

THE STUDY GROUP

Behind every data point is a child



**Screening technology-enhanced
assessments for safety, privacy, & security**

SEPTEMBER 2026

Evidence before assessment decisions

Quality resources help assessment, privacy, security and operations teams review tools before purchase, pilot or renewal.

Why share these resources?

Reuse credible questions and evaluators. Divide the review across the people who can judge the evidence.

How to read the profiles

Summaries describe publisher guidance. Evidence requests and assessment applications are pulled together by Study Group.

Scope of the shortlist

This curated set supports discussion.



Protection and measurement quality

Every score belongs to a person. Technology choices affect the evidence we collect and the decisions we make.



Concern	Measurement consequence
Privacy	Responses and inferred profiles can expose more than a reported score.
Security	Altered records or exposed items can undermine score integrity.
Safety and fairness	Harmful feedback or unequal errors can affect participation and decisions.
Operations	Outages and broken transfers can change who completes an assessment.

A manageable starting set

Five questions to guide a first review

1EdTech

Profile p. 8

What data practices does the provider disclose?

GESS

Profile p. 10

What product security controls have evidence?

CISA

Profile p. 11

Can the school system operate and recover safely?

UNICEF

Profile p. 15

How does the experience protect children?

ITC/ATP

Profile p. 17

Are the assessment interpretations defensible?

For AI, add Digital Promise (p. 14) and NIST (p. 16). The full directory adds resources for contracts, governance and data exchange.



Privacy, security and operations

Resource	Primary job
Common Sense (p. 7)	Identify privacy-policy concerns
1EdTech TrustEd Apps (p. 8)	Apply a consistent privacy rubric
SDPC NDPA (p. 9)	Specify contractual data obligations
SDPC GESS (p. 10)	Examine product security controls
CISA K–12 toolkit (p. 11)	Prepare school-system operations
Project Unicorn (p. 12)	Evaluate usable data exchange



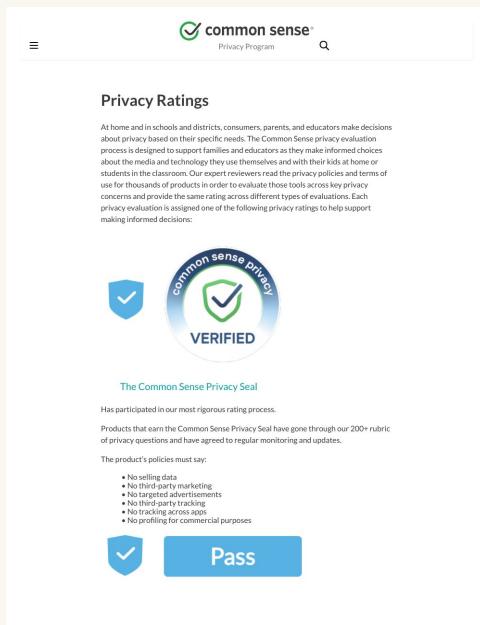
AI safety and assessment quality

Resource	Primary job
EDSAFE SAFE (p. 13)	Organize AI governance concerns
Digital Promise AI (p. 14)	Screen responsible AI design
UNICEF AI and Children (p. 15)	Examine children's rights and safety
NIST AI RMF + GenAI (p. 16)	Manage technical AI risks over time
ITC/ATP guidelines (p. 17)	Review digital assessment practice

The decision and the people affected determine which resources you need.



Common Sense Privacy Evaluations



Privacy policy review

A clear first pass through a product's published privacy promises, with questions and product-level evaluations.

Study Group evidence request

The current evaluation, its depth and date, plus answers about collection, sharing, advertising, retention and deletion.

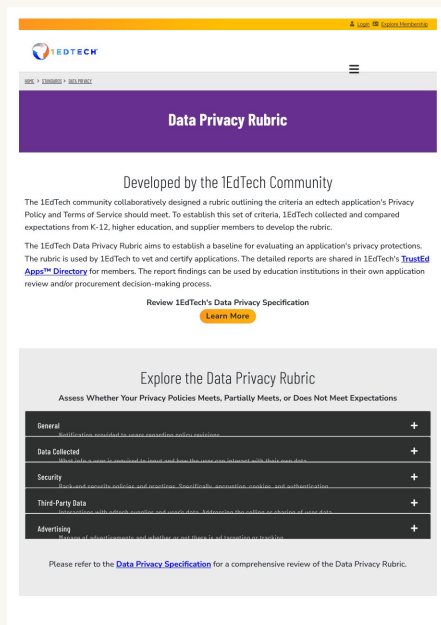
Assessment application

Include recorded speech, student responses and inferred learner profiles in the data inventory.

