A PRACTICAL DOCUMENT FOR SCHOOL AND DISTRICT LEADERS

Is your school's AI use *actually* safe?

A 25-question audit you can complete in 30 minutes, designed to surface the privacy, compliance, and procurement risks that hide inside most consumer and enterprise AI tools deployed in K-12 today. Built from real district reviews, not vendor marketing.

WHY THIS EXISTS

Most schools are using AI without knowing what they're using.

Teachers are turning to ChatGPT, Claude, Gemini, and a wave of new ed-tech AI tools — often without district guidance, sometimes against district policy, and almost always without anyone fully understanding what happens to student data once it's typed into a prompt. **This checklist is a tool for catching those risks before they become incidents.** It is also, frankly, a tool for catching vendors who overstate their privacy and compliance posture. Use it on every AI product your district is evaluating, deploying, or has already deployed.

How to use this checklist

Print one copy per AI product or service your school or district uses or is evaluating. Walk through all 25 questions with the relevant team — usually some combination of your technology director, curriculum lead, and an administrator with budget authority.

For each question, check the box only if you have a confident, documented yes. If the answer is "I don't know," "I think so," or "the vendor said yes but we haven't verified," leave the box empty. Empty boxes are not failures — they are conversations you need to have with the vendor before deploying further.

Total your checked boxes at the end and compare against the scoring rubric below. Bring the completed checklist to your next board meeting or vendor review. The goal is not to score perfectly — the goal is to know what you're actually using.

INTERPRETING YOUR SCORE

What each range means.

22 – 25	This vendor is operating at a level most districts should require. Document the answers and proceed with confidence.
17 – 21	Reasonable foundation with material gaps. Address the missing items in writing with the vendor before expanding deployment.
11 – 16	Significant exposure. Limit deployment to non-sensitive uses, do not allow direct student-AI interaction, and escalate to district legal counsel.
10 or below	Do not deploy or continue use without a remediation plan. Notify any teachers or administrators currently using the tool.

1 Data handling

FERPA, COPPA CORE

- [ ] Is the vendor contractually prohibited from training any AI model on data submitted from your district?
  Look for explicit language in the contract or DPA, not just terms-of-service claims. **"We don't train" in marketing is not the same as a contractual prohibition.**
- [ ] Can your district request and receive a complete deletion of all student data within 30 days?
  Ask the vendor to describe the deletion process step by step, including backups and audit logs.
- [ ] Is student data encrypted both in transit and at rest, with documented key management?
  "Yes, we use HTTPS" is the bare minimum. Ask about at-rest encryption and who holds the keys.
- [ ] Does the vendor provide a clear data retention schedule, with defaults that minimize what's stored?
  Default retention should be measured in days or weeks, not years. Longer retention should require explicit opt-in.
- [ ] If a parent requests a copy of all data the vendor holds about their child, can the vendor produce it within statutory timelines?
  FERPA gives parents the right to inspect education records. Vendors who can't produce this on request put the district in legal jeopardy.

2 Compliance posture

FERPA, COPPA, STATE LAW

- [ ] Has the vendor signed a Data Privacy Agreement (DPA) that aligns with your state's standard form, or your district's specific DPA?
  Most states have a model DPA. The Student Data Privacy Consortium maintains versions for many states. Vendors who refuse to sign should be treated with skepticism.
- [ ] For students under 13, does the vendor support COPPA-compliant verifiable parental consent — and route through the school's authority correctly?
  Schools can act as agents for parental consent under COPPA in specific circumstances. The vendor should know the rules, not just claim "we're COPPA compliant."
- [ ] Does the vendor maintain a SOC 2 Type II report (or equivalent) and provide it on request under NDA?
  SOC 2 Type II takes a year to earn and is a meaningful trust signal. Type I, ISO 27001, or "in progress" are weaker but acceptable starting points.
- [ ] Does the vendor commit in writing to notify the district of any security incident affecting student data within a specific timeframe (typically 72 hours)?
  Vague language like "promptly" or "as soon as practical" creates legal exposure for the district. Specific timeframes are non-negotiable.
- [ ] Has the vendor reviewed and confirmed compliance with your state's specific student data privacy law beyond the federal floor?
  Texas has SB 820. California has CalOPPA and SOPIPA. New York has Ed Law 2-d. Most states now have their own. National vendors often miss state-specific requirements.

