



**WEST VALLEY WATER DISTRICT
855 W. BASE LINE ROAD, RIALTO, CA 92376
PH: (909) 875-1804
WWW.WVWD.ORG**

**SPECIAL SAFETY AND TECHNOLOGY COMMITTEE MEETING
AGENDA**

Monday, October 5, 2026, 6:00 PM

NOTICE IS HEREBY GIVEN that West Valley Water District has called a meeting of the Safety and Technology Committee to meet in the Administrative Conference Room, 855 W. Base Line Road, Rialto, CA 92376.

BOARD OF DIRECTORS

**Director Daniel Jenkins, Chair
President Kelvin Moore**

Members of the public may attend the meeting in person at 855 W. Base Line Road, Rialto, CA 92376, or you may join the meeting using Zoom by clicking this link: <https://us02web.zoom.us/j/8402937790>. Public comment may be submitted via Zoom, by telephone by calling the following number and access code: Dial: (888) 475-4499, Access Code: 840-293-7790, or via email to administration@wwwd.org.

If you require additional assistance, please contact administration@wwwd.org.

CALL TO ORDER

PUBLIC PARTICIPATION

Any person wishing to speak to the Board of Directors on matters listed or not listed on the agenda, within its jurisdiction, is asked to complete a Speaker Card and submit it to the Board Secretary, if you are attending in person. For anyone joining on Zoom, please wait for the Board President's instruction to indicate that you would like to speak. Each speaker is limited to three (3) minutes. Under the State of California Brown Act, the Board of Directors is prohibited from discussing or taking action on any item not listed on the posted agenda. Comments related to noticed Public Hearing(s) and Business Matters will be heard during the occurrence of the item.

Public communication is the time for anyone to address the Board on any agenda item or anything under the jurisdiction of the District. Also, please remember that no disruptions from the crowd will be tolerated. If someone disrupts the meeting, they will be removed.

DISCUSSION ITEMS

1. Minutes of the September 15, 2026, Special Safety & Technology Committee
2. Updates to the Safety and Technology Committee
3. Artificial Intelligence ("AI") Acceptable Use Policy

ADJOURN

Please Note:

Material related to an item on this agenda submitted to the Board of Directors after distribution of the agenda packet is available for public inspection in the District's office located at 855 W. Base Line Road, Rialto, CA 92376, during normal business hours. Also, such documents are available on the District's website at www.wvwd.org subject to staff's ability to post the documents before the meeting.

Pursuant to Government Code Section 54954.2(a), any request for a disability-related modification or accommodation, including auxiliary aids or services, to attend or participate in the above agendized public meeting should be directed to the Board Secretary, Brandon Yoshida, at least 72 hours in advance of the meeting to ensure availability of the requested service or accommodation. Brandon Yoshida may be contacted by telephone at (909) 875-1804 ext. 703, or in writing at the West Valley Water District, P.O. Box 920, Rialto, CA 92377-0920.

DECLARATION OF POSTING:

I hereby declare under penalty of perjury, that I am employed by the West Valley Water District, and that the foregoing agenda was posted at the District Office's bulletin boards and the District website at www.wvwd.org on October 1, 2026, by 6:00 pm., in compliance with the provisions of the Brown Act.



Brandon Yoshida, Board Secretary

Date Posted: October 1, 2026

MINUTES
SPECIAL SAFETY AND TECHNOLOGY SPECIAL COMMITTEE
MEETING
of the
WEST VALLEY WATER DISTRICT
September 15, 2026

I. CALL TO ORDER

Chair Jenkins called the Safety and Technology Committee meeting to order at 6:03 p.m.

Attendee Name	Present	Absent	Late	Arrived
Daniel Jenkins	☒	☐	☐	
Kelvin Moore	☒	☐	☐	
Jose Velasquez	☒	☐	☐	
Linda Jadeski	☒	☐	☐	
Jon Stephenson	☒	☐	☐	
Albert Clinger	☒	☐	☐	

II. PUBLIC PARTICIPATION

Chair Jenkins inquired if anyone from the public would like to speak. No requests were received; therefore Chair Jenkins closed the public comment period.

