted service?

Who are the subprocessors and can they change without notice?

What happens if the free product becomes paid?

Security and safety

How are accounts authenticated and disabled?

Is data encrypted in transit and at rest?

What security testing, logging and incident response exist?

Can users contact strangers, share publicly, upload harmful content or bypass school controls?

// STOP SIGNS

STOP OR ESCALATE WHEN	WHY
The terms allow unilateral material changes without meaningful notice.	The school cannot maintain informed approval.
The vendor claims broad ownership or license rights over student content.	Conflicts may arise with school control, student rights and state contract law.
Student data supports targeted advertising, unrelated profiling or sale.	May conflict with COPPA, PPRA, state law and district policy.
Deletion is unavailable, undefined or excludes subprocessors / backups.	The district cannot close the data life cycle.
The service requires a personal account or age misrepresentation.	Creates consent, terms and account-control risks.

// TERMS OF SERVICE

Checklist for click-through and contracts

Do not confuse acceptance of terms with district approval

Read the actual Terms of Service and Privacy Policy.

The Department of Education's Model Terms of Service resource is a framework for evaluating how an app collects, uses and transmits information. [7]

Acceptable terms should state

- ☐ Clear contracting entity, service and governing documents.
- ☐ School / student ownership or control of records and content.
- ☐ Use limited to the approved educational purpose.
- ☐ No sale, targeted advertising or unrelated commercial profiling.
- ☐ Defined security, subprocessor and incident obligations.
- ☐ Access, correction, export, retention and deletion procedures.
- ☐ Notice and approval for material changes.

Warning language

"We may use any content for any purpose."

"We may sell or share information with partners."

"Continued use means acceptance" with no school notice.

"Data may be retained as long as useful" or after account deletion.

Broad disclaimers with no security commitment or breach process.

Mandatory arbitration, indemnity or venue terms the school cannot accept.

A consumer privacy policy that does not address school use.

// TERMS REVIEW RECORD

DOCUMENT / VERSION / DATE	KEY TERM	RISK / REQUIRED CHANGE	REVIEWER

Protective vendor terms

Turn privacy promises into enforceable obligations

Minimum contract clauses

Purpose and instructions: Use data only to provide the specified service.

Ownership and control: School records remain under school control; student content rights are defined.

Confidentiality: Authorized access, workforce training and no unauthorized redisclosure.

Security: Reasonable safeguards, encryption, authentication, logging, vulnerability management and secure development.

Subprocessors: List, equivalent obligations and advance notice of changes.

Incident notice: Prompt notice, required facts, cooperation, preservation and cost responsibilities.

Data life-cycle clauses

Access and correction: Support FERPA and state-law rights.

Retention: Specific periods tied to the educational purpose.

Deletion: Production, backups and subprocessors; written certification.

Export and transition: Usable format before termination.

Advertising and profiling: No targeted advertising, sale or unrelated profile.

AI training: No use of student data, prompts or output to train shared/public models unless expressly authorized and lawful.

Audit / evidence: Right to receive compliance and security information.

// CONTRACT GAP TRACKER

CLAUSE	VENDOR LANGUAGE	REQUIRED DISTRICT LANGUAGE	STATUS
Purpose / use limits			
Security / incident notice			
Retention / deletion			
Ads / profiling / AI training			
Subprocessors / changes			

// RETENTION

Data retention and secure deletion

Close the data life cycle deliberately

Keep data only as long as the approved purpose and applicable records rules require.

Indefinite retention increases breach impact, access complexity and vendor dependence. The FTC's amended COPPA Rule expressly limits covered operators to purpose-based retention. [5][6]

Retention schedule fields

Data category and system of record.

Educational / legal purpose.

Start event and retention period.

Authority: records schedule, contract or policy.

Production deletion method.

Backup / subprocessor deletion timing.

Export and legal-hold exception.

Owner and verification evidence.

Deletion triggers

Student leaves class, school or district.

Teacher or employee account is disabled.

Pilot ends or tool is rejected.

Contract expires or is terminated.

Purpose changes or data is no longer necessary.

Parent / eligible-student request where applicable.

Vendor or subprocessor is replaced.

Incident response requires preservation before later deletion.

// RETENTION AND DELETION SCHEDULE

DATA / APP	PURPOSE / AUTHORITY	RETENTION	DELETE FROM	OWNER / EVIDENCE

Do not promise immediate deletion if law or a legal hold requires retention. State who decides and how affected families are informed.

