



AI Implementation Reference Guide for IT Teams

Section 1 – Tool Classification and Intended Use

AI-enabled tools vary significantly in how they operate and the level of oversight they require. Before evaluating technical, privacy, or legal considerations, districts should first understand what type of tool they are reviewing and how it will be used. The level of risk and required controls may differ depending on whether the tool is publicly accessible, enterprise-managed, or embedded within an existing system.

Type of Tool

- ☐ Is this a public AI tool that individuals can access without district approval?
- ☐ Is this an enterprise-managed platform with district-level administrative control?
- ☐ Is AI functionality embedded within another product already approved by the district?
- ☐ Does the tool require individual account creation, or can it be managed centrally?

Intended Users and Scope

- ☐ Who will use the tool (students, staff, administrators)?
- ☐ What grade levels will have access?
- ☐ Is the tool intended for instructional use, operational use, or both?
- ☐ Will the tool be optional or required?

System Integration and Data Access

- ☐ Does the tool integrate with district systems (e.g., SIS, LMS, Google Drive, Microsoft 365)?
- ☐ Does it require access to district files or shared drives?
- ☐ Does it allow users to upload documents or connect external data sources?
- ☐ Does it allow sharing of content outside the district?

Agentic and Automated Use

- ☐ Does the tool operate autonomously on behalf of users (e.g., browsing the web, sending emails, writing to files, or executing multi-step tasks)?
- ☐ If so, what actions can it take, and what are the boundaries of those actions?
- ☐ Does the tool maintain persistent credentials or ongoing access to district systems between sessions?

Agentic and Automated Use (Continued)

- ☐ Can autonomous actions be logged, reviewed, and reversed if necessary?
- ☐ Can the scope of autonomous actions be restricted by role or user group?

Section 2 – Data Collection and Storage

AI-enabled tools may collect, store, and reuse user inputs, uploaded documents, and system-generated data in ways that differ from traditional educational software. Districts should clearly understand what data is collected, how it is stored, how long it is retained, and whether it is reused for other purposes. Careful review of data practices is essential to protect student and staff information and ensure compliance with district policies.

Data Collected

- ☐ What types of data does the tool collect (student information, staff information, usage data)?
- ☐ Does the tool collect personally identifiable information (PII)?
- ☐ Are user prompts or inputs stored?
- ☐ Are uploaded files stored?
- ☐ Does the tool collect metadata such as interaction timing, engagement metrics, or activity history?

Data Storage and Retention

- ☐ Where is district data stored (country or region)?
- ☐ Is data encrypted in transit and at rest?
- ☐ How long are prompts, uploads, and usage logs retained?
- ☐ Can the district configure retention settings?
- ☐ Can the district request permanent deletion of data?
- ☐ What happens to district data when the contract ends?

Data Reuse and Model Improvement

- ☐ Is district data used to improve or train the vendor's system?
- ☐ If so, can the district opt out in writing?
- ☐ Is training opt-out controlled at the district (administrator) level?

Data Reuse and Model Improvement (Continued)

- ☐ Is district data combined with data from other customers?
- ☐ Is de-identified or aggregated district data used for product development?

Data Sharing and Subprocessors

- ☐ Does the vendor share data with subprocessors or affiliates?
- ☐ Is a list of subprocessors available?
- ☐ Does the vendor notify the district of changes to subprocessors?
- ☐ Are subprocessors contractually bound to the same data protections?

Section 3 – Account Management and Administrative Control

Effective oversight of AI-enabled tools depends on strong identity management and administrative controls. Districts should ensure that access can be centrally managed, features can be configured appropriately, and usage can be monitored when necessary. Tools that cannot be managed at the district level may present increased operational and compliance risk.

Identity and Access Management

- ☐ Does the tool support single sign-on (SSO) with Google, Microsoft, or other district identity providers?
- ☐ If SSO is not supported, does the tool support Multi-Factor Authentication (MFA)?
- ☐ Does it support automated provisioning (e.g., ClassLink, Clever, SCIM)?
- ☐ If automated provisioning or SSO is not supported, can accounts be provisioned in bulk via CSV file upload or SFTP?
- ☐ Can accounts be created and managed centrally?
- ☐ Can accounts be deactivated immediately when users leave the district?
- ☐ Does the tool require personal email addresses or phone numbers for account creation?