III. DISCUSSION ITEMS

1. Updates to the Safety and Technology Committee

Staff provided updates on the implementation of FortiNAC (Fortinet Network Access Control), which is in progress and nearly complete; and Utility Payment API / iPaySmart updates, in which Tyler has completed their configuration and provided access to iPaySmart; and the Website Redesign, where the staff team has been assembled to develop an RFP for website redesign services; and Policies where staff is working on an AI Acceptable Use Policy with BBK

2. Minutes of the August 3, 2026, Special Safety & Technology Committee Meeting

The Committee approved the minutes as presented.

3. Resolution No. 2026-15 - Approval and Adoption of the SCADA Master Plan

The Committee approved the Resolution as presented to be placed on the Consent Calendar of the next Regular Board of Directors Meeting.

4. Professional Services Agreement with SDI Presence, LLC for an IT Master Plan

The Committee approved the Agreement as presented to be placed on the Consent Calendar of the next Regular Board of Directors Meeting.

IV. ADJOURN

Chair Jenkins adjourned the meeting at 6:21 p.m.

ATTEST:

Brandon Yoshida, Board Secretary



STAFF REPORT

DATE: October 5, 2026
TO: Safety and Technology Committee
FROM: Jon Stephenson, Director of Technical Services
SUBJECT: Artificial Intelligence ("AI") Acceptable Use Policy

STRATEGIC GOAL:

Strategic Goal 5 – Apply Sound Planning, Innovation, and Best Practices; E. Define, Develop, and Implement Best Practices.

MEETING HISTORY:

None.

BACKGROUND:

West Valley Water District ("District") recognizes that artificial intelligence technologies are rapidly becoming integrated into everyday business processes, decision-making tools, and public-facing services. While these tools offer meaningful opportunities to improve efficiency, enhance data analysis, and expand service capabilities, they also introduce new risks related to privacy, accuracy, security, and compliance with existing regulations. Without clear guidance, employees may inadvertently expose sensitive information, rely on AI-generated outputs without proper verification, or adopt tools that do not meet District standards.

An AI Acceptable Use Policy establishes consistent expectations for how staff may interact with AI systems in a responsible, secure, and ethical manner. It provides safeguards to protect confidential data, ensures transparency around AI-assisted work, and promotes accountability in how automated tools are used to support organizational decision-making. Implementing such a policy now will help the District leverage emerging technologies effectively while reducing potential operational, legal, and reputation risks.

DISCUSSION:

This AI Acceptable Use Policy, included as **Exhibit A** to Resolution 2026-16, was drafted by staff to address the District's needs and environment, and it has been reviewed by legal counsel. It sets forth the District's requirements for the responsible and ethical use of AI Systems by identifying permitted AI uses, prohibited AI uses, and AI uses requiring prior District approval. This Policy is intended to benefit the District and the public while also safeguarding privacy, security, confidentiality, public records, intellectual property rights, civil rights, and the reliability of District operations and communications.

To ensure that this Policy continually aligns with emerging AI risks, the evolving regulatory landscape, and AI-governance best practices, this Policy will be reviewed at least annually.

FISCAL IMPACT:

No fiscal impact is anticipated from adopting the AI Acceptable Use Policy.

REQUESTED ACTION:

Staff recommends that the Committee forward a recommendation to the Board of Directors to:

1. Adopt Resolution No. 2026-16 adopting the AI Acceptable Use Policy.

Attachments

[Resolution No. 2026-16 AI Acceptable Use Policy.pdf](#)

RESOLUTION NO. 2026-16

A RESOLUTION OF THE BOARD OF DIRECTORS OF THE WEST VALLEY WATER DISTRICT ADOPTING THE AI ACCEPTABLE USE POLICY

WHEREAS, the West Valley Water District ("District") Board of Directors ("Board") recognizes that, artificial intelligence technologies are rapidly becoming integrated into everyday business processes, decision-making tools, and public-facing services, which introduces new risks related to privacy, accuracy, security, and compliance with existing regulations; and

WHEREAS, the Board desires to adopt the necessary policies to establish consistent expectations for how staff may interact with AI systems in a responsible, secure, and ethical manner; and to provide safeguards to protect confidential data, ensure transparency around AI-assisted work, and promote accountability in how automated tools are used to support organizational decision-making;

NOW, THEREFORE, THE BOARD OF DIRECTORS OF THE WEST VALLEY WATER DISTRICT DOES HEREBY RESOLVE AS FOLLOWS:

SECTION 1. The Board hereby approves and adopts the AI Acceptable Use Policy set forth in Exhibit "A" attached hereto and incorporated herein by reference.

