Jefferson County

Employee Administrative Rules & Regulations

Acceptable Artificial Intelligence Usage Rule

Rule Number: **5.5.2025**
Date Established: **4.22.2025**

1.0 PURPOSE

The purpose of Jefferson County Commission's (JCC) Acceptable Artificial Intelligence (AI) rule is to ensure legal and ethical use of AI technology. The guidance below defines acceptable and prohibited uses and outlines employee obligations related to the use or development of AI/GenAI models and applications. This rule applies to any data system, software, hardware, application, tool or utility that operates in whole or in part using AI, and any users & developers (employees, contractors, executives, elected officials, third parties) with access to county data or systems.

Jefferson County Commission recognizes that the use of AI solutions has the potential to provide significant benefits to JCC by enabling employees to work more effectively and efficiently. In cases where the use of AI can help users to do so, users are allowed to use approved AI technologies in accordance with the requirements and guidelines set forth in this policy. The use of AI should always be subject to careful consideration and evaluation to ensure that it aligns with the Commission's values, goals and best practices.

2.0 DEFINITIONS

Algorithm: A set of rules or instructions given to an AI, neural network, or other machine to help it learn on its own; an algorithm is a process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer.

Artificial intelligence (AI): endeavors to replicate core cognitive functions within computer systems. This involves endowing computers with the capacity for learning, reasoning, problem-solving, perception, and natural language understanding.

AI Hallucination: An instance where a generative AI model generates incorrect or nonsensical output that is not supported by its training data.

Deep Learning: A subfield of machine learning that uses artificial neural networks with multiple layers to extract higher-level features from raw input data.

Deep Fake: The creation and manipulation of audiovisual media using advanced artificial intelligence and machine learning technologies, particularly deep learning, to generate or alter human likenesses and voices in a manner that appears realistic. This includes, but is not limited to, the synthesis of human facial or vocal characteristics to create entirely new, false representations or

the alteration of existing media to create misleading or untruthful portrayals. The term encompasses both the technology used for such purposes and the resultant media.

Ethical Artificial Intelligence (Ethical AI): Refers to the development and deployment of AI systems in a way that aligns with human values, moral principles, and societal well-being.

Generative AI (GenAI): technology that creates new content resembling human-created content (including text, images, voices, and videos) in response to user prompts.

Large Language Model (LLM): A deep learning algorithm that can recognize, summarize, translate, predict, and generate text and other content based on knowledge gained from massive datasets.

Machine Learning (ML): A type of AI that allows software applications to become more accurate in predicting outcomes without being explicitly programmed to do so. Machine learning algorithms use historical data as input to predict new output values.

Privacy, Security and Confidentiality: Information is shared with an AI tool by user prompts, or a series of instructions or questions for the tool. Generally, providing access to information constitutes sharing data with the tool. The sharing of data potentially makes confidential or sensitive information public as the tool may train its model on the data shared. In some cases, data that has been anonymized could be linked to personal information and become exposed. Any citizen or employee personal information, data categorized as sensitive information or intellectual property, or otherwise confidential information entered into the prompt may appear in other users' output. Therefore, users of AI should avoid entering any information into an AI tool which they do not want to be made public or is otherwise restricted by law or rule.

Responsible Artificial Intelligence (Responsible AI): A comprehensive approach to the development, deployment, and use of AI systems that prioritizes ethical principles and societal well-being while also focusing on practical implementation and governance.

3.0 PROCEDURE

Any use of AI/GenAI, via platforms, tools, and software must be consistent with JCC code of conduct, county rules, and applicable law. Use of AI/GenAI on County devices must be limited to business purposes. Use of AI/GenAI tools on personal devices or personal accounts to conduct County business is prohibited.

This table is not inclusive of all possible use cases and if a use case is not specifically listed, a user should ask before proceeding. We reserve the right to make changes to, or update this table periodically:

Accepted Use	All Other Use
-The following use cases are permitted: • Translating text from a secondary, publicly available source	-All other use requires preauthorized approval. -To request approval, please submit the request via the JCC Support Portal

• Conducting high-level background research into a non-sensitive topic • Brainstorming ideas for technical solutions or viable options	

For any use of AI/GenAI applications, employees must adhere to the following:

3.1 To maintain the security of JCC's data and IT systems, the Information Technology Services Department will maintain a list of approved AI/GenAI tools on the JCC Support Portal. Accessing unapproved AI applications is prohibited when using County's systems, networks, or conducting business on behalf of the County, or when using the County's data.

To avoid potential data leaks or security incidents:

- **Do not** use County credentials, email addresses, or telephone numbers as a login to publicly available AI applications.
- **Do not** install non-approved Application Programming Interfaces (APIs), plug-ins, connectors, or software related to AI systems.
- **Do not** implement or use in any way code generated by AI on County systems.
- **Do not use AI recording or transcription tools not vetted by ITS.** Many of the AI recording and transcription tools maintain usage rights to all data acquired by the tools.
- Any use of embedded AI within vendor managed or hosted solutions shall be disclosed to the IT Department and the County Manager.

3.2 To maintain the confidentiality of JCC's sensitive information, **do not input county data categorized as *sensitive* or *restricted* into AI applications** per the county's Data Classification Security Rules & Regulations, which can be found in the Information Security Rules & Regulations.

- Contact infosec@jccal.org if you have questions about whether the data you are using is classified as sensitive or restricted.

3.3 To maintain transparency with citizens and employees and protect the County from claims against copyright infringement and/or theft of intellectual property, all AI generated content must be cited and fact-checked.