3 Architecture & sovereignty

WHERE THE DATA GOES

- [ ] Can the vendor name, by company, every third party that processes student data — including AI model providers, cloud hosts, and analytics services?
  "Subprocessors" should be a published list in the contract, with notice required before adding new ones.
- [ ] Does student data ever pass through OpenAI, Anthropic, Google AI, or other consumer-grade AI providers?
  If yes, ask under what contractual terms. Standard API terms are not the same as enterprise terms with no-training and zero-retention guarantees.
- [ ] Is the data physically stored in the United States, with a documented region commitment?
  Some state laws specifically require US-only data residency. "We use AWS" is not sufficient — AWS has regions globally.
- [ ] Is the deployment single-tenant or multi-tenant — and is the answer documented in the contract?
  Multi-tenant is usually fine with proper isolation. But the district should know which it is, and the vendor should be able to explain the isolation guarantees.
- [ ] If the vendor is acquired or shuts down, does the contract guarantee data return and deletion?
  "Acquihire" exits are common in ed-tech. Without explicit clauses, your data can be transferred to entities you never approved.

4 Pedagogy & classroom safety

EFFECT ON LEARNING

- [ ] When a student asks for the answer to a homework problem, does the AI refuse to give it directly and instead guide the student to find it themselves?
  A tool that just gives answers is an academic dishonesty engine, not a tutor. Test this directly with a sample problem before deploying.
- [ ] Does the system have explicit content safety policies for age-appropriateness, and have they been tested with the actual grade levels you'll deploy to?
  "GPT-4 has guardrails" is not enough. The tool should refuse to engage with topics outside its educational scope, including emotional crisis topics that should escalate to a human.
- [ ] If a student expresses signs of distress, self-harm, or a serious safety concern, does the system have a documented escalation path to a real human at your school?
  This is non-negotiable for any student-facing AI. Ask the vendor to walk through what happens, end to end, when this is triggered.
- [ ] Can teachers see and review every AI interaction their students have, and flag any that seem inappropriate or concerning?
  Teacher oversight should not require admin permissions or special tooling. It should be a default part of the daily teacher workflow.
- [ ] Is the content the AI generates aligned to your specific state standards (TEKS in Texas, etc.) at the depth-of-knowledge level the standard requires?
  "Common Core aligned" is often a marketing claim, not a verified one. Ask for specific standard-to-content mappings.

5 Operational readiness

SUSTAINABILITY OF USE

- [ ] Does the vendor provide documented teacher onboarding and training — and is the time commitment realistic for your teachers' actual schedules?
  A tool nobody is trained to use becomes shelfware. If onboarding requires more than two hours initially or more than one hour per month after, ask how that fits in.
- [ ] Are the vendor's pricing terms transparent, with no usage-based fees that could create budget surprises mid-year?
  Per-student annual pricing is preferable to per-query or per-token pricing for school budgets. If usage caps exist, what happens when they're hit?
- [ ] Does the vendor commit to advance notice (typically 90+ days) for any pricing changes, feature removals, or contract changes?
  Without this, vendors can change material terms mid-year, leaving the district to absorb the cost or scramble for replacements.
- [ ] Are the success metrics for the deployment defined upfront, with the vendor's compensation or contract renewal tied to outcomes — not just adoption?
  "95% of teachers logged in" is not success. "Students improved on standards-aligned assessments" is. Outcomes-based contracts are rare but worth pursuing.
- [ ] Does the vendor provide a documented integration plan with your existing SIS, LMS, and identity systems — and is the integration cost included in the price?
  Hidden integration costs can double the real price. PowerSchool, Infinite Campus, Clever, ClassLink — the vendor should know your stack and be ready for it.

AFTER COMPLETING THIS CHECKLIST

What to do with what you've learned.

If your score is 22 or above, document the answers in your vendor file. You've done the diligence; the deployment is defensible.

If your score is between 11 and 21, send the unchecked items to the vendor with a request for written response. Most reputable vendors will engage. The ones who don't are telling you something.

If your score is below 11, pause the deployment. Notify any teachers currently using the tool. Convene your district's data privacy review committee. The risks are too high to continue without a remediation plan.

FROM THE TEAM THAT WROTE THIS

We're MillionRoots — private AI for K-12 classrooms.

We built this checklist because we're tired of seeing schools take risks they don't fully understand. We're also building a tutor and lesson assistant that scores 25 of 25 on it ourselves — because that's the only kind of AI we think belongs in classrooms. If you'd like to talk about a pilot, or just want to ask us about anything in the checklist, write to us. We respond personally.

admin@millionroots.com
www.millionroots.com