Role-Based Controls and Feature Restrictions

- ☐ Can features be turned on or off by role (student, teacher, administrator)?
- ☐ Can student access be restricted by grade level?
- ☐ Can public sharing be turned off?

Role-Based Controls and Feature Restrictions (Continued)

- ☐ Can file uploads be restricted or disabled?
- ☐ Can external integrations be limited?
- ☐ Can access to the tool be restricted to district networks or approved locations?

Logging and Monitoring

- ☐ Are user activities logged?
- ☐ Can administrators view or export usage logs?
- ☐ Are prompts and outputs retained for administrative review?
- ☐ Can log retention settings be configured?
- ☐ Are alerts available for inappropriate or unusual activity?

Classroom and Instructional Controls

- ☐ Can teachers monitor student activity within the tool?
- ☐ Can teachers restrict or guide student AI interactions?
- ☐ Can parents or guardians request access to their student's AI interaction history?

Classroom and Instructional Controls

- ☐ Can teachers monitor student activity within the tool?
- ☐ Can teachers restrict or guide student AI interactions?
- ☐ Can parents or guardians request access to their student's AI interaction history?

Administrative Visibility and Support

- ☐ Does the vendor provide an administrative dashboard?
- ☐ Can administrators view system-wide usage trends?
- ☐ Is technical support available to district administrators?
- ☐ Does the vendor provide documentation specific to K-12 environments?

Section 4 - Security and Legal Compliance

These tools must meet the same security, privacy, and contractual standards as other district technology systems. Districts should verify that vendors maintain appropriate security safeguards, comply with applicable student privacy laws, and agree to contractual protections that clearly define data ownership, permitted use, and breach response obligations.

Security Standards and Certifications

- ☐ Does the vendor maintain current security certifications (e.g., SOC 2, ISO 27001)?
- ☐ Has the vendor completed a recent third-party security assessment or penetration test?
- ☐ Are security controls documented and available for review?

Breach Notification and Incident Response

- ☐ Does the contract specify a breach notification timeline?
- ☐ Is the notification timeline consistent with district policy and applicable law?
- ☐ Does the vendor provide a documented incident response process?
- ☐ Are responsibilities clearly defined in the event of a data breach?

Contractual Protections

- ☐ Will the vendor sign the district's Data Privacy Agreement (DPA) or the CA-NDPA?
- ☐ Does the contract clearly state that the district retains ownership of its data?
- ☐ Does the contract prohibit the sale of student data?
- ☐ Does the contract define permitted uses of district data?
- ☐ Does the contract address data return and deletion upon termination?

Compliance with Student Privacy Laws

- ☐ Does the vendor comply with applicable federal and state student privacy laws (e.g., FERPA, COPPA, SOPIPA)?
- ☐ If parental consent is required, does the vendor provide documentation to support compliance?
- ☐ Does the vendor disclose subprocessors and data-sharing practices?

Section 5 – Advertising, Profiling, and Secondary Use of Data

Many AI tools collect detailed usage information about students and staff. In addition to privacy and security considerations, districts should evaluate whether this data is used for advertising, profiling, or other commercial purposes.

Advertising and Marketing

- ☐ Does the tool display advertising to students or staff?
- ☐ Does the vendor use student or staff data for targeted advertising?
- ☐ Is district data shared with third parties for marketing purposes?
- ☐ Does the contract explicitly prohibit targeted advertising?

Profiling and Behavioral Analytics

- ☐ Does the tool collect detailed usage analytics (e.g., prompts entered, interaction timing, engagement metrics)?
- ☐ Does the vendor build user profiles based on behavior or usage patterns?
- ☐ Are profiles used for marketing, promotion, or commercial analysis?
- ☐ Does the contract prohibit behavioral profiling for non-educational purposes?