- Clearly cite any use of AI/GenAI when using the content.
  - For example, "*A common example of alliteration is the child's tongue twister "Peter picked a peck of pickled peppers" (ChatGPT, 2025)."*
  - Another example, "This document was drafted with support from ChatGPT. The content was edited and fact-checked by county staff."
- Fact-check all information with trusted verifiable sources. (county resources, newspapers, research papers, etc.)
- Check for possibly copyrighted information using free online plagiarism tools.
- Notify the respective Department Head and County Manager when AI tools are used to author official Jefferson County Commission documentation, including communications
- AI shall not be used to generate or alter human likenesses and voices in a manner that appears realistic, i.e. deepfakes, for the purpose of misrepresentation, spreading misinformation or other malicious or unlawful purposes.

3.4 To protect JCC employees and constituents from harm, and to protect the County from reputational damage, employees must use AI/GenAI pursuant to the County's code of conduct and non-discrimination policies. AI-created content that is inappropriate, not considered ethical AI nor responsible AI, discriminatory or otherwise harmful to JCC employees or citizens must not be used for work purposes. Such use will result in disciplinary action, up to and including termination.

To protect JCC employees, citizens, and the County:

- **Verify all AI/GenAI Output via knowledge or other sources:** Outputs created by AI/GenAI tools may provide fictitious answers, these are sometimes referred to as hallucinations. Furthermore, many open-source AI/GenAI models are often trained on large, publicly available datasets (e.g., through data extraction of public webpages). The outputs may therefore contain copyrighted information, or others' intellectual property. While ownership in many of these cases is unclear, users should err on the side of caution and not use any output that contains material they suspect to be under copyright protection in any materials, internal or externally facing.
- Users of AI/GenAI tools must also be aware that those tools incorporate biases of the data sets that were used to train them. This modeling bias may not always align with Jefferson County Commission's core values. Therefore, model output may make systematic errors or favor certain groups, leading to unfair or discriminatory outcomes. Users of AI must adhere to existing review processes where AI/GenAI is used to make decisions or provide analysis of information that may be subject to bias. Using output from AI/GenAI tools without reviewing it for accuracy places the County at risk and may harm the County's reputation with the general public and constituents.
- Do review the output of AI/GenAI applications to make sure it meets County's standards for principles of equity, ethics, and appropriateness.
- Do not use any output that discriminates against individuals on the basis of race, color, religion, sex, national origin, age, disability, marital status, political affiliation or sexual orientation.
- Do not use AI/GenAI applications to create text, audio, or visual content for purposes of committing fraud or to misrepresent an individual's identity.
    - Do not use AI/GenAI to create a deepfake, to misrepresent the county or others.

3.5 All employees and contractors are expected to comply with applicable laws, regulations, and JCC policies regarding the use or development of AI/GenAI content or tools.

3.6 All third-party contracts for organizations that will have access to county data should incorporate language restricting the use of county data in AI tools.

3.7 <u>Evaluation and Procurement of Proposed AI tools</u>

The County shall conduct a thorough evaluation using established processes and procedures before acquiring any AI or GenAI solution. Evaluation criteria shall include:

- Assessing the vendor's reputation for security, reliability and protection of intellectual property rights.
- Evaluating the solutions compatibility with existing systems.

- Ensuring compliance with relevant data privacy laws. Reviewing the vendor's commitment to responsible AI.

- Procurement decisions shall prioritize vendors that prioritize security, privacy, respect for intellectual property rights and transparency in their AI solutions. Appropriate language shall be added to contracts to address vendor's obligations.

4.0 MONITORING

Jefferson County Commission Information Technology Services Department reserves the right to access and monitor AI/GenAI applications used on any County-issued devices or appearing on County managed networks to ensure compliant use of these systems.

5.0 FAILURE TO COMPLY

Users who fail to comply with any provision of this Rule may be subject to discipline up to and including termination of employment. If a contractor's agreement includes provisions restricting the use of Generative AI, violations of those specific provisions may be considered a breach of contract and result in removal from assignment. Any AI-related activities which appear to violate applicable laws will be reported to external law enforcement. If monitoring systems and processes detect a possible rule violation or if a User reports a possible rule violation, the suspect event should be processed using appropriate security incident response processes (see the Cybersecurity Incident Response Rule).

6.0 ROLES AND RESPONSIBILITIES

Role	Responsibilities
Information Technology Advisory Board (ITAB), Compliance Department, Risk Management, County Attorney	Review and approve AI applications or non-approved uses.
ITS Governance Compliance Team County Attorney	Develop and manage the AI rule Answer any rule-related questions escalated from managers Manage ethics and integrity misconduct investigations resulting from the use of AI (e.g., generated content, allegations of harassment of employees, IP loss) Support IT Security incident response for investigations that involve data leaks or breaches resulting from the use of AI.
ITS Information Security Group ITS Governance	Manage access to AI if tools require registration and are owned at the enterprise level Conduct security risk assessments for AI applications and use cases Monitor all use of AI
ITS Governance	Conduct privacy risk assessment for AI applications and use cases

All Managers	Conduct review of specific uses of AI that have been escalated to them for review. Assist employees with escalating questions on AI to subject matter experts. Escalate questions on rule to compliance team when necessary. Ensure that AI-generated content is appropriately labeled as such in all media
Employees	Review all AI output for bias, accuracy, and appropriateness Review policies and procedures on an annual basis (i.e., mandatory training).