

AI Use in Local Government

John Maschman

Iowa League of Cities Annual Conference
September 24, 2026 | Bettendorf



Today's working questions

- 1** Where can AI actually help?

- 2** What becomes a public record?

- 3** What information should never enter a public tool?

- 4** What controls make use defensible?

1 Useful work

Where AI saves time and where human judgment still controls



Generative AI in one sentence

- A tool that predicts and creates text, images, code, audio, or other content from patterns in its training and instructions.
- It can sound confident while producing an incomplete, distorted, or entirely fabricated answer.
- Treat the output as a draft from a fast, inexperienced assistant whose work always needs review.

The practical rule

AI can accelerate the first draft.
A responsible city employee
owns the final work.

Good starting points

- Turn rough notes into a meeting agenda or resident-facing explanation.
- Summarize a long, nonconfidential document and identify questions for staff review.
- Draft routine correspondence, FAQs, job-posting language, or training materials.
- Compare two versions of a policy or reorganize information into a checklist.
- Brainstorm options while keeping the decision with staff and the governing body.

High-risk uses

- Making eligibility, hiring, discipline, enforcement, or benefits decisions about a person.
- Producing legal, engineering, financial, medical, or safety conclusions without qualified review.
- Summarizing confidential personnel, law-enforcement, utility, litigation, or resident information in an unapproved tool.
- Publishing facts, citations, quotations, calculations, or meeting summaries that no one has checked.

Higher stakes

The closer the output gets to a person's rights, public safety, or binding city action, the stronger the review and controls must be.

A safer workflow

1

Classify

What information will the tool receive?

2

Choose

Use an approved account and tool.

3

Constrain

Ask for a draft, not a final decision.

4

Verify

Check facts, sources, math, and omissions.

5

Preserve

Save the record where city policy requires.

The employee remains accountable for the finished work.

2 Public records

AI changes the tool, not the city's Chapter 22 obligations



The public-record question

- Iowa Code chapter 22 covers records “of or belonging to” government bodies and officials in their official capacities.
- Content can qualify regardless of whether it sits in city email, a personal account, a vendor platform, or an AI chat history.
- Focus on the substance and purpose of the record, not the device, account, or file format.

“stored or preserved in any medium”

Iowa Code § 22.1(3)(a)

Ask this

Does this prompt, upload, response, or revision document the transaction of city business?

One task can create several records

- The source document or data supplied to the tool.
- The user's prompt and follow-up instructions.
- The model's response, including summaries or proposed language.
- The edited version circulated internally.
- The final city document and any approval trail.

A city cannot avoid access obligations by using a private vendor.

Iowa Code § 22.2(2)

Scenario: the council memo

A clerk uploads resident emails and staff notes to a free AI service. The tool drafts a council memo. The clerk deletes the chat after copying the memo into Word.

Discuss

What records may exist? What confidential information may have left city control? Which version should the city retain? Who verifies the summary?

Deletion inside the AI service does not answer the legal or records-management questions.

Open-records response

- Search approved city systems and identify whether relevant work occurred in an AI platform.
- Preserve potentially responsive material when a request, claim, audit, or litigation hold arises.
- Review each record for applicable confidentiality rather than withholding everything because AI was involved.
- Explain redactions or denials under the applicable legal authority.
- Coordinate with counsel when prompts or responses mix public and confidential material.

“Ignorance of the legal requirements ... is not a defense.”

Iowa Code § 22.10(4)

3 Confidentiality and security

The most serious risk often begins with what the employee types or uploads



A traffic-light rule for data

GREEN

Public ordinances, published agendas, approved website copy, generic formatting requests

Generally suitable in an approved tool

YELLOW

Internal drafts, operational details, vendor material, nonpublic contact information

Check policy, contract, and necessity first

RED

Attorney-client material, personnel files, protected health or justice data, passwords, security details

Do not enter without express authorization and safeguards

Vendor questions before approval

- Does the provider use city prompts, files, or responses to train its models?
- How long does it retain content, backups, and logs, and can the city retrieve or delete them?
- Where is the data stored and which subcontractors can access it?
- Does the contract address security incidents, audit rights, indemnity, and data return?
- Can administrators control accounts, sharing, plug-ins, and integrations?
- Can the city meet records requests, retention duties, and litigation holds?

Cybersecurity failure modes

- A convincing phishing message drafted with public information about city staff.
- A malicious file or webpage that instructs an AI assistant to reveal or misuse connected data.
- An employee sharing credentials, internal network details, or incident information in a prompt.
- An AI-generated script or configuration deployed without testing.
- An unapproved plug-in gaining broader access than the employee realizes.

Assume exposure

AI tools can amplify familiar risks. Strong identity controls, limited access, testing, and incident reporting still matter.

Minimum technical safeguards

- Approved enterprise accounts with multifactor authentication and centralized administration.
- Least-privilege access to files, email, databases, and external actions.
- Logging that supports incident response, records management, and appropriate oversight.
- Contractual controls for retention, training use, breach notice, deletion, and data return.
- Testing before any AI feature can send messages, change records, publish content, or control equipment.
- A fast way for employees to report an accidental upload or suspicious AI behavior.

Cybersecurity records may be confidential when disclosure could jeopardize life or property.

Iowa Code § 22.7(50)

4 Governance

A short policy, a usable review path, and visible accountability



What the city's policy should cover

- Scope: employees, officials, contractors, accounts, embedded AI features, and automated agents.
- Approved tools and prohibited information, with a process for requesting exceptions.
- Human review requirements tied to the consequence of an error.
- Records retention, public-records searches, litigation holds, and audit access.
- Procurement, security review, incident reporting, and consequences for misuse.
- Periodic review as tools, contracts, laws, and city operations change.

Review matched to consequence

CONSEQUENCE OF ERROR

LOW

Formatting, brainstorming,
public-source drafts

Employee verification

MODERATE

Resident communications, staff
analysis, code or calculations

**Second-person or subject-matter
review**

HIGH

Rights, enforcement,
personnel, safety, binding
action

**Qualified human decision-maker
and documented approval**

Data sensitivity can move any use into a higher review category.

Transparency without theater

- Identify a responsible employee or department for public-facing AI work.
- Disclose AI assistance when it would matter to a reasonable reader or when law, grant terms, or city policy requires it.
- Avoid suggesting that an automated tool made a discretionary government decision.
- Keep enough documentation to explain the sources, review, and approval for consequential uses.
- Provide a practical route for residents and employees to question or correct an output.

A 30-day starting plan

WEEK 1

Inventory current use

Ask departments what tools, accounts, plug-ins, and workflows already exist.

WEEK 2

Set interim rules

Name approved tools, prohibit sensitive uploads, require verification, and identify a contact.

WEEK 3

Review contracts and records

Confirm data terms, retention, access, and how staff will search or preserve official work.

WEEK 4

Train and test

Use real city scenarios, document lessons, and select a small number of low-risk pilots.

Before you press Enter

- 01 Am I using an approved tool and account?

- 02 May I share every item in this prompt or upload?

- 03 Could the prompt or response document city business?

- 04 What harm follows if the answer is wrong or biased?

- 05 Who will verify the facts, sources, math, and omissions?

- 06 Where should the final work and supporting record be saved?

If any answer is unclear, pause and ask.

Questions?

John Maschman

AI Use in Local Government

Thank you

