CITE™
CALIFORNIA IT IN EDUCATION

AI Implementaion Checklist Companion Guide

CALIFORNIA **IT IN EDUCATION**
Shaping the Future of Education Through Technology

cite.org

How to Use This Guide

This guide supports the AI Implementation Checklist by helping districts interpret vendor responses and identify when additional review is needed. Use it alongside the AI Implementation Checklist, with each section providing additional context for interpreting the corresponding checklist questions.

Use it to:

- Understand what vendor answers should include
- Recognize incomplete or unclear responses
- Determine when to follow up, restrict use, or delay adoption

When reviewing vendor responses:

- Prioritize written documentation (privacy policy, DPA, security materials)
- Do not rely on verbal assurances
- Treat unclear or incomplete answers as unresolved

This guide does not replace legal review or procurement processes.

Tool Classification and Intended Use

Related to Section 1 of the AI Implementation Checklist

Why This Matters

Districts should first understand what type of AI tool they are reviewing and how it will be used. Public tools, enterprise platforms, and embedded AI features present different levels of risk and control. Agentic AI tools require particular attention — unlike prompt-and-response tools, they take actions on behalf of users such as browsing the web, sending emails, writing to files, or executing multi-step tasks. Districts should understand what actions a tool can take before evaluating any other considerations.

Questions This Section Addresses

- What type of tool is this (public, enterprise, embedded)?
- Who will use it and how broadly?
- Can access be controlled or restricted?
- Does it connect to district systems?

Questions This Section Addresses (Continued)

- Does the tool operate autonomously on behalf of users?
- If so, what actions can it take, and what are the boundaries of those actions?
- Can autonomous actions be logged, reviewed, and reversed?
- Can the scope of autonomous actions be restricted by role or user group?

Where to Find the Answer

- Vendor website or product overview
- Terms of Service
- Product documentation or demos
- Vendor technical or architecture documentation

What a Good Answer Looks Like

- Tool type and deployment model are clearly defined
- Users and scope are clearly identified
- Access can be limited (pilot, role-based, or group-based)
- Vendor distinguishes public vs. enterprise environments
- Vendor clearly defines what actions the tool can and cannot take
- Autonomous actions are logged and available for administrative review
- The scope of actions can be restricted by role or user group
- The tool does not maintain persistent credentials without district knowledge
- Actions can be reversed or undone if necessary

Red Flags

- Tool type is unclear or inconsistent
- Users can sign up independently without district control
- Scope of use is undefined or expanding
- AI features added without notice
- Product behavior differs from what was approved
- Vendor cannot clearly define the boundaries of autonomous action
- Actions taken by the tool are not logged or reviewable
- Persistent access to district systems cannot be revoked between sessions
- Scope of autonomous actions cannot be restricted by role

What to Do Next

If tool classification, scope, or agentic capabilities are unclear, consider the following steps:

- Request written clarification from the vendor
- Limit use to a pilot until scope and controls are clear
- Involve IT and instructional leadership before broader rollout
- Request written documentation of all actions the tool can take
- Confirm logging and reversibility before any deployment involving agentic features
- Limit agentic features to staff only until controls are verified
- Treat any tool with autonomous system access as high risk until fully evaluated

Data Collection, Storage, and Use

Related to Section 2 of the AI Implementation Checklist

Why This Matters

AI tools may collect and reuse prompts, uploaded content, and usage data in ways that differ from traditional software. Districts should understand how data is stored, retained, and used, especially whether it is used for system improvement or model training.

Questions This Section Addresses

- What data is collected (prompts, uploads, metadata)?
- How is data stored, and how long is it retained?
- Can data be deleted?
- Is district data used for system improvement or model training?
- Is data combined across customers?
- Is data shared with subprocessors?

Where to Find the Answer

- Privacy policy
- DPA or CA-NDPA
- Terms of Service
- Vendor trust center or security documentation

What a Good Answer Looks Like

- Data types (including prompts and uploads) are clearly identified

What a Good Answer Looks Like (Continued)

- Storage location and retention timelines are defined
- Vendor clearly states whether data is used for training or improvement
- District can control or opt out of training where applicable
- Data ownership, retention, and deletion are defined in writing
- Subprocessors are disclosed

Red Flags

- “Data may be used to improve services” with no detail
- Vendor cannot confirm whether prompts or uploads are stored or reused
- No clear retention or deletion process
- Training use is unclear or cannot be disabled
- Data use differs across policy, contract, and vendor statements
- Vendor relies on verbal assurances

What to Do Next

If data collection, storage, or use practices are unclear:

- Request written clarification of data use and retention
- Ask vendor to confirm training and improvement practices explicitly
- Require key protections (no training, retention limits) in DPA/CA-NDPA
- Limit use (e.g., no student data, pilot only) until clarified
- Involve legal/privacy review if student data is involved

Infrastructure and Technical Environment

Related to Section 2 and 3 of the AI Implementation Checklist

Why This Matters

AI tools may introduce new integrations, network requirements, and data flows within the district environment. Understanding these dependencies helps avoid unexpected performance, compatibility, and system access issues.

