


Policy Title:		Artificial Intelligence and Machine Learning – Acceptable Use	
	OFFICE OF THE CHIEF INFORMATION OFFICER	Category	Information Technology Services
		Administrative Policy #	
		Revision #	N/A
		Review Frequency	As Needed – no less frequently than annually
Administrative Division	Information Technology Services (ITS)	Reviewed By	Chief Information Officer; Human Resources Director
BOWC Approval		Last Reviewed/Update Date	
Implementation Date		Resolution No.	

TABLE OF CONTENTS

1. OBJECTIVES	1
2. PURPOSE	1
3. DEFINITIONS	1
4. SCOPE	2
5. RESPONSIBILITIES	2
5.1 Information Technology Services	2
5.2 Management	2
5.3 Employees	2
5.4 Human Resources	2
6. POLICY	2
6.1 Alignment with Business Objectives	2
6.2 Ethical AI Usage	3
6.3 Data Privacy and Security	3
6.4 Responsible AI Development	3
6.5 Approval Process	4
6.6 Monitoring and Reporting	4
6.7 Training and Awareness	4
6.8 Guidelines for AI Use by DWSD Employees	4

6.9 Prohibited Use for AI Systems	4
6.10 Accountability	5
6.11 Compliance and Violations	5
6.12 Reasonable and Necessary Accommodations.....	6

1. OBJECTIVES

- 1.1. To ensure that Artificial Intelligence (AI) and Machine Learning (ML) technology aligns with and enhances the Detroit Water and Sewerage Department's (DWSD) business goals.
- 1.2. To maintain transparency, ethics, and accountability in AI and ML usage.
- 1.3. To protect Sensitive Data and information from misuse.
- 1.4. To promote responsible AI and ML acquisition, development, and deployment.
- 1.5. To ensure that any AI tools are assessed to mitigate certain ethical, legal, and other risks before implementation.

2. PURPOSE

- 2.1. The purpose of this policy is to ensure that AI and ML technologies are used in ethical, transparent, and useful ways at DWSD, and that they are used with the knowledge and approval of DWSD's Information Technology Leadership Board. AI plays a vital role in automation as it develops and integrates with situational awareness and analytics systems, intelligent robotics, and software-defined capabilities applied to asset management, network operations, and systems optimization. AI will also play a key role in field service, customer service, legal, and most other commercial and support operations, as this will increasingly be sought across the utility value chain (supply, transmission, distribution, retail, and end-use) and all utility commodity products.

3. DEFINITIONS

“Artificial Intelligence (AI)” means a combination of technologies that can include machine learning. AI systems perform tasks that mimic human intelligence, such as learning from experience and problem-solving. AI makes its own decisions without human intervention.

“ChatGPT” means an AI-powered chatbot application built on OpenAI's GPT implementation that accepts text prompts to generate text-based output.

“Generative AI (Gen AI)” means a subfield of AI that focuses on creating models and algorithms capable of generating new content, such as images, text, music, or even videos. It involves training AI models to learn patterns and characteristics from existing data, then using that knowledge to generate new content that resembles the original data.

“Machine Learning (ML)” means systems that learn from experience and without explicit instructions. They learn patterns from data, then analyze and make predictions based on past behavior and the patterns learned.

“Natural Language Processing (NLP)” means a subset of AI that involves the machine interpretation and replication of human language. NLP focuses on the study and analysis of linguistics and other AI principles to create an effective method of communication between humans and machines/computers.

“Responsible AI” means guiding principles to govern the development, deployment, and maintenance of AI applications. They also provide human-based requirements that AI

applications should address, including safety and security, privacy, fairness, bias detection, explainability and transparency, governance, and accountability.

“Sensitive Data” means data which are classified as DWSD-Critical or DWSD-Restricted per DWSD’s Data Classification Policy.

4. SCOPE

4.1. This policy applies to all DWSD employees, contractors, student interns, volunteers, and other persons authorized to use DWSD’s computer and technology resources.

5. RESPONSIBILITIES

5.1. Information Technology Services

5.1.1. The Chief Information Officer (CIO) is responsible for developing and updating this policy as needed, no less frequently than annually.

5.1.2. Information Technology Services has the authority to disable any equipment or services that are in violation of this policy.