Limit Policy review cannot establish how the software behaves or whether technical controls work.

Open the official resource

1EdTech TrustEd Apps



Privacy rubric and certification

An inspectable rubric turns published privacy policies and terms into consistent review questions.

Study Group evidence request

Completed privacy criteria with dated evidence. For AI, add the separate Generative AI Data Rubric on training data and prompt use.

Assessment application

Clarify whether student work or assessment responses train the provider's model or a third party's model.

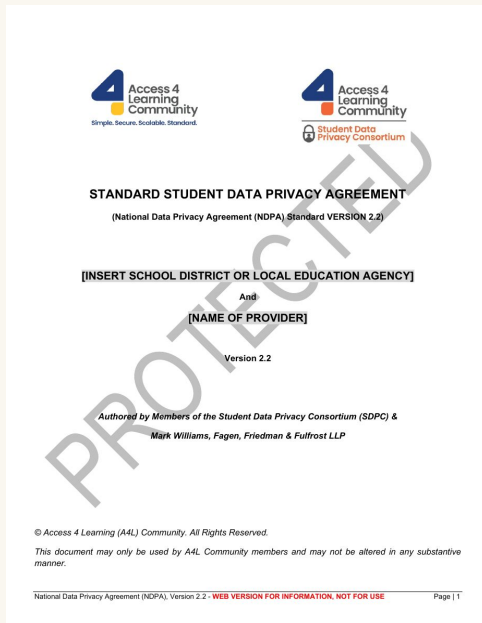
Limit Privacy certification reviews policy evidence. The AI rubric is a separate self-assessment. Detailed vetting results require membership.

[Open the official resource](#)

[Open the AI data rubric](#)

National Data Privacy Agreement

SDPC contract framework · v2.2



The agreement puts data obligations into the school system's relationship with a provider.

Study Group evidence request

A completed product and data schedule, authorized uses, subcontractor terms, deletion provisions and applicable state terms.

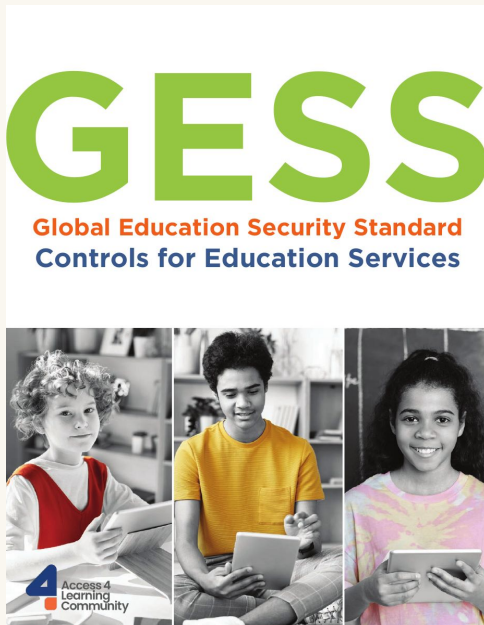
Assessment application

Name scores, recordings, student work and derived data explicitly. Examine exceptions for de-identified data and service changes.

Limit The posted copy is for reference. Use is limited to A4L members. A contract also needs implementation evidence and local counsel's review.

Open the official resource

Global Education Security Standard



SDPC security controls and assessment

GESS turns security and privacy controls into education-specific questions, with an assessment route that verifies evidence.

Study Group evidence request

Product scope, risk tier, assessment date, report, unresolved findings and remediation evidence. Demonstrate access and deletion controls.

Assessment application

Give persistent student profiling and predictive attainment scoring deeper scrutiny under the published tiering approach.

Limit An assessment applies to its stated scope and date. Self-alignment and third-party assessment provide different levels of assurance.

Open the official resource



CISA K–12 Cybersecurity Toolkit



School-system operational guidance

Protecting Our Future gives school leaders a concrete starting point for reducing cyber risk.

