Legal 101: What to Know About AI and Florida Law

> ***Disclaimer:*** *This article is for general educational purposes and does not constitute legal advice. City officials should consult their city attorney before adopting or using AI tools or responding to public records or Sunshine Law requests involving AI.*

Across Florida, city halls are buzzing with quiet experiments in artificial intelligence. City managers are asking chatbots to draft memos. Finance teams are exploring AI tools that scan budgets for savings. Clerks are wondering whether an AI-generated draft counts as a public record.

It's a moment of possibility and pause. Cities are eager, but cautious, to see what this technology can do without crossing legal lines.

This 101 guide breaks down important Florida-specific legal and ethical questions that city leaders should keep in mind as they responsibly experiment and implement AI tools.

Public Records: When a Prompt Becomes a Document

Florida's public-records law, Chapter 119, Florida Statutes, is famously broad: If it's made or received in connection with official business, it's a record — no matter where it lives or how it was created. That includes AI prompts, drafts, chat logs, and outputs if they document city business.

The takeaway: When an employee uses AI to draft a memo or summarize citizen comments, that content may be subject to disclosure. Even transient messages must follow the same retention rules under the GS1-SL schedule and Rule 1B-24.003, F.A.C.

Think of AI materials in three buckets:

Type	Likely Record Type	Retention Guidance
Quick prompts or test runs	Transitory messages	Retain until obsolete, superseded, or administrative value is lost
Draft reports or letters	Working drafts	Retain until obsolete, superseded, or administrative value is lost
Final outputs or logs supporting a decision	Supporting documentation	Retain under the same schedule as the related case or action

Designate your city clerk (or other official records custodian) as responsible for AI workspaces and logs. That includes deciding where chats live, how they're exported, and how requests will be routed and tracked.

Security information and bona fide trade secrets remain protected by statute (§119.0715), but broad exemptions are rare. When in doubt, save first and ask later.

Sunshine Law: Meetings in the Age of Machines

Florida's Sunshine Law (§286.011) requires public notice and deliberation whenever two or more members of a governing body discuss matters that may foreseeably come before it. Technology doesn't change that.

What to watch out for: If city officials collaborate inside a shared AI workspace that aggregates or circulates their feedback, that may trigger Sunshine Law requirements. Even using an AI "assistant" to pass ideas between members can raise the same concerns the Attorney General has long flagged about staff acting as intermediaries.

A safer option is to use AI individually for research or drafting, and to treat any shared, member-visible AI workspace as you would a collaborative document (i.e., only inside a properly noticed meeting with public access and minutes).

Procurement and Contracts: Clarity Beats Clever Code

As cities begin purchasing AI subscriptions or embedding AI into existing software, procurement laws still apply. Your local purchasing code may set thresholds and notice rules for technology purchases.

When negotiating AI-related contracts, consider raising these questions with counsel:

- Who owns the data the AI system ingests and produces?
- What security standards and certifications apply (e.g., CJIS, HIPAA, NIST controls)?
- What happens when the model changes mid-contract?
- Do indemnity clauses respect Florida's sovereign immunity caps (§768.28)?
- Can the vendor use your city's data to train other models?

For the last question, consider adding an explicit "no training on your data" clause to help your city keep control of its data and exposure. For example:

Vendor shall not use City Data, Derived Data, or Metadata to train, fine-tune, or otherwise improve models for any customer other than City, except as strictly necessary to provide the contracted services within City's dedicated environment.

Privacy, Cybersecurity, and Sensitive Data

Florida's Local Government Cybersecurity Act (§282.3185) and the Florida Information Protection Act (§501.171) require municipalities to safeguard personal information and report breaches promptly. Feeding personally identifiable or confidential data into a public AI tool could violate both.

A simple rule: Do not input PHI (protected health information), CJI (criminal justice information), or confidential, exempt, or otherwise sensitive information into an unapproved AI platform.

HIPAA Do: use AI only inside compliant, access-controlled environments and confirm Business Associate Agreements (BAA) where needed.
HIPAA Don't: paste patient, benefits, or personnel details into public or consumer AI tools.

CJIS Do: ensure police or fire applications meet FBI CJIS Security Policy standards and local controls.
CJIS Don't: export or analyze CJI through non-CJIS-certified vendors or systems.

