

K-12, EXCEPTIONAL STUDENT EDUCATION AND HIGHER EDUCATION LEADERS

The practical AI guide for education

Useful classroom and campus work, with clear privacy boundaries

A focused guide to choosing useful education pilots, protecting student information, reviewing tools and measuring learning and staff outcomes.

INSIDE THIS GUIDE

- | | | | |
|----|-----------------------------------|----|---------------------------------|
| 01 | Start with an educational purpose | 02 | Set student privacy boundaries |
| 03 | Make classroom use reviewable | 04 | Approve tools and prepare staff |
| 05 | Use a pilot to earn the next step | | |

01

Start with an educational purpose

Choose one problem educators recognize, define success, and keep responsibility with the people who serve students.

Choose a manageable first use

Begin with work that uses public or synthetic information: draft a lesson outline, convert a public handbook into a staff FAQ, or build a rubric from published course outcomes. An educator checks every result before use. Avoid starting with admissions, discipline, disability eligibility or student risk scoring.

Write a short pilot charter: the problem, participating staff, approved tool, permitted information, reviewer, end date and stop conditions. Compare the proposed workflow with how staff do the same task today. Faster drafting is useful only if the final material remains accurate and appropriate.

Keep the settings distinct

- K-12: involve instructional leadership, families and age-appropriate student guidance. Define what students may use and what teachers must review.
- Exceptional student education (ESE): use AI for generic supports and preparation. Qualified staff and the student's team retain responsibility for individualized plans and services.
- Higher education: separate teaching, research, student services and administration. Research data, financial aid and clinical activities need their own approvals.

Try this first

Ask an approved assistant: "Using only these published learning objectives, draft a 30-minute activity for [grade or course]. Include materials, an accessible participation option and three checks for understanding. Flag assumptions." Have the teacher verify alignment and adapt the activity to the actual class. Record the review time and revisions needed. Keep student records out of this first exercise.

Set student privacy boundaries

Approve the data flow before staff or students enter information into an AI tool.

Know what the tool receives

List the information sent through prompts, uploaded files, recordings, browser extensions and connected learning systems. Include outputs, logs, backups and support access. A name removed from a detailed narrative may still leave a student identifiable. Use synthetic examples for training and early pilots.

The U.S. Department of Education's online-services guidance explains privacy questions under FERPA. Have the institution's privacy lead determine the applicable consent or exception, permitted purpose and vendor obligations. Do not treat a vendor's privacy badge as the institution's legal analysis.

Ask before approving

- Who can access prompts and files, including subcontractors and human reviewers?
- Can the institution restrict training, secondary use and redisclosure? What do the actual contract and settings say?
- Where is information processed, how long is it retained, and how can the institution retrieve or delete it?
- What happens when a student leaves, a contract ends, or a security incident occurs?
- For children's services, who reviews COPPA applicability, notices and consent requirements? The FTC's guidance is a starting point.

Give staff a clear rule

Publish an approved-tool list that names permitted uses and data types. An approved lesson-planning tool is not automatically approved for student evaluations. Tell staff whom to contact when a task falls outside the list. If protected information enters an unapproved tool, stop using that workflow and report it through the institution's incident process. Preserve necessary evidence without spreading the information further.

Make classroom use reviewable

Good prompts name the task, provide trusted material and leave the educator able to explain the result.

Lesson and assessment template

"Act as a drafting assistant for [subject and level]. Use only the supplied standards and approved source text. Create [activity or assessment] for [duration]. Include learning objectives, instructions, an answer key with reasoning, accessibility options and likely misconceptions. Do not invent standards or citations. List gaps for teacher review."

Before distributing, solve the assessment, check reading level and inspect examples for stereotypes. Confirm accommodations through the normal educational process.

ESE preparation template

"Using this fictional classroom scenario, suggest three ways to present [concept] through visual, spoken and hands-on activities. Describe materials, possible barriers and ways a teacher could check understanding. Do not diagnose, infer a disability, or recommend eligibility or placement."