Study Group evidence request

Evidence of multifactor authentication, vulnerability remediation, tested backups, incident-response exercises and staff training.

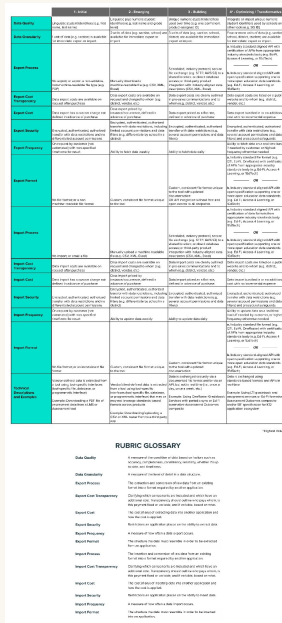
Assessment application

Rehearse an assessment outage. Establish how staff recover responses, protect score integrity and decide whether students need another session.

Limit District readiness requires local execution. The toolkit does not certify a vendor or establish a product's safety.

Open the official resource

Project Unicorn Interoperability Rubric



The image shows a detailed table with multiple columns and rows, representing the Project Unicorn Interoperability Rubric. The table is organized into sections, with the first section having a teal header. The rows contain specific criteria and evidence for each category.

Vendor evaluation rubric

The rubric makes usable data exchange a procurement question and gives school systems language for vendor review.

Study Group evidence request

A live export and transfer demonstration using representative assessment records, with field definitions and access permissions.

Assessment application

Check that student identifiers, score meanings and assessment versions survive transfer into the receiving system.

Limit Interoperability alone cannot establish appropriate data use, secure implementation or valid score interpretation.

Open the official resource



EDSAFE AI SAFE Benchmarks

**what is the
EDSAFE AI SAFE Framework?**

**EDSAFE AI
ALLIANCE**

Founded in 2020, the EDSAFE AI Alliance is a global initiative coordinated by InnovateEDU and powered by a coalition of organizations representing stakeholders across the education sector to provide global leadership for developing a safer, more secure, more equitable, and more trusted AI education ecosystem through a focus on research, policy, and practice.

By joining forces and complementing rather than competing with stakeholders in the space, we can address one of the most pressing educational policy challenges of our time: how to build and develop an ecosystem that reflects the best practices for AI use in education.

With a shared mission to leverage AI to facilitate better, more equitable student outcomes, save time for teachers and other educators, and increase efficiencies for those invested in teaching and learning ecosystems, EDSAFE AI is an uncommon alliance dedicated to furthering safe, accountable, fair and transparent, and efficacious AI use within the K-12 education space through the SAFE framework.

We believe that AI should not be used to replace educators in classrooms or in decision-making processes: instead, AI can be used to reduce educator paperwork and help to synthesize and make suggestions based on learner data. In this fashion, AI can be leveraged to allow teachers more time for direct instruction with their learners, using technology as a "co-pilot" that supports teachers in doing the human, emotional, affective work that is at the heart of the learning process.

Led by a Steering Committee of organizations and their leaders who are already working at the intersection of AI and education, EDSAFE AI aims to bring diverse voices to help educate policymakers and shape an equitable and safe AI education ecosystem.

STEERING COMMITTEE

AASA, The School Superintendents Association	Education Counsel
AI in Education	Federation of American Scientists (FAS)
aiEDU	IRTE/ASCD
American Association of Colleges for Teacher Education (AACTE)	National Center for Learning Disabilities (NCLD)
American Federation of Teachers (AFT)	National Digital Inclusion Alliance (NDIA)
CAST	National Education Association (NEA)
Coda.org	National Parents Union
Consortium for School Networking (COSN)	Opportunity Labs
Council of Great City Schools	Project Evident
Data Science 4 Everyone	SETDA
Digital Promise	Software & Information Industry Association (SIIA)
Districts Institute	The New Teacher Project (TNTP)
EdTrust	Transcend

edsafeai.org

Shared framework for educational AI

SAFE has four domains: Safety, Accountability, Fairness and Transparency, and Efficacy.

Study Group evidence request

For each domain, name a responsible person, a reviewable artifact and a decision rule for the proposed use.

Assessment application

Keep data protection and equitable educational benefit in the same review while recording separate findings for each.