If an AI system is breached, isolate the environment, preserve logs, and notify your vendor and counsel. Assess whether PII/PHI/CJI was exposed, and meet statutory reporting timelines. The records custodian and city attorney should coordinate on any security-related exemptions for incident materials.

Human Resources: Tread Lightly with Automated Hiring

Federal civil rights and disability laws still govern AI-assisted hiring or promotion. The EEOC warns that algorithmic screening tools count as "selection procedures," meaning cities must avoid disparate impact unless job-related and consistent with business necessity.

Keep humans in the loop, validate that tools are job-related, and document every step. When in doubt, run potential systems through legal review before using them to rank applicants. The same caution should apply to monitoring tools (e.g., productivity, keystrokes, attention analytics).

Copyright and Ownership

If an AI tool drafts text, designs a logo, or generates an image, who owns the resulting work?

Under U.S. law, only human authorship qualifies for copyright, but a city can still hold rights to final works that incorporate AI output edited by a person.

For any creative product (e.g., reports, visuals, code), verify that you have proper licenses and the AI didn't reproduce copyrighted material. When in doubt, treat AI content like stock imagery: useful, but check the fine print.

Liability, Insurance, and Risk Transfer

Florida's sovereign immunity statute (§768.28) caps damages and limits indemnities, so vendors' standard contractual language may exceed those limits and need to be adjusted accordingly.

Many cities are also reviewing how their insurance *generally* treats AI-related risk. For example, does your existing cyber or technology errors insurance cover AI-related incidents, such as data leakage or misinformation? The details vary, but a short call with your risk manager now can prevent surprises later.

Algorithmic Impact Assessments

For higher-risk AI uses — anything influencing eligibility, enforcement, or resident benefits — cities can borrow a page from the NIST AI Risk Management Framework and conduct a brief Algorithmic Impact Assessment (AIA). It's structured common sense. It documents what the tool does, what data it uses, who reviews results, and how accuracy or bias will be monitored. Keeping that file shows diligence and builds public confidence.

The City Attorney's Evolving Role

City attorneys are quickly becoming a go-to resource for AI governance and standards, translating Sunshine Law to AI applications, reviewing procurement clauses, helping classify AI outputs for retention, and coordinating breach response duties under §501.171.

They may also guide cultural change, reminding local officials and staff that, while machines can assist in drafting, humans remain accountable for judgment and legality.

As the Florida Bar's recent opinion on lawyer use of generative AI put it: confidentiality and accuracy still rest with the professional, not the algorithm.

Practical Next Steps

- **Inventory usage.** Ask which departments already use AI informally, then bring those pilots into the open.
- **Name your custodian.** Assign the clerk (or other official custodian) to own AI workspaces/logs.
- **Draft a short internal policy.** Focus on acceptable use, data sensitivity, and record retention. Link it to your computer acceptable use policy.
- **Train staff.** Explain both potential and pitfalls; require fact-checking of every AI output.
- **Coordinate with the clerk and IT.** Build export and retention workflows for AI materials.

- **Plan for changes.** Track potential state and federal-level AI standards that may shape future reporting or governance needs. As rules evolve, treat your AI policy as a living document.

The Road Ahead

Florida's local leaders don't need to be technologists to guide their cities through the AI era. They just need awareness, curiosity, and a healthy respect for existing laws that already cover much of this new terrain.

Used wisely, AI can help a city write faster, analyze better, and serve residents more efficiently. Used carelessly, it can expose sensitive data or erode trust.

The path forward is the same one that built Florida's civic reputation: transparency, accountability, and good governance, now with a digital co-pilot.

Quick Glossary

AI/GenAI: Software that creates text, images, or data analysis from prompts.
AIA: Algorithmic Impact Assessment — a short review of an AI tool's risks.
CJI/CJIS: Criminal Justice Information and the FBI policy governing its security.
PHI/HIPAA: Protected health information and its federal privacy rules.
GS1-SL: Florida's general records schedule for state and local agencies.
FIPA: Florida Information Protection Act — the state's breach notification law.
Sunshine Law: Florida's open-meetings statute ensuring transparency.

Sources: insights adapted from the Florida League of Cities' environmental scan of municipal AI adoption, state statutes (Ch. 119, 286, 282, 501, 768, 1B-24.003 F.A.C.), and federal EEOC, HIPAA, and NIST guidance.