// COMMERCIAL USE

Advertising, tracking, profiling and AI training

School-authorized education data is not a marketing asset

Reject or restrict

Targeted advertising based on student activity or persistent identifiers.

Sale, licensing or unrelated disclosure of student information.

Commercial profiles of students or families beyond the school service.

Cross-site tracking, third-party pixels or ad networks not integral to the educational service.

Use of prompts, content, voice, images or behavior to train public/shared AI models without express lawful approval.

Collection of biometrics, precise location or contacts without a documented necessity and legal review.

Require transparency

List every category of data and each purpose.

Identify advertising, analytics, AI, personalization and recommendation functions.

Identify subprocessors and data-sharing categories.

Explain whether data is combined across services or accounts.

Provide school controls to disable nonessential collection.

State how parents / eligible students can exercise applicable rights.

// TRACKING AND COMMERCIAL-USE CHECK

FEATURE	YES / NO / UNKNOWN	APPROVAL CONDITION / EVIDENCE
Targeted or behavioral advertising		
Third-party advertising or analytics SDKs		
Commercial profiles or data brokerage		
AI model training or product improvement		
Biometric, voiceprint or face analysis		
Precise location, contacts or social graph		

COPPA and schools. The FTC states a school cannot consent on behalf of parents when a provider uses student information for unrelated commercial purposes such as behavioral advertising or commercial profiles. [5]

// SECURITY

Minimum security review for education apps

Match evidence and controls to the data and consequence

Account and access

- [ ] District-managed SSO or approved account method.
- [ ] MFA for staff / administrators where available.
- [ ] Role-based access and least privilege.
- [ ] Automated or prompt account disablement.
- [ ] Administrative audit logs.

Data protection

- [ ] Encryption in transit and at rest.
- [ ] Secure backups and tested recovery.
- [ ] Tenant separation and no public-by-default sharing.
- [ ] Secure deletion and export.
- [ ] Configuration documentation.

Vendor security evidence

Security contact and incident process.

Independent assessment or assurance report appropriate to risk.

Vulnerability management and patching.

Penetration testing and secure development.

Subprocessor oversight and staff training.

School-side controls

Approved integrations only.

Minimal roster attributes.

Staff cannot make classes public by default.

Review sharing links and external messaging.

Monitor admin alerts and vendor change notices.

// SECURITY REVIEW RECORD

CONTROL / EVIDENCE	FINDING	RISK / CONDITION	OWNER / DUE

// BREACH RESPONSE

Vendor breach and notification workflow

Coordinate facts, containment, law and communication

A vendor breach is a school incident too.

Use the district incident-response plan. Preserve evidence, determine affected data and people, coordinate with the vendor and counsel, and meet federal, state, contract and insurance requirements.

First actions

01 Record the notice, source, time, affected service and known facts.

02 Activate IT, privacy, leadership, legal, communications and student-support roles.

03 Contain access: disable integration, reset credentials or suspend use when appropriate.

04 Preserve logs, notices, contracts, configurations and communications.

05 Determine data categories, individuals, dates, cause, access, acquisition and ongoing risk.

Vendor information to demand

Discovery and containment timeline.

Affected products, tenants, accounts and subprocessors.

Data elements and number of affected individuals.

Whether data was accessed, acquired, altered or published.

Indicators, logs and recommended school actions.

Law-enforcement, regulator and insurance coordination.

Root cause, corrective action and deletion / recovery status.

// NOTIFICATION DECISION LOG

REQUIREMENT / AUDIENCE	DEADLINE / TRIGGER	DECISION / COUNSEL	STATUS
Parents / eligible students			
State education / privacy authority			
State attorney general / consumer authority			
Law enforcement / CISA / insurer			

New-app and breach notices

Plain language about purpose, data, rights and action

Model parent / guardian notice for a new education app

Use before launch when district policy or law requires notice, consent or an opt-out, and whenever transparency would help families understand the use.

Subject: Notice of [App / Service] for [class / school / purpose]

[District / School] plans to use [service] for [specific educational purpose] with students in [grades / classes] beginning [date]. The service will be used through [district-managed accounts / classroom access].

The service will collect or generate the following information: [plain-language data categories]. The district is authorizing use only for [purpose]. [State whether advertising, profiling, AI training, public sharing or direct messaging is disabled or prohibited.]

The provider will retain data for [period / trigger] and will [delete / return] it when [event]. The district reviewed the service for educational value, privacy, security and accessibility under [policy / law].

More information, including the provider privacy policy and district approved-app entry, is available at:

_____

Parents / guardians may ask questions, request applicable records, or exercise any consent / opt-out right by contacting:

_____

[Insert exact consent, opt-out or state-law language if required.]