Limit This is an organizing framework. Its headings need specific tests and evidence before they can support product approval.

Open the official resource

Digital Promise Responsibly Designed AI



Education product certification

Five published evidence requirements give procurement teams a concise screen for responsible AI design.

Study Group evidence request

Privacy and security policies, bias mitigation examples, a reporting route, generated-content labels and a demonstrated user override.

Assessment application

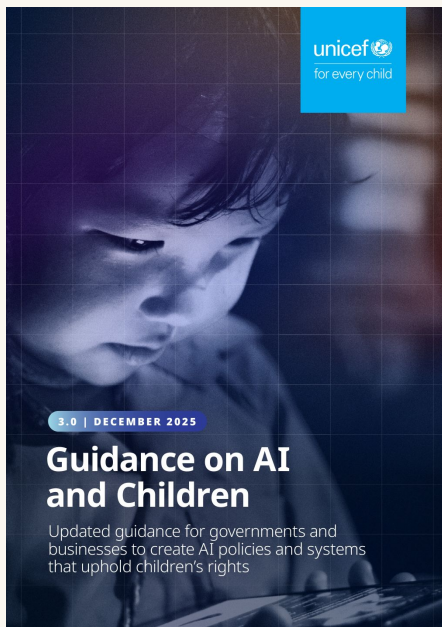
Check how educators challenge AI feedback or recommendations. Certification requires override of at least one learning decision.

Limit The badge does not establish score validity or complete security. Check the exact product and date. Certification expires after two years.

Open the official resource

UNICEF

AI and Children



Child-rights guidance and checklist · v3

The 2025 guidance makes children's safety, privacy, inclusion and development explicit, alongside accountability and fairness.

Study Group evidence request

A child-rights impact assessment, age-appropriate safety tests, understandable disclosures and a route to report harm and obtain redress.

Assessment application

Examine conversational assessment, emotional feedback and voice collection through the child's experience and developmental needs.

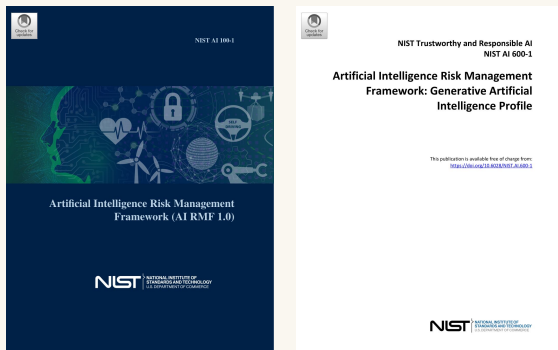
Limit The guidance needs product-specific acceptance criteria. It does not offer a universal passing score or technical certification.

[Open the official resource](#)

[Open the checklist](#)

NIST AI Risk Management Framework

RMF 1.0 and Generative AI Profile



Govern, Map, Measure and Manage organize technical evaluation and responsibility throughout an AI system's life.

Study Group evidence request

An intended-use statement, risk register, representative evaluation results, adversarial tests, monitoring plan and model-change records.

Assessment application

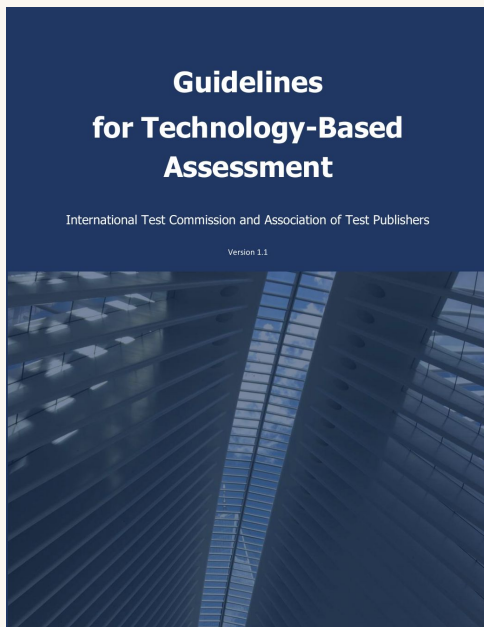
Recheck scoring and feedback after model changes. Define when a human intervenes, the service pauses or the prior version returns.

