DFO HR CONSULTING · TEMPLATE · OCTOBER 2026

AI Use Policy Template for Public Agencies

Prepared by Dr. Frank Olmos, Ed.D. · drfrankolmos.com

> **How to use this template.** Replace the highlighted fields, delete what does not apply, and add your agency's own procedures. This is a starting draft, not legal advice. Review it with your legal counsel before adoption, and give your recognized employee organizations notice and an opportunity to meet and confer where the policy affects terms and conditions of employment.

1. Purpose

[Agency name] (the "Agency") permits the responsible use of artificial intelligence (AI) tools to improve service to the public and the quality and efficiency of staff work. This policy sets the rules for that use so that AI supports staff judgment without replacing it, protects confidential information, and keeps the Agency accountable for its decisions and records.

2. Scope

This policy applies to all employees, elected and appointed officials, contractors, interns and volunteers who use AI tools for Agency business, on any device or account. It covers generative AI tools (such as chat assistants, writing and summarization tools, image and audio generators, and AI meeting note-takers) and AI features built into other software.

3. Definitions

- **Generative AI:** software that produces text, images, audio, code or other content in response to a prompt.
- **Approved tool:** an AI tool, account or feature listed in Appendix A after review by [IT / Information Security / designated AI lead].
- **Confidential information:** any information the Agency must or may withhold from public disclosure, including the categories in Section 5.
- **Human review:** a qualified person reading, checking and taking responsibility for an AI output before it is used.
- **Public-facing AI:** an AI tool that communicates directly with members of the public, such as a website chat assistant.

4. Approved tools

- Use only approved tools for Agency business. Appendix A lists each tool and the data it may handle.
- Do not use personal AI accounts for Agency work, and do not connect AI tools to Agency systems, email or files without approval.

- Requests for a new tool go to [designated AI lead], who reviews security, data retention, vendor terms, accessibility and cost before approval.

5. Protecting confidential information

Never enter the following into an AI tool unless Appendix A expressly approves that tool for that category of data:

- Personnel records, applicant and examination materials, and disciplinary or investigation files
- Social Security numbers, driver's license numbers, bank or payment information, and passwords
- Medical or health information, including workers' compensation and leave records
- Student records [school and community college districts] and criminal justice information [if applicable]
- Attorney-client privileged material, closed-session material, and records exempt from disclosure under the California Public Records Act
- Security plans, network details and other information that could compromise Agency systems or facilities

When in doubt, remove names and identifying details, use fictional examples, or ask your supervisor first.

6. Permitted and prohibited uses

Permitted with human review	Prohibited
Drafting and editing correspondence, reports, notices and job materials	Making or recommending final decisions about hiring, promotion, discipline, pay or termination without documented human judgment
Summarizing public documents, meeting material and research	Determining eligibility for public benefits, permits or services without human decision-making
Brainstorming, outlining and plain-language rewriting	Creating content that impersonates a real person or misrepresents the Agency
Translation drafts, checked by a fluent reviewer before release	Monitoring or evaluating employees with AI except as negotiated and disclosed
Data analysis on approved, de-identified data	Entering confidential information into an unapproved tool

7. Human review and accountability

- The employee who uses an AI output is responsible for its accuracy, tone and compliance, the same as for any other work product.
- Check facts, figures, citations and legal references against original sources. AI tools can produce confident but incorrect content.
- Supervisors decide which tasks in their unit require a second reviewer.

8. Transparency and public-facing AI

- Any AI that communicates with the public must clearly disclose that it is AI. California's bot law (Business and Professions Code §17940 and following) restricts using a bot to mislead people about its artificial identity.
- Public-facing AI must draw only on approved Agency sources and must be tested and approved by [department head] before launch. The Agency is responsible for the information its tools give the public.
- Disclose substantial AI assistance in public reports and staff reports when [criteria set by the Agency].

9. Recording, transcription and AI note-takers

- California law generally requires the consent of all parties before a confidential communication is recorded. Announce any recording or AI note-taker at the start of a meeting or call, and stop if a participant objects.
- Do not use AI note-takers in closed sessions, investigations, disciplinary meetings, medical or accommodation discussions, or attorney consultations.

10. Public records and retention

Prompts, outputs and AI-generated drafts used in Agency business may be public records under the California Public Records Act. Retain and produce them under the Agency's records retention schedule, and use approved tools whose records the Agency can access.

11. Employment decisions, fairness and bias

- Any AI used in recruitment, selection, promotion or other employment decisions must be approved in advance by Human Resources and reviewed for adverse impact, consistent with the Fair Employment and Housing Act and the Civil Rights Council's regulations on automated-decision systems.
- Selection tools must remain job-related and consistent with merit-system rules [Personnel Commission / Civil Service rules, if applicable].
- Report outputs that appear biased, offensive or discriminatory to [designated AI lead].

12. Labor relations

The Agency will provide notice to affected recognized employee organizations, and meet and confer where required, before implementing AI uses that affect wages, hours or other terms and conditions of employment, including changes to job duties, workload or monitoring.

13. Procurement and vendors

Contracts for AI tools or services must address data ownership, confidentiality, data retention and deletion, use of Agency data to train models, security, accessibility, breach notification and audit rights.

14. Training

Employees must complete [Agency-approved AI training] before using approved tools for Agency business, and refresher training when this policy changes.

15. Incidents

Report suspected disclosure of confidential information, a harmful or inaccurate output that reached the public, or a security concern to [IT / Information Security] and your supervisor immediately.

16. Compliance

Violations may result in loss of tool access and discipline consistent with Agency rules and applicable agreements.

17. Review

The [designated AI lead] will review this policy at least every [12] months, and sooner when laws, tools or Agency needs change.

Appendix A. Approved AI tools

Tool and account type	Approved uses	Data allowed	Owner
[e.g., Microsoft 365 Copilot, Agency tenant]	[drafting, summarizing]	[internal; no personnel records]	[IT]

Appendix B. Employee acknowledgment

I have read the [Agency name] AI Use Policy, I understand it, and I agree to follow it. I understand that I am responsible for reviewing any AI output I use in my work.

Employee name	Department
Signature	Date

Template provided by DFO HR Consulting for adaptation by public agencies. It does not constitute legal advice. Laws and regulations change; confirm current requirements with your legal counsel. For help adapting it, see the AI Readiness and Governance Sprint at drfrankolmos.com.