Sincerely,

_____

// BREACH COMMUNICATION ELEMENTS

Include

What happened and when.

What information was involved.

What the district and vendor have done.

What families should do.

Contact, complaint and support routes.

Avoid

Unverified attribution.

Technical detail that creates new risk.

Promises that no harm will occur.

Blaming students or staff.

Using "no evidence" as if it proves no access.

// TRANSPARENCY

Approved-app inventory and change log

Make approval visible, specific and reviewable

Publish enough information for trust and control.

An approved-app inventory also helps IT disable unused tools, helps teachers find approved alternatives and helps families understand data use.

APP / PROVIDER	PURPOSE / GRADES	DATA CATEGORIES	AUTHORITY / NOTICE	RETENTION	OWNER / REVIEW	LINKS / CONDITIONS

// STATUS LABELS

APPROVED Approved for named grades, purpose, account and conditions.

PILOT Time-limited use with named users, data and evaluation.

RESTRICTED Staff-only, no PII, no under-13 use or other stated condition.

RETIRED Do not use; accounts, integrations and data are being removed.

// CHANGE CONTROL

DATE	CHANGE	PRIVACY / SECURITY EFFECT	DECISION / NOTICE

Re-review trigger: New AI feature, advertising, subprocessor, public-sharing option, data category, terms change, ownership change, breach or age-range expansion.

// STAFF GUIDE

One-page rules for classroom app use

Make the safe route easy to follow

Teacher quick rules

- ☐ Check the approved-app list before use.
- ☐ Use district-managed accounts and minimum roster data.
- ☐ Do not tell students to misstate age or create personal accounts.
- ☐ Do not upload student work, names, photos, voice or records to an unapproved service.
- ☐ Use private class settings and review sharing permissions.
- ☐ Report a terms change, privacy concern or breach promptly.

Stop and ask before

Adding an app through a browser extension or marketplace.

Connecting Google / Microsoft / LMS permissions.

Using AI with student work or records.

Turning on chat, public galleries, social feeds or location.

Collecting voice, face, fingerprints, health or behavior data.

Accepting new terms on behalf of the district.

// STAFF ACKNOWLEDGMENT

I understand that only approved education apps may be used with student accounts, student data or district systems. I will follow approval conditions, protect credentials, use minimum necessary data, avoid personal-account workarounds, and report incidents or material changes.

Name: _____ Role: _____

Signature: _____ Date: _____

// HELP ROUTE

App approval contact:

_____

Privacy / records:

_____

Security incident:

_____

Urgent student safety:

_____

Official state-law examples

Adapt approval, contracts, notices and breach response

State student-data laws can impose duties beyond FERPA and COPPA.

The examples below show common state approaches. Complete a local addendum using current official state sources and district counsel.

STATE EXAMPLE	OFFICIAL REQUIREMENTS / APPROACH	LOCAL ACTION
Georgia	The Student Data Privacy, Accessibility, and Transparency Act, O.C.G.A. sections 20-2-661 through 20-2-667, focuses on privacy, security, transparency and authorized educational use. GaDOE provides model policies and terms resources. [12][13]	
New York	Education Law section 2-d and Part 121 require data privacy and security policies, a Parents' Bill of Rights and supplemental information for contracts receiving protected PII. [14][15]	
Colorado	The Student Data Transparency and Security Act requires transparency, vendor obligations and local policies addressing data indexes, retention/destruction, contracts, breaches, parent notice and staff training. [16][17]	
California	Education Code section 49073.1 requires specified contract terms including school control, purpose limits, parent/student review, security, breach notice, deletion, FERPA compliance and targeted-advertising prohibition. [18]	

// LOCAL STATE CHECKLIST

- ☐ Public app / vendor inventory
- ☐ Parents' bill of rights or annual notice
- ☐ Required contract clauses / data plan
- ☐ Data protection officer / named contact
- ☐ State breach reporting / parent deadlines
- ☐ Retention / destruction schedule
- ☐ Advertising / profiling / biometric limits
- ☐ Complaint and enforcement process

Record: State citation _____ Checked by _____ Date _____

// PROGRAM REVIEW

Annual audit and action tracker

Keep the approved-app environment accurate and controlled

Annual program review

- ☐ Approved-app inventory reconciled with SSO, LMS and network records.
- ☐ Unused accounts, integrations and apps retired.
- ☐ Terms, privacy policies, subprocessors and ownership changes reviewed.
- ☐ Retention and deletion certificates checked.
- ☐ Incidents, complaints and parent questions analyzed.
- ☐ State law, federal guidance and COPPA updates checked.

