



CITY OF LITTLE ROCK

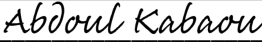
Department of Information Technology

ARTIFICIAL INTELLIGENCE ACCEPTABLE USE POLICY

Document Title	Artificial Intelligence Acceptable Use Policy
Policy Owner	Chief Information Officer (CIO)
Classification	INTERNAL — All City Personnel
Version	1.0
Effective Date	3/9/2026
Review Date	3/2/2026
Approved By	City Manager / CIO / City Attorney's Office / Department of Human Resources

Ver.	Date	Author	Summary	Approved By
1.0	3/23/2026	Information Technology	Initial Release	City Manager

Approval Signatures

Name	Title	Signature / Date
Frank Scott Jr.	Mayor	 / 3/24/26
Abdoul Kabaou	CIO & AI Committee Chair	 / 4/15/2026
Lynette Perez	Chief Deputy City Attorney	/
Sheridan Richards	Chief People Officer	/

1. Purpose and Scope

The City of Little Rock is committed to the ethical, responsible, and lawful use of Artificial Intelligence (AI) across all its operations, services, and programs. This policy establishes clear requirements and guidelines governing how AI tools may be adopted and used by all City personnel and those performing work on the City's behalf.

AI presents meaningful opportunities to improve public service delivery, operational efficiency, and decision support — but also introduces risks related to data privacy, security, bias, accountability, and legal compliance. This policy enables the City to leverage AI's benefits while managing those risks in a manner consistent with its values and obligations to the public.

1.1 Scope

This policy applies to all City of Little Rock elected officials, employees, contractors, representatives, affiliates, agents, and any person or entity performing services for or on behalf of the City — on City-owned or personal devices used for City business purposes.

It covers all AI tools and systems including generative AI, machine learning, automated decision-making, and AI-embedded features within approved software.

1.2 Policy Owner

The Chief Information Officer (CIO), supported by the AI Committee, owns and enforces this policy. Department Directors are accountable for compliance within their departments.

► *Questions should be directed to the AI Committee at innovation@littlerock.gov.*

2. Definitions

Term	Definition
Artificial Intelligence (AI)	Machine learning technology, software, automation, and algorithms that perform tasks, generate content, or make predictions based on existing datasets and instructions.
AI Committee	An internal City committee responsible for reviewing and approving AI uses, maintaining the approved tool list, and overseeing this policy.
AI System	Software using machine learning, logic-based, or statistical approaches that generates outputs such as content, predictions, recommendations, or decisions.
Open AI System	An AI system where user inputs may be used to train the model or shared with others. Non-public City data must never be entered into an Open AI System.
Closed AI System	An AI system where user data is isolated, not used to train a shared model, and not exposed to other users. More secure for non-public data — subject to vendor agreement review.
Embedded AI Tool	An AI feature built into City-approved software (e.g., predictive text, AI-powered search). Use within intended functions does not require separate AI Committee approval.
Generative AI	AI systems that generate text, images, code, or other content in response to prompts (e.g., ChatGPT, Microsoft Copilot, Google Gemini).
Non-Public City Data	Information whose disclosure could violate privacy, regulations, or statutes; harm the City's finances or reputation; or undermine operations. Includes personnel files, legal correspondence, and unpublished financial data.
Personal Information	Any information that identifies or could reasonably be linked to a specific individual or household.
Sensitive Information	A subset of personal information including medical, financial, political, racial/ethnic, religious, gender, sexual orientation, or disability data that individuals would reasonably expect to be kept private.
AI-Generated Content	Any output — text, images, code, decisions, or recommendations — produced in whole or in part by an AI system. All AI-generated content requires human expert review before use.