Questions This Section Addresses

- How is the tool hosted (cloud, local, hybrid)?
- What systems does it integrate with?
- What data is exchanged through integrations?
- What network or access requirements exist?
- Does the tool impact performance or system load?
- Does it introduce new data flows or storage locations?

Where to Find the Answer

- Vendor technical or architecture documentation
- Integration or API documentation
- Implementation or setup guides
- Vendor support resources

What a Good Answer Looks Like

- Hosting model and system requirements are clearly documented
- Integration points and data access are defined
- Network requirements (domains, ports, allow-listing) are provided in advance
- Data flows between systems can be identified
- Performance impact (API usage, data transfers) is disclosed

Red Flags

- No clear documentation of integrations or architecture
- Integration details are vague or incomplete
- Network requirements are not disclosed until implementation
- Vendor cannot explain data flow between systems
- Performance impact is unknown
- New data storage locations are created without visibility

What to Do Next

If infrastructure or integration requirements are unclear:

- Request technical documentation before deployment
- Involve IT operations and network teams early

What to Do Next (Continued)

- Validate integrations and performance through a pilot
- Do not assume the tool behaves like standard SaaS
- Delay rollout until system impact is understood

Account Management and Administrative Control

Related to Section 3 of the AI Implementation Checklist

Why This Matters

Districts need to manage user access, permissions, and usage centrally. Tools that rely on individual accounts or personal devices can reduce visibility and create administrative and compliance challenges.

Questions This Section Addresses

- How users access the tool (SSO, MFA, or individual accounts) and how accounts are provisioned
- Whether accounts can be centrally managed
- How access can be controlled by role or group
- Whether personal devices, emails, or phone numbers are required
- How licensing and billing are managed
- What administrative visibility and monitoring tools are available

Where to Find the Answer

- Vendor identity and access documentation
- Admin console or configuration settings
- Implementation or onboarding guides
- Licensing and billing documentation

What a Good Answer Looks Like

- Supports district-managed authentication (e.g., SSO)
- Accounts can be provisioned and deprovisioned centrally
- Access can be controlled by role or group

What a Good Answer Looks Like (Continued)

- No requirement for personal email, phone, or device
- Licensing and billing are managed at the district level
- Administrators have access to usage logs and system controls

Red Flags

- Users must create accounts outside district control
- Personal email or phone number required
- Billing tied to individual users or credit cards
- Accounts cannot be quickly disabled
- Limited or no administrative controls
- Little visibility into usage

What to Do Next

If account management or administrative control is limited:

- Request written clarification of data use and retention
- Ask vendor to confirm training and improvement practices explicitly
- Require key protections (no training, retention limits) in DPA/CA-NDPA
- Limit use (e.g., no student data, pilot only) until clarified
- Involve legal/privacy review if student data is involved

Security and Legal Compliance

Related to Section 4 of the AI Implementation Checklist

Why This Matters

AI-enabled tools must meet the same security, privacy, and contractual standards as other district systems. Districts should confirm that vendors protect data appropriately and that key expectations are defined in written agreements. These expectations should be reflected in written agreements, not solely in vendor statements or marketing materials.

Questions This Section Addresses

- Vendor security practices and certifications
- Encryption and protection of data
- Breach response and notification procedures
- Availability of security documentation
- How customer data is separated in shared environments
- Contractual protections for data ownership, use, and retention
- Compliance with student privacy laws (e.g., FERPA, COPPA, SOPIPA)

Where to Find the Answer

- Data Privacy Agreement (DPA) or CA-NDPA
- Vendor trust center or security documentation
- Privacy policy and Terms of Service
- Security certifications or summaries
- Vendor legal or compliance documentation

What a Good Answer Looks Like

- Security practices are clearly documented in writing
- Data is encrypted in transit and at rest
- Vendor maintains recognized security certifications or assessments
- Breach response timelines and responsibilities are defined
- Vendor explains how customer data is separated from other customers
- Contract clearly defines data ownership, use, retention, and deletion
- Vendor demonstrates compliance with applicable student privacy laws

Red Flags

- Security claims are vague or marketing-based
- No documentation of controls or certifications
- Breach response is unclear or undefined
- Vendor cannot explain data separation across customers
- Contract does not address ownership, retention, or deletion
- Legal compliance claims are not supported in writing
- Vendor relies on verbal assurances

What to Do Next

If security or legal practices are unclear or incomplete:

- Request written security documentation from the vendor
- Ensure key protections are included in the DPA or CA-NDPA
- Involve legal and privacy review for tools handling student data
- Do not rely on undocumented vendor claims
- Delay adoption until expectations are clearly defined in writing

Advertising, Profiling, and Secondary Use of Data

Related to Section 5 of the AI Implementation Checklist

Why This Matters

AI tools may collect and analyze user activity in ways that could be used for advertising, profiling, or other commercial purposes. Districts should ensure that data is used only to provide educational services and not for marketing or unrelated business purposes.

