



City of Cortez

Generative AI & AI Tools Policy

Version Number	Date	Changed By	Description of Change
0.1	9/22/2025	Jay Rohrer	Created
0.2	4/14/2026	Patrick Coleman	Edits
1.0	7/14/2026	City Council	Approval of Policy

Contents

Overview.....	2
Purpose.....	3
Scope.....	3
Definitions.....	3
Guiding Principles.....	4
Allowed Uses (Examples).....	4
Prohibited or Restricted Uses.....	5
Data Classification and Tool Matching.....	5
Accounts and Access.....	5
Attribution and Public Communication.....	6
Public Records and Retention.....	6
High-Risk Use Approval.....	6
Procurement and Vendor Requirements.....	6
Staff Responsibilities.....	6
IT Department Responsibilities.....	7
Incident Reporting.....	7
Training and Change Management.....	7
Pilots (Low-Risk Sandbox).....	7
Enforcement.....	8
References.....	8
Appendix A (Separate Document): CJIS-Aware Guidance for Police.....	8

Overview

The City of Cortez’s Artificial Intelligence (“AI”) Policy allows AI to improve the services provided to the public while keeping humans accountable. Staff must use City-approved tools appropriate to the data, never place sensitive or regulated information (e.g., Criminal Justice Information Systems (“CJIS”), Health Insurance Portability and Accountability Act (“HIPAA”) in unapproved systems, and verify outputs for accuracy and bias. AI assisted public content requires a disclosure, and prompts/outputs are public records under Colorado Open Records Act (“CORA”) and the Colorado Criminal Justice

Records Act (“CCJRA”). High-risk uses need IT and City Attorney approval, and a CJIS aware appendix sets extra rules for Police.

Purpose

Enable safe, effective, and transparent use of AI, including Generative AI (“GenAI”), to improve services while protecting privacy, complying with public-records and accessibility laws, and maintaining public trust.

Scope

This policy covers any AI/GenAI tool used for City business, whether City-provided or accessed online, by employees, elected officials, contractors, interns, or volunteers. Vendors operating AI for the City must comply.

Definitions

The following definitions apply in this policy:

- Artificial Intelligence (“AI”): A machine-based system that, for a given set of human-defined objectives, makes predictions, recommendations, or decisions that influence physical or virtual environments.
- Generative AI (“GenAI”): A type of AI system capable of creating new content, such as text, audio, code, images, or video, based on patterns learned from training data. Examples include ChatGPT, Microsoft Copilot, and Google Gemini.
- User Prompt: A question, instruction, information, or input submitted by personnel to a GenAI tool.
- Authorized Use: Use of a GenAI tool that complies with this policy, with a tool that has been approved by the IT Director or City Manager or their designee when necessary and does not involve prohibited content or purposes.
- Personal Information: Any information about an individual that can be used to identify them, including but not limited to names, addresses, dates of birth, Social Security numbers, financial data, or personal photographs.
- Public Record: Any writing, recording, or data generated, received, or maintained by the organization for use in the performance of a public function, as defined by C.R.S. § 24-72-202(6)(a)(I), including AI-generated content created in the course of official duties.
- Personally Identifiable Information (“PII”): Any information that can be used to distinguish or trace an individual’s identity, either alone or when combined with

other personal or identifying information. This includes, but is not limited to, names, addresses, phone numbers, email addresses, dates of birth, Social Security numbers, driver's license numbers, financial account information, medical or health data, biometric identifiers, photographs, or other data that could reasonably identify a specific individual.

- **Shadow AI:** The unauthorized, unmonitored, or unreported use of GenAI tools for official purposes, whether on personal or work devices.
- **Personnel:** Any individual performing work on behalf of the City, including full-time and part-time employees, interns, temporary workers, volunteers, and elected or appointed officials, whether compensated or not.

Guiding Principles

- **Human-in-the-loop:** Staff remain responsible for outcomes; AI assists but does not replace judgment.
- **Transparency:** Disclose AI assistance in public-facing materials when AI is a key contributing resource.
- **Privacy and Security:** Only use tools approved for the data classification involved.
- **Accuracy and Bias Mitigation:** Treat outputs as drafts; verify facts; screen for bias or harm.
- **Public Records and Retention:** Prompts and outputs may be public records when created for City business, subject to any exemptions in CORA or CCJRA. Retention of prompts and output records are subject to the City's record retention policy.
- **Accessibility:** Public materials must meet digital accessibility requirements.
- **Compliance:** Follow CORA, CCJRA, records schedules, procurement, data protection, and state and federal law.

Allowed Uses (Examples)

- Drafting internal memos, reports, agendas, summaries, or checklists.
- Creating outlines, brainstorming ideas, policy options, or content drafts.
- Summarizing public documents or records.
- Assisting with translation, grammar, rewriting, or clarity improvements.
- Drafting website copy, FAQs, or social media text with human review.
- Low-risk data exploration using de-identified datasets only.
- Code assistance without secrets or credentials.

- Customer service chatbots with proper disclosure and human oversight.
- A starting point for researching legal, legislative, scientific or technical information.