3. Guiding Principles

All AI use at the City of Little Rock must align with the following principles, regardless of the tool, department, or task:

Principle	Requirement
Lawful	AI use must comply with all applicable federal, state, and local laws, regulations, and contractual obligations — including CJIS, HIPAA, PCI-DSS, Arkansas APIPA, and civil rights statutes.
Ethical	AI must be used fairly and without discrimination. Users must actively review outputs for bias and correct findings before any use or publication.
Transparent	AI use must be documented. When AI materially contributes to work products or decisions, that contribution must be disclosed as required by law, contract, or City policy.
Human-Overseen	AI is a tool, not a replacement for human expertise or judgment. All AI outputs must be reviewed by a qualified person before use. No consequential decision may be delegated solely to AI.
Necessary	AI use must serve a valid, documented business purpose. Benefits must be weighed against risks, cost, and alternatives.
Secure & Privacy-Preserving	AI use must comply with the City's data classification and security policies. Data minimization applies — only input what is necessary.
Accountable	AI use must be documented to enable audit and oversight. Named individuals remain accountable for all AI-assisted work — accountability cannot be assigned to the AI.

4. AI Committee and Approval Process

4.1 AI Committee

The AI Committee serves as the City's central governing body for AI adoption. Its responsibilities include reviewing and approving requests for new AI systems, maintaining the Embedded AI Approved Software List, overseeing the AI Use Case Registry, investigating instances of non-compliance, and reporting AI-related risks to City leadership.

To support City users during the rollout of this policy, the Embedded AI Software Exception List will document all AI systems currently in use within the City. These systems may continue to be used temporarily while they undergo review by the AI Committee. Use of any system on the Exception List will be discontinued if the AI Committee issues a disapproval or IT identifies an inherent risk.

Role	Department	Member Name
Chair — CIO	Department of Information Technology	Abdoul Kabaou
Chief Data Officer	Office of Executive Administration	Marquis Willis
Network Security Manager	Department of Information Technology	April Prewitt
Enterprise Architect	Department of Information Technology	TBD
Legal Counsel	City Attorney's Office (CAO)	Sherri Latimer\Reed Edwards
Human Resources	Department of Human Resources	Sheridan Richards
Rotating Department Representative	TBD	TBD

4.2 Approval Process

► All AI systems — except Embedded AI Tools in pre-approved software — require AI Committee approval before use.

Step	Action	Owner	Timeline
1	Submit a New Technology service desk request and attach AI System Use Request Form (Appendix A) to the AI Committee	Requesting employee + Department Director	Before any use
2	AI Committee intake review — assess completeness and flag risks	AI Committee Chair / CISO-Network Security Manager	≤ 5 business days
3	Legal Counsel reviews terms of service and data agreements	City Attorney's Office	≤ 5 business days
4	LRIT/CISO security and data classification assessment	CISO-Network Security Manager	≤ 5 business days
5	AI Committee votes — approved, conditional, or denied with written rationale	AI Committee (majority quorum)	≤ 10 business days of submission
6	Approved uses logged in AI Use Case Registry; requester notified	AI Committee Chair	≤ 2 business days of decision

[Link to AI System Use Request Form: <https://kmanagement.littlerock.state.ar.us/userui/welcome.php>]

[Link to Embedded AI Approved Software List: [AI Governance Tool Register.xlsx](#)]

5. Permitted and Prohibited Uses

5.1 Permitted Uses

The following uses are permitted subject to applicable consultation, approval, data handling, and documentation requirements:

Category	Permitted Activity	Example
Research & Information	Gathering publicly available information, exploring ideas, generating outlines or draft content for human development	✓ "Summarize this public report on traffic safety trends."
Content Drafting	Drafting internal communications, reports, or templates — subject to expert review and editing before use	✓ "Draft a first version of a parks event announcement."
Productivity	Summarizing non-sensitive meeting notes, automating repetitive tasks using public or anonymized data	✓ "Create a meeting agenda template for team planning."
Code Development	Writing or reviewing code — only by individuals with verified coding expertise who review all output before deployment	✓ "Suggest a function to validate email input." (reviewer must have coding expertise)
Training Materials	Developing quizzes, learning resources, or training modules using approved content	✓ "Generate 10 quiz questions on workplace fire safety."
Data Analysis (Anonymized)	Analyzing datasets where all personal identifiers have been removed, using an approved Closed AI System	✓ "Identify trends in this anonymized permit application dataset."