5.2. Management

5.2.1. DWSD management is responsible for the actions of its staff, contractors, and volunteers and must ensure that all standards applicable to each division’s unique circumstances are followed and alert Human Resources when a violation has occurred.

5.3. Employees

5.3.1. All DWSD computer and technology resource users are responsible for being familiar with and fully complying with this policy.

5.3.2. All DWSD computer and technology resource users are expected to exercise good judgment and act in a professional manner when using DWSD-approved AI and ML technology resources.

5.3.3. Effective security is a team effort involving the participation and support of every DWSD employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly

5.4. Human Resources

5.4.1. Human Resources is responsible for approving and/or implementing any disciplinary action for employees who do not comply with this policy.

6. POLICY

6.1. Alignment with Business Objectives

6.1.1. AI initiatives must be directly aligned with DWSD’s business objectives and strategies.

6.1.2. AI projects will be approved only if they contribute to the goals of DWSD, such as efficiency, productivity, customer satisfaction, or innovation.

6.2. Ethical AI Usage

- 6.2.1. All AI activities must adhere to ethical principles, including fairness, transparency, accountability, and privacy as outlined in DWSD's Ethics Policy.
- 6.2.2. AI systems must not be used for activities that violate any DWSD policies.

6.3. Data Privacy and Security

- 6.3.1. AI applications must adhere to DWSD's Information Security Policy and Data Classification Policy.
- 6.3.2. Sensitive Data should only be used for AI purposes with appropriate consent from a supervisor or Human Resources, and encryption security measures in place, with the understanding that the data may be ingested by the AI's public model and become available in that model once used.
- 6.3.3. As with any online system, personal information should not be entered into an AI tool or service unless a contract is in place with the supplier and covers how the information will be used and protected. Before using an AI tool, the Business Unit must also make sure that the collection and use of personal information, including information used to train the tool, meet their privacy obligations.
- 6.3.4. AI systems are subject to novel security vulnerabilities that need to be considered alongside standard cybersecurity threats. With the rapid pace of development of AI, security will be a core requirement--not just in the development phase, but throughout the life cycle of the system. DWSD's Information Technology Department ("IT Department") and the CIO will develop guidelines that are broken down into four key areas within the AI system development life cycle: secure design, secure development, secure deployment, and secure operation and maintenance.

6.4. Responsible AI Development. Subject to the Approval Process in Section 6.5 of this policy, AI systems must be developed, acquired, and deployed responsibly to meet the following principles and considering potential biases, risks, and unintended consequences:

- a) Human-Centered Design: AI systems are developed and deployed with a human-centered approach that evaluates AI-powered services for their impact on the public.
- b) Security & Safety: AI systems maintain confidentiality, integrity, and availability through safeguards that prevent unauthorized access and use. Implementation of AI systems is reliable and safe, and minimizes risks to individuals, society, and the environment.
- c) Privacy: Privacy is preserved in all AI systems by safeguarding Sensitive Data from unauthorized access, disclosure, and manipulation.
- d) Transparency: The purpose and use of AI systems are proactively communicated and disclosed to the public. An AI system, its data sources, operational models, and policies that govern its use are understandable and documented.
- e) Equity: AI systems support equitable outcomes for everyone. Bias in AI systems is effectively managed to reduce harm for anyone impacted by its use. Regular audits and assessments of AI models must be conducted to ensure fairness and accuracy.
- f) Accountability: Roles and responsibilities govern the deployment and maintenance of AI systems, and human oversight ensures adherence to relevant laws and regulations. DWSD must clearly indicate where DWSD has used generative AI to develop content.

- g) Effectiveness: AI systems are reliable, meet their objectives, and deliver precise and dependable outcomes for the utility and contexts in which they are deployed.
- h) Workforce Empowerment: Staff are empowered to use AI in their roles through education, training, and collaborations that promote participation and opportunity.

6.5. Approval Process

- 6.5.1. Any proposed AI project or initiative that connects to the DWSD system must go through an approval process that includes a clear business case, ethical considerations, and potential impacts on stakeholders.
- 6.5.2. Proposed AI projects or initiatives must be approved by the DWSD Chief Information Officer and DWSD IT Leadership Board before implementation.

