



Tulare Local Healthcare District

Policy Name:	Artificial Intelligence (AI) Use Policy
Policy Number:	
Version Number:	001
Approved by Board on:	
Scheduled review date:	

1. Purpose and Scope

The Tulare Local Healthcare District (District) recognizes that artificial intelligence (AI) tools can help improve efficiency, support daily tasks, and assist with research, writing, planning, and other District operations.

AI tools may be used to support work, but they do not replace human judgment, professional expertise, or individual responsibility. The District permits thoughtful use of AI while maintaining appropriate safeguards for confidentiality, accuracy, security, public accountability, and responsible stewardship of public resources.

This policy applies to anyone conducting business on behalf of or for the benefit of the District, including District Staff, Board Members, contractors, consultants, vendors, and other representatives.

The policy covers all AI tools, including standalone applications and AI features built into other software or services. Only AI tools approved by the Chief Executive Officer (CEO) may be used for District Business. This requirement applies whether the tool is accessed through a District device, personal device, or online account.

2. Definitions

- Artificial Intelligence (AI): Technology that performs tasks typically requiring human intelligence, including generating content, analyzing information, and identifying patterns.
- Generative AI: AI tools that create text, images, presentations, code, or other content based on user instructions.
- Confidential Information: Confidential, personal, financial, proprietary, privileged, security-related, protected health information (PHI), or other information that is not intended for unrestricted public release.

3. Guiding Principles and Appropriate Use

AI tools may be used to support routine District activities, including:

- Drafting and editing correspondence, reports, presentations, and other documents.
- Summarizing publicly available information and non-sensitive materials.
- Developing templates, checklists, training materials, and project plans.
- Brainstorming ideas and identifying potential operational improvements.
- Organizing non-sensitive information and assisting with preliminary research and analysis.

AI must not replace required professional judgment, supervisory review, legal advice, financial controls, or official decision-making. AI-generated recommendations must not serve as the sole basis for personnel, legal, financial, procurement, or policy decisions. Personnel remain responsible for reviewing AI-generated content for accuracy, completeness, appropriateness, and consistency with District policies and applicable law.

4. Confidentiality, Security, and Prohibited Uses

AI tools must be used in ways that protect confidential information, District systems, and public trust.

Personnel must not:

- Enter confidential, sensitive, proprietary, or legally protected information into AI tools.
- Enter passwords, security credentials, or sensitive internal security information into AI prompts.
- Use AI to create misleading information, impersonate individuals, or misrepresent District activities.
- Use AI to circumvent District policies, security controls, records retention requirements, or legal obligations.
- Upload copyrighted, licensed, or contractually restricted materials in violation of applicable terms or law.
- Distribute AI-generated work as an official District product without appropriate review and approval.

Connecting AI tools to District email accounts through plug-ins, extensions, add-ons, or other integrations is strictly prohibited.

Uploading, entering, or otherwise sharing privileged, confidential, sensitive, proprietary, or legally protected information into AI tools is strictly prohibited.

Personnel should use publicly available, generalized, or anonymized information whenever possible; review privacy settings and vendor terms; and use District-approved tools when available and required. Questions about the sensitivity of information or the suitability of a tool should be referred to a supervisor or the Chief Executive Officer. Suspected security incidents, unauthorized disclosures, or violations of this policy must be reported promptly through established District procedures.

5. Accuracy, Public Records, and Accountability

Personnel remain responsible for all work produced with AI assistance. AI tools must not independently authorize or take actions reserved for authorized personnel or the Board of Directors. As a public agency, the District must comply with applicable public records, records retention, and open-meeting requirements, including the California Public Records Act (CPRA) and the Ralph M. Brown Act. AI-generated content, prompts, outputs, and related communications may constitute District records depending on their purpose, content, and use.

Personnel must preserve applicable District records and must not use AI tools to evade disclosure requirements, circumvent open-meeting laws, or improperly delete or conceal records. Questions concerning public records, Board communications, or legal compliance should be referred to the Chief Executive Officer or appropriate legal counsel.

6. Intellectual Property and Approved Tools

AI use must comply with applicable copyright laws, software licenses, vendor terms, confidentiality obligations, and District procurement and technology policies. AI-generated material should be reviewed for potential copyright concerns and inappropriate use of third-party content before publication or distribution.

The District may approve, restrict, or prohibit AI tools based on privacy protections, cybersecurity, vendor practices, cost, reliability, and operational needs. Personnel must obtain appropriate authorization before purchasing AI services, connecting tools to District systems, or using AI to process sensitive District information.

7. Training and Compliance

The District encourages personnel to develop familiarity with AI tools appropriate to their roles and to understand their limitations and risks. Training or guidance may address appropriate use, accuracy, confidentiality, cybersecurity, public records, and responsible evaluation of AI-generated content.

Personnel should consult a supervisor or the Chief Executive Officer when questions arise regarding appropriate AI use. Potential security incidents, unauthorized disclosures, or other significant concerns must be reported promptly through established District procedures.

Violations of this policy may result in appropriate corrective or disciplinary action consistent with applicable law and District policies.

Date	Version #	Description
10 28 2026	001	Initial Release