SECTION 2. This Resolution shall be effective as of the date of adoption.

SECTION 3. If any section, subsection, sentence, clause, or phrase of this Resolution is for any reason held invalid or unenforceable, such decision shall not affect the validity of the remaining portions of this Resolution.

BE IT FURTHER RESOLVED that said Resolution shall be effective _____, 2026.

PASSED, APPROVED AND ADOPTED this ____ day of _____ 2026.

KELVIN MOORE

President

Board of Directors

West Valley Water District

ATTEST:

Brandon Yoshida

Board Secretary

CERTIFICATION

I, Brandon Yoshida, Board Secretary of the West Valley Water District, do hereby certify that the foregoing Resolution No. 2026-16 was duly adopted by the Board of Directors of the West Valley Water District at a regular meeting held on _____, 2026, by the following vote:

AYES: BOARD MEMBERS:

NOES: BOARD MEMBERS:

ABSENT: BOARD MEMBERS:

ABSTAIN: BOARD MEMBERS:

Dated: _____, 2026

Brandon Yoshida

Board Secretary

RESOLUTION NO. 2026-16

EXHIBIT A

AI ACCEPTABLE USE POLICY

WEST VALLEY WATER DISTRICT

AI ACCEPTABLE USE POLICY

I. PURPOSE

West Valley Water District (“**District**”) recognizes that, when used appropriately, artificial intelligence (AI) tools can support personnel in their work, improve overall operational efficiency, and enhance the District’s services to ratepayers.

This AI Acceptable Use Policy (this “**Policy**”) sets forth the District’s requirements for the responsible and ethical use of AI Systems by identifying permitted AI uses, prohibited AI uses, and AI uses requiring prior District approval. This Policy is intended to benefit the District and the public while also safeguarding privacy, security, confidentiality, public records, intellectual property rights, civil rights, and the reliability of District operations and communications.

Responsible Use Principles

The District will acquire, configure, use, monitor, suspend and discontinue AI Systems consistent with the following principles:

- **Human-Centered Design and Supervision.** The AI System must support legitimate District purposes and remain subject to appropriate human judgment and oversight.
- **Security, Safety, and Privacy.** The AI System must protect confidentiality, integrity, availability, privacy, public safety, water services, and the environment through safeguards proportionate to risk.
- **Transparency and Documentation.** The District will document approved AI System uses and provide transparency appropriate to the context, legal requirements, and risks involved.
- **Equity and Nondiscrimination.** The AI System must be evaluated and used to prevent unlawful discrimination and to identify and mitigate harmful bias.
- **Accountability and Effectiveness.** Responsible persons must be identifiable, outputs must be reviewed, and the AI System must be monitored to confirm that it remains reliable, secure, lawful, and useful for its approved purpose.]

II. SCOPE

This Policy applies to all District officials, employees, temporary staff, interns, and volunteers, and any other persons working under the District’s direction or supervision (“**District Personnel**”). This Policy also establishes requirements for District Personnel who procure, engage, oversee, or grant access to District systems or District Data to contractors, consultants, vendors, or other third parties (collectively, “**Contractors**”). A Contractor is bound by this Policy only to the extent it is incorporated into the Contractor’s written agreement with the District or separately accepted in writing as a condition of access to District systems or District Data. For purposes of this Policy,

“AI Users” means District Personnel and any Contractor contractually required to comply with this Policy.

Roles and Responsibilities

- **AI Users:** In order to protect the integrity of the District’s systems and District Data, all AI Users must comply with this Policy and promptly report any known or suspected violations of this Policy or any other concerns or incidents relating to the use of AI Systems on the District’s behalf.
- **Supervisors:** Supervisors and department heads are responsible for: identifying business needs, confirming that proposed uses are and remain appropriate; ensuring that AI Users receive sufficient training on AI Systems and comply with required human-review and verification procedures; and escalating new or higher-risk uses for approval.
- **Legal, HR and Risk:** Legal and the Human Resources and Risk Manager will review legal, civil rights, employment, privacy, public-records, claims, and other risk issues as appropriate to the proposed use or incident.
- **Procurement:** If a Contractor will have access to District Data that includes Sensitive Data or PII or will have direct access to District servers, then as part of the evaluation of the Contractor with respect to cybersecurity, District personnel should evaluate whether the use of AI tools by the Contractor to provide services to the District will protect the confidentiality of such data.
- **Information Technology:** The Director of Technical Services or designee is responsible for approving AI Systems, configurations, integrations, and technical safeguards; coordinating cybersecurity and privacy review; maintaining the approved-use inventory; and suspending access when necessary or appropriate.
- **Management:** The General Manager or designee may require one or more AI Users to alter, suspend, or discontinue use of an AI System on the District’s behalf.

