MILWAUKEE POLICE DEPARTMENT

STANDARD OPERATING INSTRUCTION

682 - GENERATIVE ARTIFICIAL INTELLIGENCE

ISSUED: January 23, 2026	**EFFECTIVE:** January 23, 2026	**REVIEWED/APPROVED BY:** Assistant Chief Craig Sarnow **DATE:** November 19, 2025
ACTION: Creates SOP		**WILEAG STANDARD(S): 6.1.2**

682.00 PURPOSE (WILEAG 6.1.2)

This generative artificial intelligence (AI) policy is intended to promote responsible and ethical usage of AI technologies within the Milwaukee Police Department. It aims to provide guidelines and principles for the proper and secure application of generative AI to enhance work efficiency while mitigating risks and ensuring accountability. This commitment ensures compliance with all relevant laws and regulations, while upholding public trust, civil liberties, and the values of transparency, accountability, and fairness.

682.05 POLICY

A. This policy establishes clear and consistent guidelines for the responsible development, acquisition, deployment, and use of AI technologies within the department. The policy ensures AI is used in ways that enhance public safety while preserving individual rights and community trust.

B. The use of generative AI systems carries unique benefits for law enforcement, providing ways to increase operational efficiency, enhance department procedures, and improve the overall effectiveness of the Milwaukee Police Department.

C. The prompts input into generative AI systems can present risks to both individuals and the department by making accessible to the public information such as department tactics, investigative and training techniques, confidential information (e.g., confidential informants, protected information), active investigations, and security procedures. In addition, without safeguards in place, generative AI can produce unintended discriminatory or biased output as well as content that is inaccurate, misleading, or copyrighted.

D. Any function carried out by a member of the department using generative AI is subject to the same laws, ordinances, and policies as if carried out without the use of generative AI. The use of generative AI does not permit any law, ordinance, or policy to be bypassed or ignored.

E. It is the policy of the department to develop, implement, and use generative AI ethically and responsibly in a way that minimizes potential risk and harm in accordance with the guidelines set forth below.

682.10 DEFINITIONS

A. ALGORITHM

Sets of instructions, such as mathematical operations or logical rules, that dictate how a machine processes data.

B. ARTIFICIAL INTELLIGENCE (AI)

Encompasses machines performing tasks that typically require human intelligence. This is the overarching field of technology that includes generative AI.

C. BIAS

Systematic error that results in unfair outcomes, particularly against protected classes.

D. GENERATIVE AI

Refers to machine learning systems capable of automatically creating content such as text, audio, or images.

E. HUMAN OVERSIGHT

Human monitoring and ability to intervene in AI decision-making.

F. MACHINE LEARNING

A subset of AI in which computers learn tasks through algorithms by analyzing data and patterns.

682.15 RESPONSIBILITIES

A. CHIEF OF POLICE

Prior to the use, implementation, or development for any department functions pertaining to AI systems, their acceptable use and authorized user group shall be approved at the discretion of the Chief of Police, or designee.

B. AI COORDINATOR

1. The Chief of Police, or designee, shall appoint department members to an AI committee to be led by an AI coordinator. The AI coordinator shall report to the inspector of the Administration Bureau.

2. The AI committee shall meet at least bi-annually, or as otherwise directed by the Chief of Police, or designee.

3. The responsibilities of the AI coordinator and AI committee shall include, but are not limited to, the following:

a. Evaluating potential generative AI systems and recommending those generative AI systems that appear to be appropriate and trustworthy to the Chief of Police, or designee. The trustworthiness of generative AI systems should be evaluated by balancing the following characteristics:

1. Validity and Reliability

   The system's apparent ability to meet the intended purpose and fulfill the needs of the department consistently over time.

2. Safety

   Any apparent risk to human life, health, property, or the environment that could result from the department's use of the system.

3. Security and Resiliency

   The system's capability to prevent unauthorized access and misuse and its ability to return to normal function should misuse occur.

4. Accountability and Transparency

   The ability to track and measure the system's use and activity through histories, audit logs, and other processes to provide insight about the system and identify potential sources of error, bias, or vulnerability.

5. Explainability and Interpretability

   The ability of the user to understand the purpose and impact of the system, how and why the system reached the resulting output, and what the output means for the user.