Secondary Use and Commercial Reuse of Data

- ☐ Is district data reused to improve commercial products?
- ☐ Is district data combined with data from other customers?
- ☐ Is “de-identified” or aggregated data used for AI training or product development?
- ☐ Can the district opt out of secondary data use?
- ☐ Does the contract prohibit the sale of student or staff data?

Section 6 – Ongoing Governance and Oversight

Approved tools require ongoing monitoring. Unlike traditional software, AI systems may change behavior as models are updated or new features are introduced. Districts should establish a process for continued oversight after initial approval.

Change Management

- ☐ Are significant updates documented and dated?
- ☐ Does the vendor provide advance notice before major changes are deployed?
- ☐ Is there a clear process for reviewing new AI-enabled features added to an existing product?

Monitoring and Review

- ☐ Can the district monitor how the tool is being used?
- ☐ Are usage logs available for review?
- ☐ Is there a process for investigating inappropriate or unsafe use?
- ☐ Has the district established, at a minimum, an annual review of approved AI tools, even if informal?

Monitoring and Review

- ☐ Can the district monitor how the tool is being used?
- ☐ Are usage logs available for review?
- ☐ Is there a process for investigating inappropriate or unsafe use?
- ☐ Has the district established, at a minimum, an annual review of approved AI tools, even if informal?

Internal Governance

- ☐ Has the district identified a single person responsible for AI oversight? This does not require a committee or formal process. Responsibility should be assigned to a specific person or team.
- ☐ Is there a cross-functional review process for new AI tools?
- ☐ Are staff trained on appropriate use and data handling expectations?
- ☐ Does the district periodically review approved AI tools for continued compliance?

Incident Response

- ☐ Districts do not need a formal incident response program. At a minimum, staff should know who to contact and how to report a concern.
- ☐ Is there a process for reporting harmful, biased, or inaccurate outputs?
- ☐ Is there a process for reporting suspected misuse of student data?

Incident Response (Continued)

- ☐ Does the vendor provide a mechanism for reporting system-level safety concerns?

Section 7 – Instructional Use, Safety, and Output Risk

Unlike traditional software, these tools generate content, recommendations, and responses that may influence teaching and learning. AI systems can produce inaccurate, biased, or inappropriate outputs. Districts should evaluate whether appropriate safeguards and expectations are in place before approving use.

Content Safety Controls

- ☐ Does the vendor use content moderation or filtering to reduce inappropriate outputs?
- ☐ Are harmful, violent, or explicit responses blocked or flagged?
- ☐ Can the district configure or restrict certain types of content?
- ☐ Are safety controls applied differently for students and staff?

Accuracy and Reliability

- ☐ Does the vendor clearly state that AI-generated responses may be inaccurate?
- ☐ Are users informed that outputs should be reviewed before relying on them?
- ☐ Does the vendor provide guidance on appropriate use in educational settings?
- ☐ Are there documented limitations of the tool?

Age Appropriateness

- ☐ Is the tool designed for K-12 use?
- ☐ Does the vendor specify minimum age requirements?
- ☐ Are there additional safeguards for younger students?
- ☐ Can student access be restricted by grade level or role?

Bias and Fairness

- ☐ Has the vendor taken steps to reduce biased or discriminatory outputs?
- ☐ Is there a process for reporting biased or harmful responses?
- ☐ Does the vendor provide documentation describing how bias is evaluated and addressed?

Academic Integrity and Misuse

- ☐ Does the tool include features to discourage academic misuse?
- ☐ Are usage logs available to support investigations when necessary?
- ☐ Does the district provide guidance to staff and students on appropriate use?

Reporting and Escalation

- ☐ Is there a clear process for reporting harmful, inappropriate, or unsafe outputs?
- ☐ Does the vendor provide a mechanism to report system-level concerns?
- ☐ Has the district identified who is responsible for reviewing and responding to reported issues?

Special Thanks

CITE produced the guide in partnership with the Technology Services Committee (TSC) of California County Superintendents. We wish to especially thank the members of the AI Subcommittee within TSC for participating in the development of the guide.