6.6. Monitoring and Reporting

- 6.6.1. Continuous monitoring of AI systems shall remain in place to detect and address issues promptly.
- 6.6.2. Any incidents, failures, or ethical concerns related to AI usage must be reported to the DWSD Chief Information Officer and DWSD IT Leadership Board and addressed immediately.

6.7. Training and Awareness

- 6.7.1. The Information Technology Department (“IT Department”) will provide regular training on ethical AI practices and guidelines to employees involved in AI development and usage.
- 6.7.2. The IT Department will conduct awareness campaigns to educate employees about the responsible use of AI.

6.8. Guidelines for AI Use by DWSD Employees. The guidelines below clarify what is expected of DWSD employees when using AI systems.

- 6.8.1. Approved AI Only: In performing their official job duties, employees may only use AI that has been vetted and approved by the DWSD’s IT Department.
- 6.8.2. Privacy & Security: Only provide information to AI tools that are classified as DWSD-Public by the Data Classification Policy, unless the AI system has received prior approval for the inclusion of sensitive information. This includes everything shared with the AI, such as text, data, photos, videos, or voice recordings. For more information about what can be publicly disclosed, see the “Data Classification Policy”. If AI output includes unexpected Sensitive Data, be sure to remove this before making it public.
- 6.8.3. Accuracy: Review and fact-check all outputs received from AI before their use. Users should consult trustworthy sources to confirm that the facts and details in the AI content are accurate. Consult with your supervisor for those trustworthy sources.
- 6.8.4. Identifying Bias: AI responses are based on patterns and relationships learned from large datasets derived from existing content, which may contain errors and are historically biased across race, sex, gender identity, ability, and many other factors. Employees who use AI need to be mindful that AI may be based on past stereotypes and needs to be corrected.

- 6.8.5. **Transparent:** DWSD shall be clear when it uses AI. This will require citing the use of AI in performing job duties.
- 6.8.6. **Responsible:** The person using AI is responsible and accountable for the content it generates. All use of AI should be approached with caution. The risk level of the use case should guide the degree of caution shown when using AI or its products.

6.9. Prohibited Uses for AI Systems

- 6.9.1. Real-time and covert biometric identification.
- 6.9.2. Emotional analysis, or the use of computer vision techniques to classify human facial and body movements into certain emotions or sentiments (e.g., positive, negative, neutral, happy, angry, nervous).
- 6.9.3. Automated evaluations or decision-making that do not require any meaningful human oversight but substantially impact individuals. This includes both the evaluation of people, such as for employee reviews, and the evaluation of programs.
- 6.9.4. Social scoring, or the use of AI systems to track and classify individuals based on their behaviors, socioeconomic status, or personal characteristics.
- 6.9.5. Cognitive behavioral manipulations of people or specific vulnerable groups.
- 6.9.6. Autonomous weapons systems.
- 6.9.7. AI systems should also never be used to create images or other media representing actual events or occurrences because of the risk of misrepresenting the event and its participants or the possibility of infringing intellectual property rights. Existing media documenting the event should be relied upon for all representations.

6.10. Accountability

- 6.10.1. Individuals responsible for AI projects, including data analysts and AI developers, are to be held accountable for the ethical and responsible use of AI technology.
- 6.10.2. Managers responsible for staff who work on AI projects are accountable for the ethical and responsible use of AI technology.

6.11. Compliance and Violations.

- 6.11.1. Employees should contact their supervisor if they have questions about whether proposed actions may violate this Policy.
- 6.11.2. Failure of a DWSD employee to comply with this Policy is a violation of DWSD's Employee Standards of Conduct Policy and may also constitute violations of other DWSD Policies, and may result in revocation of system privileges and/or disciplinary action up to and including termination according to DWSD's Corrective Action Policy.
- 6.11.3. Failure to comply with this policy by a contractor using DWSD technology resources may be considered grounds for breach of its contract and revocation of system privileges.
- 6.11.4. Employees or contractors who use data for illegal purposes are subject to legal action by DWSD or other government authorities.

6.12. Reasonable and Necessary Accommodations

6.12.1. Management may take reasonable and necessary actions to accomplish the intent of this policy.