Prohibited or Restricted Uses

- Submitting as part of a prompt or including personal, sensitive, confidential, or legally protected data in AI prompts. This includes personally identifiable information (PII), Social Security Numbers (SSNs), CJIS, HIPAA or medical, Payment Card Industry (PCI), proprietary data of the City, personnel records, legal documents, court records, or internal policies not otherwise public.
- Communications related to legal, disciplinary, or personnel decisions (e.g., performance evaluations, letters of reprimand, termination notices).
- Uploading documents or records that contain confidential information, even if the goal is only to summarize or edit the content.
- No use of content protected by copyright laws or other intellectual property laws (“Copyrighted Data”) unless the City has a legal right to use such content.
- Using personal AI accounts for work-related activities.
- Generating images, videos, or multimedia using Copyrighted Data.
- Generating images, videos, or multimedia that impersonate real individuals or public officials.
- Using AI tools that have not been vetted and approved for business use by City leadership.
- Using any GenAI that does not retain a record of prompts and outputs for inspection or archiving, or that prohibits City officials from accessing or downloading those records for retention or review purposes.

Violations of these restrictions may result in disciplinary action, up to and including termination, and/or referral under Cortez’s Employee Handbook and ethics policy.

Data Classification and Tool Matching

IT will maintain an Approved AI Tools list with the maximum data classification permitted (Public, Internal, Confidential, Restricted). Staff must select tools approved for the intended data class.

Accounts and Access

GenAI must be used on accounts owned by the City and personal accounts may never be used for work performed for the City. Account credentials for AI platforms must not be shared between users and must be stored securely. Enable Multi Factor Authentication (MFA). Do not share Application Programming Interface (API) keys or credentials. Contractors must follow this policy.

Attribution and Public Communication

When GenAI meaningfully contributes to public facing content, include a disclosure (e.g., “This content includes AI-assisted drafting and was reviewed by City staff.”). Record the tool, model and human approver in internal publishing notes.

Public Records and Retention

Prompts and outputs created for City business may be public records and must be retained per applicable records retention schedules in approved repositories (e.g., project folder, case file, ticket).

- Prompts must not include any personal, sensitive, or confidential information.
- Prompts must be free from discriminatory or inappropriate language unless such language is necessary for the conduct of proper City business.
- Users must treat all prompt and uploaded information as public records which might be open to the public under the CORA and/or CCJRA.

Consult the Clerk, Records Officer, or the City Attorney’s Office on exemptions and timelines.

High-Risk Use Approval

For any use that could affect rights, benefits, or access to services, departments must obtain pre-approval from IT and the City Attorney after completing:

- 1) AI Risk Assessment
- 2) Algorithmic Impact Assessment
- 3) Privacy & Security Review
- 4) Human Oversight Plan (including appeals).

Procurement and Vendor Requirements

Contracts for AI tools must address: data ownership (City owns inputs and outputs), usage limits (no vendor training on City content without permission), security controls and audit rights, breach notice, model transparency (capabilities and limits), bias testing results, accessibility conformance, and public records cooperation.

Staff Responsibilities

Before prompting: select an approved tool and limit data to the lowest classification needed.

AI-generated content must be reviewed for factual accuracy and consistency before being used or shared. Personnel must:

- Review and verify all information created by GenAI.
- Cross-check facts, citations, figures, and quotes.
- Independently verify any interpretations, policy recommendations, or statistical summaries generated by AI.
- Write in your voice.
- Add citations to authoritative sources.

AI-generated content may never be relied upon as authoritative or final without human oversight and verification.

After prompting: store prompts and outputs with the work file; disclose public use; log significant uses per [Data Classification and Tool Matching](#).

IT Department Responsibilities

Maintain the approved tools catalog and data-class mappings; provide training and “dos and don’ts”; review high-risk uses with the City Attorney; monitor major model updates and adjust guidance.

Incident Reporting

Immediately notify IT and the City Attorney if sensitive data entered a non-approved tool, biased or unsafe outputs were published, or an AI vendor reports a breach/abnormal behavior.

Training and Change Management

New users complete a 60-minute introduction covering safety, privacy, CORA, CCJRA, accessibility, bias, and approved use cases; annual refreshers thereafter.

Pilots (Low-Risk Sandbox)

Departments may run opt-in pilots on low-risk tasks using de-identified data with explicit human review; share lessons learned City-wide.

Enforcement

Violations may result in access limits, retraining, or disciplinary action per Human Resources (HR) policy and applicable law.

References

Boulder County IT AI Policy; City of Boston (Interim GenAI Guidelines); City of San José (GenAI Guidelines); City of Seattle (GenAI Policy); State of Washington (Generative AI Guidelines); OpenGov (AI for Government); National Association of Counties; Governing (Cities/Counties draft guidelines); National League of Cities; MRSC (Use of Generative AI); CORA; Colorado AI Act (effective Feb 1, 2026).

Appendix A (Separate Document): CJIS-Aware Guidance for Police

See 'PoliceCJISAnnexCortez.docx' for detailed rules for law enforcement uses, including CJIS data handling with AI tools, approved workflows, and prohibited practices.