5.2 Prohibited Uses

Unless specifically approved by the AI Committee and Department Director, the following are strictly prohibited:

Prohibited Use	Description	Example of Violation
Inputting Non-Public or Sensitive Data into Open AI Systems	PII, PHI, CJ, financial data, legal correspondence, or any non-public City information must never be entered into an Open AI system	<i>✗ "Analyze this employee's performance review." / "Summarize this police incident report."</i>
Political Lobbying	Generating content aimed at influencing government officials, legislation, or policy	<i>✗ Drafting letters urging opposition to state legislation.</i>
Categorizing by Protected Class	Using AI to identify or score individuals based on race, religion, gender, disability, age, or other protected characteristics	<i>✗ Filtering job applicants by inferred protected class characteristics.</i>
Obtaining Legal Advice	Using AI to generate legal opinions, draft legally binding policies, or substitute for qualified legal counsel. Note: This prohibition applies to non-legal City personnel. Licensed attorneys in the City Attorney's Office are authorized to use approved AI tools for legal research, case analysis, and document drafting within their professional capacity and subject to applicable professional conduct rules.	<i>✗ "Does this clause make our contract binding under Arkansas law?"</i>
Creating Registrable Intellectual Property	Creating IP the City intends to copyright or patent without Legal review of AI ownership implications	<i>✗ Generating an official City logo via AI for public use.</i>
Creating Misleading Content	Generating content that is factually inaccurate, deceptive, or intended to mislead	<i>✗ Using AI to fabricate statistics or policy outcomes in a public report.</i>
Illegal Activities	Any use that violates federal, state, or local law	<i>✗ Using AI to access systems without authorization.</i>
Unauthorized Personal Use	Using City time, devices, or licensed AI accounts for personal purposes without approval	<i>✗ Using a City AI license during work hours for personal projects.</i>

6. Data Classification and AI Use

Before entering any data into an AI system, employees must determine the data's classification and match it to the appropriate AI system type. When uncertain, treat data as Confidential and consult your manager or LRIT.

Level	Examples	Regulations	Open AI	Closed AI
PUBLIC	Published reports, press releases, public policies	None specific	✓ Permitted	✓ Permitted
INTERNAL	Internal memos, non-sensitive departmental data, anonymized datasets	City policy	⚠ Consult manager	✓ With approval
CONFIDENTIAL	Personnel files, legal files, vendor contracts, financial data Note: Licensed attorneys in the City Attorney's Office may use Confidential legal files in pre-approved Closed AI Systems designated for legal research (see Appendix C) without separate Committee approval, subject to attorney oversight, Arkansas Rules of Professional Conduct, and applicable records retention and public records obligations.	APIPA, contractual	✗ PROHIBITED	⚠ Committee approval
RESTRICTED	CJI, PHI, PII, payment card data, SSNs, biometric data	CJIS, HIPAA, PCI-DSS, APIPA	✗ PROHIBITED	✗ PROHIBITED

7. Ethical Guidelines

The City is committed to ethical AI use that reflects its obligations to residents, employees, and the public. These guidelines apply to all AI use, even where legally permissible.

7.1 Integrity and Transparency

Users must be honest about AI's contribution to their work. Do not present AI-generated content as solely your own. Managers and requesting departments must be aware of AI involvement. Seek explicit permission before using AI for sensitive tasks — for example, informing HR before using AI to assist in writing a performance evaluation. AI-generated code must be labeled with the tool used and the human reviewer's name.

7.2 Bias Awareness

AI systems may reflect biases in their training data. All users must actively review AI outputs for bias — especially content related to hiring, personnel matters, or communications targeting specific demographic groups. Identified bias must be corrected before any AI output is used or published.

7.3 Brand Consistency

AI-generated content intended for external or public-facing use must conform to City of Little Rock brand, voice, and communication standards, and must be reviewed by the Communications team before release.

7.4 Intellectual Property

Legal Counsel must review any situation where the City intends to assert ownership over AI-generated content or use it in a legally significant context. Do not input third-party copyrighted content into AI systems without authorization.

8. High-Risk AI Uses

The following AI applications carry elevated risk to individual rights, legal compliance, or public trust. They require AI Committee approval, documented human oversight, and in some cases legal review before deployment.