6. Privacy

   The ability of the system to protect confidentiality and meet applicable privacy standards for the types of data intended to be input into the system (e.g., state privacy laws, Criminal Justice Information Services (CJIS)).

7. Fairness

   The ability of the system to operate in a way that avoids or minimizes bias and discrimination.

b. Ensuring appropriate contractual safeguards are in place to manage third-party use of department data and to restrict the use of input in AI training data sets. If the input of protected information is necessary for the proper use of the generative AI system, an information-exchange agreement in compliance with applicable rules and standards (e.g., CJIS requirements) should be used to outline the roles, responsibilities, and data ownership between the department and third-party vendor.

c. Coordinating with others within the department as appropriate to ensure generative AI systems are procured, implemented, and used appropriately. This shall include a legal review by the Risk Manager to ensure any generative AI systems comply with applicable local, state, and federal laws including civil rights protections, data privacy regulations, and public safety statutes.

d. Maintaining a list or inventory of department-approved generative AI systems and, when appropriate for department transparency, making the list or inventory available to the public.

e. Developing and maintaining appropriate procedures related to the use of generative AI systems, including procedures for editing and fact-checking output.

f. Ensuring any public-facing generative AI systems notify the user that generative AI is being used.

g. Developing and updating training for the authorized users of each department approved generative AI system.

h. Ensuring access to department generative AI systems is limited to authorized users and establishing requirements for user credentials (e.g., two-factor authentication, appropriate password parameters).

i. Conducting audits at reasonable time intervals for each of the generative AI systems utilized by the department to evaluate the performance and effectiveness of each approved system and to determine if it continues to meet the department's needs and expectations of trustworthiness.

    1. These audits must ensure each of the generative AI systems are tested for biased outcomes and data used to train these generative AI systems is diverse and representative of the Milwaukee population.

    2. Any identified biases must be promptly addressed with technical and procedural remedies.

j. Ensuring each generative AI system is updated and undergoes additional training as reasonably appears necessary in an effort to avoid the use of outdated information or technologies.

k. Keeping abreast of advancements in generative AI and any generative AI-related legal developments. Reviewing this policy and department practices and proposing updates as needed to the Chief of Police, or designee, and the Office of Management, Analysis, and Planning (OMAP).

682.20 PRINCIPLES FOR USING GENERATIVE AI

A. PRIVACY

It is imperative members understand the privacy policies of AI tools, including how data is collected, used, and protected. Members shall:

1. Ensure all submissions comply with privacy laws and department policies.

2. Be mindful that AI-generated outputs may sometimes contain unintended personal information from other users.

3. Always carefully review and remove private or sensitive data before sharing or publishing the results.

B. ACCURACY

Members shall thoroughly fact-check all AI-generated content before use or distribution. Members shall ensure the accuracy and reliability of the content by cross-checking with reliable sources. Members shall use AI-generated content as a supplement to human expertise and review and edit the content to meet department policies.

C. TRANSPARENCY

Transparency is key when using generative AI to ensure accountability and trust. Members must indicate when they are employing generative AI tools, which often includes citing AI's contribution to the creation of any product. This transparency allows others to differentiate between AI-generated content and human work. Being transparent also involves providing clear explanations of how AI systems function, what data they rely on, and any limitations or biases in their outputs.

D. EQUITY

AI system responses are based on patterns and relationships learned from large datasets derived from existing human knowledge. These datasets may contain errors and historical biases related to race, sex, gender identity, ability, and other factors.

1. Users of generative AI need to be mindful that such systems may make assumptions based on past stereotypes and require correction.

2. Additionally, the algorithms responsible for parsing and processing content may introduce biases. Bias identification, management, and mitigation must be considered at all stages of the generative AI development lifecycle, including designing, developing, deploying, evaluating, using, and auditing.

3. Members must carefully evaluate any content generated by generative AI systems or applications to identify inaccuracies and mitigate unintended or undesirable biases.

Note: Members shall be cognizant of SOP 001 Fair and Impartial Policing when evaluating any content generated by generative AI systems or applications.