Questions This Section Addresses

- Whether the tool displays advertising
- Whether data is used for marketing or targeted advertising
- Whether user activity is used to build profiles
- Whether data is shared with third parties
- Whether data is reused for commercial purposes beyond the service
- Whether the district can limit or opt out of secondary data use

Where to Find the Answer

- Privacy policy
- Terms of Service
- DPA or CA-NDPA
- Vendor FAQs or disclosures

What a Good Answer Looks Like

- No advertising is shown to users
- Data is not used for marketing or targeted advertising
- Data is used only to provide the contracted service
- Vendor does not build commercial profiles from user activity
- Any use of aggregated data is clearly defined and limited
- Contract explicitly prohibits sale or commercial reuse of data

Red Flags

- “Data may be used for business purposes” without explanation
- Data is shared with marketing partners or affiliates
- Vendor builds behavioral or usage profiles
- Data is reused for unrelated commercial products
- Vendor cannot clearly explain how aggregated data is used
- Contract does not address advertising or commercial use

What to Do Next

If advertising, profiling, or commercial data use practices are unclear:

- Request written clarification of how data is used beyond the core service
- Ensure contract prohibits advertising, profiling, and sale of data
- Ask vendor to define any use of aggregated or de-identified data
- Avoid tools with unclear or advertising-based business models, especially for students
- Involve legal or privacy review if data use extends beyond educational purposes

Ongoing Governance and Oversight

Related to Section 6 of the AI Implementation Checklist

Why This Matters

AI tools can change over time through updates, new features, or changes in vendor practices. Most districts cannot sustain a formal governance program. What they can do is assign ownership, set a minimum annual review, and ensure staff know how to report a problem. That is enough to maintain basic accountability.

Questions This Section Addresses

- How the district monitors vendor updates and system changes
- Whether changes are communicated and reviewed
- Who is responsible for oversight
- Whether tools are periodically re-evaluated
- How issues or concerns are reported and addressed
- How staff are supported in responsible use

Where to Find the Answer

- Vendor release notes or update notifications
- District review or approval processes
- Staff guidance and training materials
- Incident reporting processes

What a Good Answer Looks Like

- Vendor communicates significant updates or changes in advance
- The district has identified a specific person or team responsible for oversight
- Approved tools are reviewed at least annually, even if informally
- Staff know who to contact if they encounter a problem
- The vendor provides a mechanism for reporting concerns

Red Flags

- Vendor can change functionality without notice
- No assigned owner for oversight
- Tools are not revisited after approval
- Staff receive little or no guidance
- Vendor has no defined process for responding to reported concerns

What to Do Next

If governance and oversight processes are not clearly defined, consider the following steps:

- Assign ownership for AI oversight to a specific person or team
- Establish a process for reviewing vendor updates

What to Do Next (Continued)

- Establish a process for reviewing vendor updates
- Define when tools will be re-evaluated
- Provide staff with basic guidance on use and data handling
- Create a simple process for reporting issues
- Limit initial deployment until basic oversight is in place, even if that means one assigned person and an annual check-in

Instructional Use, Safety, and Output Risk

Related to Section 7 of the AI Implementation Checklist

Why This Matters

AI tools can generate content that is inaccurate, biased, or inappropriate. Districts should ensure these tools are used with appropriate safeguards and that staff and students understand their limitations.

Questions This Section Addresses

- Whether safeguards exist to reduce harmful or inappropriate outputs
- How the vendor communicates limitations related to accuracy
- Whether the tool is appropriate for K–12 use and different age groups
- How bias and fairness are addressed
- How the district supports responsible use
- How unsafe outputs or misuse are reported

Where to Find the Answer

- Vendor product documentation or help center
- Safety or moderation policies
- Administrative settings or controls
- District policies (AUP, AI guidance)

What a Good Answer Looks Like

- Tool includes safeguards such as content moderation or filtering

What a Good Answer Looks Like

- Vendor clearly communicates that outputs may be inaccurate
- Tool can be configured for age-appropriate use
- Vendor describes steps to reduce biased or harmful outputs
- District provides guidance for staff and students
- Clear process exists for reporting inappropriate outputs

Red Flags

- Outputs are presented as authoritative without limitations
- No safeguards for inappropriate or harmful content
- Vendor cannot explain how bias is addressed
- Students use the tool without clear expectations
- No way to report harmful or inappropriate outputs
- Users are expected to rely on outputs without review

What to Do Next

If instructional safety and output risks are not clearly addressed, consider the following steps:

- Provide staff with guidance on the appropriate use and verification of outputs
- Limit student access until safeguards and expectations are in place
- Use available controls to restrict features or content
- Establish a process for reporting and responding to unsafe outputs
- Reinforce that AI tools support, not replace, professional judgment

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.