High-Risk Category	Risk	Required Safeguards
Personal Data in AI Systems	Risk of unauthorized disclosure, re-identification, or regulatory violation	Closed AI System only
Screening Candidates Job	Adverse impact on protected class members; civil rights and equal employment law exposure	HR and Legal co-review; bias testing; human HR makes all final decisions
Personnel Decisions	Amplification of workforce bias; legal and HR liability	HR, Legal, and Director review; human decision-maker must own and document the final call
Law Enforcement Support	Civil liberties, accuracy, and CJIS Policy compliance concerns	CJIS Systems Officer approval; City Manager notification; strict human oversight
Public Benefits / Service Eligibility	Unfair restriction of access to public programs	Legal review; human final decision; documented appeal mechanism
Assessment of Students / Program Participants	Discriminatory scoring; inequitable outcomes	Extreme caution; Committee and HR approval; bias audit; human educator makes final assessment
Enrollment Admission Decisions	Discriminatory outcomes in City program admission	Extreme caution; Legal review; human final decision required

9. Documentation and Tracking

Tracking AI system use is mandatory for all non-Embedded AI tools. Documentation enables audit readiness, institutional knowledge, and oversight accountability. All AI records are subject to the City's records retention and public records obligations.

What to Document	Detail Required	Where
AI System Used	Tool name, vendor, Open vs. Closed classification	AI Use Case Registry
Purpose / Use Case	Brief description of the task	Registry / Departmental records
Data Input Classification	Classification level of data entered	AI Use Request Form ; project file
Human Reviewer	Name and title of the expert who reviewed the output	Work product record ; Registry
AI-Generated Code	Label with AI tool and reviewer name	Code repository comments
Decision Outcome	What decision was made and who was accountable	Project file / HR / department records
Approval Reference	AI Committee approval reference number	AI Use Case Registry

[Link to AI Use Case Registry — [AI_Governance_Tool_Register.xlsx](#)]

10. Third-Party and Vendor AI Use

AI tools used by contractors, vendors, or service providers must be evaluated with the same rigor as internal AI adoption. Vendor use of AI does not exempt the engagement from City policy requirements.

10.1 Requirements

- All contracts involving AI-enabled services must include an AI-specific clause reviewed and approved by City Attorney's Office
- Vendors must disclose what AI tools are used, what City data is processed, and how it is protected
- Vendors processing Confidential or Restricted City data via AI must provide Data Processing Agreements and demonstrate regulatory compliance
- Vendor AI tools are subject to the same data classification restrictions as internal use
- LRIT must assess vendor AI security posture before contract execution

10.2 AI Contract Clause Requirements

The City Attorney's Office will maintain a standard AI addendum for vendor contracts covering: disclosure of AI tools used; data handling and retention obligations; prohibition on training AI models with City data; breach notification requirements; and audit rights. For major enterprise AI platform providers, the City Attorney's Office shall conduct a review of the provider's standard Data Processing Agreement and enterprise Terms of Service in lieu of a City-drafted addendum and shall document the results of that review in the AI Use Case Registry.

[FILL IN — Standard AI Contract Addendum — to be issued by City Attorney's Office]

11. Training and Awareness

All City personnel who interact with AI systems must complete training on this policy along with any LRIT required security awareness training before using any AI tool for City business. Training is refreshed annually and upon material policy updates.

Audience	Content	Frequency	Owner
All Employees	Policy overview, permitted/prohibited uses, data classification, reporting	Annual + upon hire	HR / LMS
AI System Users	Tool-specific training, security awareness, data handling, documentation, bias review	Before first use of each system	Dept. Director / AI Committee / LRIT
Department Directors	Governance, approval process, High-Risk oversight	Annual	CIO / AI Committee
AI Committee	Risk management, regulatory updates, evaluation criteria	Quarterly	CIO /CDO
Legal / Procurement	Contract clause requirements, vendor AI assessment, IP liability	Annual	City Attorney / CIO

[LMS link and completion tracking process]

12. Reporting Non-Compliance

All City employees and agents who become aware of any conduct that may violate this policy are responsible for reporting it — preferably through normal reporting relationships beginning with their manager.