E. ACCOUNTABILITY

1. It is crucial to ensure the responsible and ethical use of generative AI. Members are responsible for verifying that AI-generated content is accurate, appropriate, and compliant with department policies before it is used or shared publicly. This includes disclosing any AI involvement in creating content or providing analysis.

2. Misuse of AI, failure to disclose its use, or negligence in fact-checking can erode public trust and violate department policies. Prioritizing transparency and careful oversight help uphold the integrity of the department and reinforce our commitment to accountability within the community.

682.25 USE OF GENERATIVE AI

A. The use of department generative AI systems by department members shall be limited to official work related purposes, and members shall only access and use generative AI systems for which they have been authorized and received proper training.

B. Members shall use AI-generated content as an informational tool and not as a substitution for human judgment or decision-making. Members should not represent AI-generated content as their own original work.

C. AI-generated content should be considered draft material only and shall be thoroughly reviewed prior to use. Before relying on AI-generated content, members should:

1. Obtain independent sources for information provided by generative AI and take reasonable steps to verify that the facts and sources provided by generative AI are correct and reliable.

2. Review prompts and output for indications of bias and discrimination and take steps to mitigate its inclusion when reasonably practicable.

3. Include a statement in the final document or work product that generative AI was used to aid in its production.

D. Prior to taking any law enforcement action based on information from an AI system or tool, the information shall be verified by a human person. Human operators must understand system functionality and have the authority to override AI decisions when necessary.

E. Members shall not opt-in to their data being used, or share any department data, to help an AI system learn unless contractual safeguards are put in place.

682.30 PRIVACY CONSIDERATIONS

Information not otherwise available to the public, including data reasonably likely to compromise an investigation, reveal confidential law enforcement techniques, training, or procedures, or risk the safety of any individual if it were to become publicly accessible, should not be input into a generative AI system unless contractual safeguards are in place to prevent such information from becoming publicly accessible.

1. Members should instead use generic unidentifiable inputs, such as "suspect" or "victim," and hypothetical scenarios whenever possible.

2. Protected information should only be input into generative AI systems that have been approved for such use and comply with applicable privacy laws and standards.

3. Unless contractual safeguards are in place to protect the privacy of all persons (e.g., victims, suspects, witnesses, etc.) members are prohibited from uploading any sensitive information into a publicly accessible AI platform including:

   a. Personally Identifiable Information (PII).

   b. Criminal Justice Information (CJI) database information.

   c. Health Insurance Portability and Accountability Act (HIPPA) information.

682.35 PROHIBITED USE

A. Members shall not use generative AI systems to rationalize a law enforcement decision, or as the sole basis of research, interpretation, or analysis of the law or facts related to a law enforcement contact or investigation.

B. Members shall not create user accounts in their official capacity or input work-related data (including information learned solely in the scope of their employment) into publicly available generative AI systems unless the system has been approved by the Chief of Police, or designee, for the intended use.

C. Members shall not use generative AI systems to categorize individuals by race, ethnicity, religion, or other protected characteristics.

D. Members shall not use generative AI systems to conduct surveillance without appropriate legal authority.

682.40 TRAINING

A. The AI coordinator shall ensure that all members authorized to use generative AI have received appropriate initial training that is suitable for their role and responsibilities prior to their use of generative AI and receive periodic refresher training.

B. Training should include, but is not limited to the following, and may be communicated through methods such as in-service training or roll call memorandums:

1. A review of this policy.

2. The need for human oversight of generative AI outputs.

3. The interpretation, review, and verification of generative AI output.

4. Checking generative AI output for bias or protected information.

5. Ethical use of generative AI technology.

6. Data security and privacy concerns.

682.45 TRANSPARENCY

A. The department will engage with the community to explain AI use, listen to concerns, and ensure technology enhances, not undermines, public confidence.

B. The department will ensure transparency in the operation of AI systems by conducting presentations for the Common Council, Public Health and Safety Committee, and Fire and Police Commission as requested. During these presentations, the department will:

1. Disclose the use of generative AI systems to the public.

2. Explain system functionality and decision logic.

3. Solicit and listen to feedback from the public, elected officials, and members of the Fire and Police Commission.

JEFFREY B. NORMAN
CHIEF OF POLICE

JBN:mfk