Program measures

Percentage of active apps with a named owner and current review.

Number of unapproved apps or integrations discovered.

Average approval time by risk level.

Deletion actions completed after retirement.

Staff training completion and repeat issues.

Vendor incidents, late notices or unresolved contract gaps.

// CORRECTIVE-ACTION TRACKER

GAP / APP	ACTION / DELIVERABLE	OWNER	DUE	EVIDENCE / STATUS

Program decision: Continue ☐ Revise ☐ Add resources ☐ Re-audit ☐ Next review _____

Federal references

Official federal government sources only

Source policy:

This toolkit uses official U.S. federal and state government sources only. Verify current requirements and legal advice before adoption or a notification decision.

[1] U.S. Department of Education, Student Privacy Policy Office. To which educational agencies or institutions does FERPA apply? https://studentprivacy.ed.gov/faq/which-educational-agencies-or-institutions-does-ferpa-apply

[2] U.S. Department of Education, Student Privacy Policy Office. K-12 School Officials and FERPA resources. https://studentprivacy.ed.gov/audience/school-officials-k-12

[3] U.S. Department of Education, Student Privacy Policy Office. Responsibilities of Third-Party Service Providers under FERPA. https://studentprivacy.ed.gov/resources/responsibilities-third-party-service-providers-under-ferpa

[4] U.S. Department of Education, Student Privacy Policy Office. FAQ: using an online tool or application under FERPA. https://studentprivacy.ed.gov/faq/i-want-use-online-tool-or-application-part-my-course-however-i-am-worried-it-violation-ferpa

[5] Federal Trade Commission. Complying with COPPA: Frequently Asked Questions, including COPPA and schools. https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions

[6] Federal Trade Commission. FTC Finalizes Changes to Children's Privacy Rule, January 2025. https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data

[7] U.S. Department of Education, Student Privacy Policy Office. Model Terms of Service checklist. https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-model-terms-service

[8] U.S. Department of Education, Student Privacy Policy Office. Protecting Student Privacy While Using Online Educational Services. https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-requirements-and-best

[9] U.S. Department of Education, Student Privacy Policy Office. Data Security: K-12 and Higher Education. https://studentprivacy.ed.gov/data-security-k-12-and-higher-education

[10] U.S. Department of Education, Student Privacy Policy Office. Data Breach Response Checklist. https://studentprivacy.ed.gov/resources/data-breach-response-checklist

[11] U.S. Department of Education, Student Privacy Policy Office. Data Retention and Data Destruction training, July 2025. https://studentprivacy.ed.gov/training/data-retention-and-data-destruction

State references

Official state government sources only

[12] Georgia Department of Education. Data Privacy portal - FERPA, COPPA, PPRA and state resources. https://georgiainsights.gadoe.org/data-privacy/

[13] Georgia Department of Education. Student Data Privacy, Accessibility, and Transparency Act - O.C.G.A. sections 20-2-661 through 20-2-667 and model resources. https://georgiainsights.gadoe.org/data-privacy/student-data-privacy-accessibility-and-transparency-act/

[14] New York State Education Department. Legal Resources, Policies, and Guidance - Education Law section 2-d and Part 121. https://www.nysed.gov/data-privacy-security/legal-resources-policies-and-guidance

[15] New York State Education Department. Required Published Documents - Parents' Bill of Rights, Data Inventory, Data Privacy and Security Policy and supplemental contract information. https://www.nysed.gov/data-privacy-security/ny-education-law-section-2-d-required-website-published-documents

[16] Colorado Department of Education. Data Privacy and Security - Student Data Transparency and Security Act. https://ed.cde.state.co.us/dataprivacyandsecurity

[17] Colorado Department of Education. Sample Privacy and Security Policies - data index, retention, destruction, contracts, breaches, parent notice and training. https://ed.cde.state.co.us/dataprivacyandsecurity/sampleitpolicies

[18] California Legislature. Education Code section 49073.1 - required contract provisions for pupil records and digital educational software. https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=EDC§ionNum=49073.1.

[19] California Department of Education. Data Privacy - state and federal student privacy resources. https://www.cde.ca.gov/ds/ed/dataprivacy.asp

Recommended adoption step. Attach the district app-request form, approved-app inventory, contract addendum, retention schedule, breach contacts and state-law checklist before formal use.

Review date: These sources were checked in July 2026. State statutes, regulations, agency guidance and vendor terms may change.