Limit The voluntary framework requires expertise. Generic model benchmarks cannot establish validity for a local assessment use. Check the current edition.

[Open the official resource](#)

[Open GenAI Profile](#)

ITC/ATP Technology-Based Assessment



Professional guidelines · v1.1, 2025

These guidelines connect digital protection with the quality of assessment interpretations and decisions.

Study Group evidence request

Evidence for the intended score use, subgroup results and a disruption plan. For automated scoring, request validation data separate from model-training data.

Assessment application

Review test security and data privacy alongside scoring, fairness, accessibility and the consequences of technology failures.

Limit The guidelines need qualified assessment judgment. They are not a product certification or a universal checklist score.

Open the official resource

Conditions for data and operations

Privacy: trace the data

Require a map of collection, inference, sharing, model training and deletion. Resolve unapproved uses before live student use.

Security: verify the controls

The provider supplies scoped control evidence and remediation status. The review team resolves critical gaps before approval.

Operations: rehearse failure and exit

Demonstrate recovery, score reconciliation and usable export. Name school and provider owners for an incident.



Conditions for safety and assessment use

Child safety: test plausible harms

Review age-appropriate scenarios and escalation routes. Address harmful feedback, unsafe interaction and inaccessible reporting.

AI: define human responsibility

Specify review, challenge and override routes. Recheck material model changes before extending an approved use.

Assessment: justify the intended use

The assessment lead reviews validity, precision and subgroup evidence for the intended use. Restrict decisions that lack this support.



An AI reading assessment

Recorded oral reading informs instructional support.

Review question	Evidence needed
What happens to recordings?	Retention and training-use terms, plus a deletion demonstration (1EdTech, NDPA)
Are results defensible?	Accuracy and subgroup evidence for the intended learners (ITC/ATP)
Can staff handle problems?	Correction route, outage plan and score-recovery exercise (CISA, ITC/ATP)
Can the system change safely?	Model-version record, change notice and revalidation trigger (NIST)



If required evidence is missing, pause the affected use. Name who must resolve the gap and what evidence would change the decision.

Where this fits

Suggested entry points, subject to source review

Existing WS3 concern	Suggested resources
Privacy and data rights (W3-13)	Common Sense, 1EdTech, NDPA
Cybersecurity (W3-14)	GESS, CISA
Child safety and age fit (W3-15 / 20)	UNICEF
Operations (W3-10 / 16 / 17)	CISA, Project Unicorn, ITC/ATP
Fairness and oversight (W3-18 / 19)	Digital Promise, NIST, EDSAFE
Outcomes and evidence (W3-11 / 24)	ITC/ATP

These mappings indicate potential relevance. They do not establish that a resource covers every criterion.



Privacy and operations

Publisher resources and guidance



01 Common Sense Privacy Evaluations

Privacy policy review

privacy.commonsense.org



02 1EdTech TrustEd Apps

Privacy rubric and certification

1edtech.org



03 National Data Privacy Agreement

SDPC contract framework · v2.2

privacy.a4l.org



04 Global Education Security Standard

SDPC security controls and assessment

privacy.a4l.org



05 CISA K–12 Cybersecurity Toolkit

School-system operational guidance

cisa.gov



06 Project Unicorn Interoperability Rubric

Vendor evaluation rubric

projectunicorn.org

AI and assessment

Publisher resources and guidance



07 EDSAFE AI SAFE Benchmarks

Shared framework for educational AI
edsafeai.org



08 Digital Promise Responsibly Designed AI

Education product certification
digitalpromise.org



09 UNICEF AI and Children

Child-rights guidance and checklist · v3
unicef.org



10 NIST AI Risk Management Framework

RMF 1.0 and Generative AI Profile
airc.nist.gov



11 ITC/ATP Technology-Based Assessment



Professional guidelines · v1.1, 2025
testpublishers.org

Resource choice depends on the intended use.

One assessment tool, one documented decision

The next Study Group review

Name the intended use

Choose one assessment tool. Identify the learners, the proposed score use and the person leading the review.

Assign the evidence requests

Use the shortlist to divide questions among assessment, privacy, security and operations reviewers. Set a due date.

Record the decision and its conditions

Document permitted uses, required controls and the next review date. Pause uses with unacceptable material risks.

