



City of Marco Island – Generative AI Policy

Version 1.2, Last Reviewed: 4/29/25

Prepared by:

Jose Duran, IT Director, City of Marco Island

Mario Blanco, Senior Network Admin, City of Marco Island

AI Task Force Committee, City of Marco Island

1. Purpose

The purpose of this artificial intelligence (AI) policy is to ensure responsible, legal, and ethical use of artificial intelligence technology across City of Marco Island Government. Generative AI is a tool.

We are responsible for the outcomes of our tools. For example, if autocorrect unintentionally changes a word - changing the meaning of something we wrote, we are still responsible for the text. Technology enables our work, it does not excuse our judgment nor our accountability.

2. Scope

This policy applies to all City of Marco Island Government exempt and classified employees, contractors, consultants, temporary employees, and other workers in various city departments.

3. Key Considerations

Includes topics such as Generative AI, Cybersecurity, Privacy, Intellectual Property, and Model Bias.

4. Transparency

City of Marco Island will strive to ensure transparency of AI technologies used for decision-making and significant communications or content creation. This includes providing clear information to individuals about the use of AI systems, their purpose, and their potential impact.

5. Fairness

The use of AI technologies within City of Marco Island will be guided by principles of fairness. Reasonable measures will be taken to prevent bias and discrimination in AI systems and to ensure that any future insights developed through the use of AI are free from unfair or unjust biases.

6. Accountability

City of Marco Island employees are accountable for the responsible use of AI technologies. Specific roles and responsibilities will be assigned as follows:

- Department Heads are responsible for approving AI use cases within their departments and ensuring compliance with policies.
- Employees must critically evaluate AI-generated content and remain accountable for the final output. AI must support—not replace—human judgment.
- Employees must not input confidential, sensitive, or personally identifiable information into public or unapproved AI tools.

7. Privacy and Data Protection

City of Marco Island will prioritize the protection of individual privacy and personal data in the use of AI technologies. All applicable data protection laws and regulations will be adhered to, and appropriate safeguards will be implemented to protect sensitive information on city approved AI platforms.

8. Security

Employees are responsible for ensuring the secure use of AI systems implemented within the City of Marco Island. Under no circumstances should employees input any personal identifiable information (PII) into unknown or unapproved AI platforms. All approved AI systems will be used in accordance with established security protocols to prevent unauthorized access, data breaches, and other potential security risks.

9. Ethical Considerations

The ethical discussion will be held by the AI Task Force. The City of Marco Island will ensure that AI technologies align with community values and goals. The AI Task Force will lead ethical discussions as needed and consider public input when AI is used in sensitive areas.

10. Policy Guidelines

Security, Confidentiality, Transparency, Ethical Use, AI Chatbot Standards, and Legal Compliance are outlined to ensure responsible AI usage.

11. Acceptable and Prohibited Use Cases

- **Under no circumstances shall employees enter, upload, or share any Personal Identifiable Information (PII)**—including but not limited to names, addresses, phone numbers, Social Security numbers, financial records, health information, or any other sensitive data—into OpenAI systems or any publicly accessible AI platform.
- This includes but is not limited to tools such as ChatGPT, DALL·E, or other generative AI platforms not hosted internally or under the City’s direct control.
- Any use of AI Platforms hosted outside of the United States is strictly prohibited.
- The use of **closed/internal AI systems**—those managed, hosted, or contracted under secure environments by the City of Marco Island or trusted vendors—is permitted.
- PII may be processed in city approved closed systems only if such processing is authorized, secure, and compliant with data governance protocols.

12. Public Records Request (PRR) Compliance

Any work performed using AI platforms—including inputs, outputs, and related data—is subject to public records laws and is the responsibility of the city employee to properly store and retain these records. This information may be disclosed in response to a Public Records Request (PRR) and must be documented and retained in compliance with applicable records retention policies (For further guidance on records retention, please contact the City Clerk).

13. Legal Compliance

Employees and contractors must comply with all applicable AI laws, regulations, and standards. This includes, but is not limited to, the Health Insurance Portability and Accountability Act (HIPAA) for the protection of medical and health-related data, and other privacy laws governing the handling of Personally Identifiable Information (PII). The Police Department’s use of AI must align with Criminal Justice Information Services (CJIS) standards and operate within a closed AI system to ensure compliance with security, confidentiality, and data integrity requirements.

14. Non-Compliance

Violations of this policy may lead to disciplinary action, termination, or legal consequences.

15. Definitions

Generative AI (GenAI):

AI that creates new text, audio, or images from large datasets in response to user prompts. It powers tools for example: ChatGPT, CoPilot, Google Gemini or features in apps like Microsoft Office.

Large Language Model (LLM):

A type of GenAI trained on massive text datasets to generate human-like language, perform translation, and summarize content. LLMs can mimic human writing and require responsible use due to their societal impact.

Hallucinations:

When AI gives confident but false answers. This can mislead users, especially given society's tendency to trust automated systems. Unchecked AI output can harm the City's credibility.

Cybersecurity:

AI tools can increase risk of cyber-attacks if not properly secured, potentially exposing sensitive data.

Confidentiality and Privacy:

Entering private or sensitive data into public AI tools risks that information being retained or reused, potentially exposing it in other users' results.

Model Bias:

AI reflects biases in its training data, which can lead to unfair or discriminatory results that conflict with organizational values.

Intellectual Property:

AI outputs may include copyrighted or proprietary content. Using such content without verification can pose legal risks for the City.

Transparency Risk:

Lack of disclosure about AI-generated content may erode public trust, especially when AI plays a major role in influencing perception.

Personally Identifiable Information (PII)

Pertains to any data that directly or indirectly identifies an individual, including but not limited to: names, addresses, email addresses, phone numbers, Social Security numbers, financial account information, biometric data, IP addresses, and any other data that can reasonably be linked to a specific individual.

16. Acknowledgements

The development of these guidelines has benefited from the contributions of the AI Task Force Committee which includes. Matthew Hayes, Emily Iacobucci, Ray Leshinger, Zurima Luff, Stuart McElvey, Josh Ooyman, Heather Reed, Daniel Zuzunegui. City Clerk: Joan Taylor.