For actual students, follow the institution's approved process and data environment. AI output must not substitute for evaluation, professional judgment, family participation or the student's voice.

Teach transparent student use

- State which assignments allow AI and what disclosure is expected. Give examples of allowed brainstorming and prohibited substitution.
- Have students compare an AI answer against assigned sources, identify unsupported claims and explain their corrections.
- Assess the student's reasoning through drafts, reflection or discussion. Avoid treating an AI-detection score as conclusive proof.
- Provide a usable alternative when a tool is inaccessible, unavailable or inappropriate for a student.

Approve tools and prepare staff

Choose the deployment that fits the institution's data and operating capacity, then test it with real classroom conditions.

Compare complete operating costs

Evaluate an institution-managed cloud service, private environment or on-premises system against the same requirements. Location alone does not establish privacy or security. Include account controls, updates, filtering, monitoring, backups, support, accessibility and the staff needed to run the service.

For a campus knowledge assistant, start with a small collection of approved public documents. Assign a content owner and review date. Require answers to identify their sources and decline when the collection does not support an answer. Test whether users can retrieve information beyond their permissions before connecting restricted repositories.

Run a practical acceptance review

- Privacy and security: verify access controls, retention settings and separation between users or departments.
- Instruction: have educators review misleading answers, missing context and inappropriate content.
- Accessibility: test keyboard navigation, screen-reader use, captions and error recovery with affected users. W3C Easy Checks offers an initial screen, not a complete evaluation.
- Operations: practice disabling a connector, withdrawing an incorrect resource and continuing without the tool.

Train for the actual job

Give staff a short, role-specific exercise using an approved template and safe data. Show how to check sources, correct an answer and report a problem. Provide office hours and an accessible quick reference. Keep accounts tied to institutional identity, remove access when roles change, and name someone who can suspend a pilot promptly.

Use a pilot to earn the next step

Set a review date and make continuation depend on evidence the institution can inspect.

A practical sequence

First, select one workflow and approve its data boundary. Next, train a small staff group and test synthetic examples, including confusing or incomplete requests. Then run a limited pilot with educator review and an established alternative. Expand only after the owner reviews both benefits and failures.

For a lesson-planning pilot, retain a safe sample of requests, sources, drafts, final lessons and educator corrections under institutional retention rules.

Keep a simple scorecard

Quality	Were standards, answers and references correct after review?
Effort	How much total drafting, checking and correction time was required?
Access	Could participating staff and students use the material and the alternative?
Safety	Were there privacy incidents, inappropriate outputs or unapproved uses?
Learning	What evidence shows the activity supported its intended objective?

Make the decision visible

Review results with instructional, privacy, accessibility and technology representatives, including ESE or research expertise where relevant. Record continue, change or stop, remaining risks and an owner. Share lessons without exposing students.

Bring one workflow, one safe example and the tool agreement to the next meeting. Identify a useful next step with evidence, responsibility and a way to pause.

REFERENCE

Sources and next steps

01 NIST AI Risk Management Framework

Voluntary framework for governing, mapping, measuring and managing AI risks. A framework is not a certification.

<https://www.nist.gov/itl/ai-risk-management-framework>

02 U.S. Department of Education student privacy guidance

FERPA considerations for online educational services; consult institutional privacy and legal reviewers for the specific use.

<https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-requirements-and-best>

03 FTC COPPA guidance

Children's online privacy considerations. The page directs readers to the revised rule for current requirements.

<https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>

04 W3C WAI Easy Checks

Initial accessibility checks. These do not replace a complete evaluation.

<https://www.w3.org/WAI/test-evaluate/preliminary/>

Choose one useful next step.

Discuss a reviewable first step with Z7 Solutions™.

Book a conversation **contact@z7solutions.com** **844-974-8669**