12.1 How to Report

- Report to your direct manager or Department Director
- Report to the AI Committee at innovation@littlerock.gov
- Report to Human Resources or Legal Counsel for sensitive matters
- Anonymous reporting: TBD

12.2 Investigation and Consequences

All reports of suspected non-compliance will be investigated by the AI Committee, Legal Counsel, Human Resources, or other appropriate parties. Employees will not face retaliation for reporting potential violations in good faith. Violations of this policy may result in disciplinary action up to and including termination of employment, and where warranted, referral for legal action.

12.3 Non-Retaliation

The City of Little Rock strictly prohibits retaliation against any individual who reports a suspected policy violation in good faith. Retaliation is itself a serious disciplinary offence subject to the same range of consequences.

13. Policy Maintenance and Review

This policy will be reviewed annually by the AI Committee and the CIO. It will also be reviewed and updated as required following material changes to applicable laws, regulations, City operations, or AI technology. All City personnel are responsible for staying informed of the current version.

Review Trigger	Lead	Timeline
Annual scheduled review	AI Committee + CIO	Within 12 months of effective date
Material change in law or regulation	Legal Counsel + AI Committee	Within 60 days of change
Significant AI incident or near-miss	AI Committee + CISO/Network Security Manager	Within 30 days of incident
Introduction of new high-risk AI use	AI Committee	Before deployment

Department responsible for policy updates: LRIT

Policy repository location: [FILL IN — intranet link]

Appendix A — AI System Use Request Form

► Submit to the AI Committee before using any non-Embedded AI system. All fields are required. Attach the tool's terms of service.

Field	Response
Requestor Name and Title	
Department	
Date of Submission	
AI Tool / System Name	
Vendor / Provider	
Open AI System or Closed AI System?	
Intended Use / Business Purpose	
Data to be Input — Type and Classification Level	
Will any Confidential or Restricted data be used? (Yes / No — explain)	
Named Human Reviewer (must have subject-matter expertise)	
How will AI outputs be reviewed before use?	
Department Director Approval (Name / Signature / Date)	
Terms of Service reviewed by Legal? (Yes / No / Pending)	
Any known contractual restrictions on this tool? (Yes / No — explain)	
Is this a High-Risk use under Section 8? (Yes / No — explain)	

Appendix B — Quick Reference: Do's and Don'ts

✓ ALLOWED	✗ NOT ALLOWED
✓ Summarize a publicly available government report	✗ Summarize a police incident report or CJI record
✓ Draft a first version of a press release (subject to Communications review)	✗ Submit AI-generated content to media without human review and approval
✓ Use AI to generate code — reviewed by a qualified developer before deployment	✗ Deploy AI-generated code without expert review
✓ Analyze anonymized, aggregated traffic data in a Closed AI System	✗ Input employee names, SSNs, or personnel data into any AI tool
✓ Use Microsoft Copilot features within approved M365 apps as intended	✗ Use free-tier ChatGPT for work tasks involving City internal data
✓ Document AI use in the AI Use Case Registry	✗ Use AI for a new task without completing the approval process
✓ Report suspected AI misuse to your manager or the AI Committee	✗ Ignore observed AI policy violations
✓ Seek manager approval before using AI for sensitive HR tasks	✗ Pass off AI-generated work as entirely your own without disclosure

Appendix C — Embedded AI Approved Software List

► Maintained by LRIT/AI Committee. Use of AI features within these tools, for their intended purpose, does not require separate AI Committee approval. This list is updated as tools are added or removed. Last updated: 3/2/2026.

Software / Platform	AI Feature(s) Permitted	Permitted Departments	Notes / Restrictions
Microsoft 365 (Copilot features)	AI-assisted drafting, summarization, Teams meeting recap	All Departments	Do not enable Copilot on documents containing Restricted data
[FILL IN — e.g., Oracle Fusion]	[FILL IN — AI features in use]	[FILL IN]	[FILL IN]
[FILL IN]	[FILL IN]	[FILL IN]	[FILL IN]