III. POLICY

AI Users may use Authorized AI Tools and other expressly approved AI Systems for approved District purposes so long as such use complies with this Policy, applicable law, and other District policies.

To ensure that this Policy continually aligns with emerging AI risks, the evolving regulatory landscape, and AI-governance best practices, the Director of Technical Services or designee, in consultation with Legal, Human Resources and Risk, records management, procurement, and affected departments as appropriate, must review this Policy at least annually and recommend updates through the District’s applicable approval process

A. Definitions

For purposes of this Policy, the following defined terms apply:

1. **AI System:** Any software, hardware, application, feature, tool, model, or service that operates in whole or in part using AI, including an AI feature embedded in another product.
2. **Artificial Intelligence (AI):** A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.
3. **Authorized AI Tool:** An AI System, including its configuration, that is approved in writing by the Director of Technical Services or designee for specified District use cases and data categories.
4. **District Data:** Any data, record, content, prompt, file, code, credential, image, communication, or other information that (i) is created, received, maintained, or controlled by or for the District in connection with District business; or (ii) is non-public information that AI Users are authorized to access through District systems or through District-provided or District-authorized accounts, credentials, subscriptions, or access rights, regardless of format, source, ownership, or storage location.
5. **Generative AI (GenAI):** AI that generates or materially modifies content, including text, images, audio, video, software code, or synthetic data, in response to a user's prompt or other input.
6. **High-Impact Decision:** A decision or recommendation that determines or materially affects a person's employment or other economic opportunity, compensation, discipline, or access to District services, customer assistance, rates, fees, billing, collections, enforcement, or other legal or regulatory rights or restrictions.
7. **Machine Learning (ML):** A subset of AI that uses data and algorithms to identify patterns or improve performance on a task without being explicitly programmed for every result.
8. **Personally Identifiable Information (PII):** Any non-public information that identifies a specific individual directly or, when combined with other information, indirectly. *Examples include Social Security or other government identification numbers, financial account information, medical information, biometric data, home addresses, personal email addresses, and personal telephone numbers.*
9. **Sensitive Data:** District Data requiring heightened protection because of law, contract, policy, security risk, or confidentiality. *Examples include PII and other non-public Personal Information; customer and account data; personnel, medical, and financial information; credentials and authentication data; attorney-client privileged information*

and attorney work product; proprietary information; cybersecurity, network, operational technology, critical infrastructure, water quality, and SCADA information; and other non-public or confidential District records.

B. Special Considerations - Accuracy

- AI outputs may be inaccurate, incomplete, biased, outdated, false or fabricated, misleading or unsupported. AI systems may also produce different outputs from similar prompts or inputs. AI Users remain responsible for all work performed and decisions made with AI assistance. All AI-assisted output must be meaningfully and independently reviewed for accuracy, relevance, validity, bias, and integrity by persons qualified in the relevant subject matter.
- Before using AI output for District business, AI Users must verify material facts, calculations, citations, quotations, and cited sources against reliable sources and review the output for relevance, bias, confidentiality, intellectual property concerns, accessibility, and compliance with applicable requirements
- AI output is an aid and may not substitute for required professional expertise, independent review, or a decision by authorized District Personnel. The level of review must be proportionate to risk. Public-facing, legal, financial, personnel, safety, water quality, cybersecurity, operational technology, and other consequential uses require review by qualified persons.

C. Risk-Based Review and Approval

Before acquiring, activating, integrating, or materially expanding an AI System, or using it with District Data, the Director of Technical Services or designee must coordinate a documented review proportionate to risk. The review must address, as appropriate, the purpose and users; data types, retention, deletion, and model training; accuracy and human oversight; cybersecurity and operational safety; privacy, civil rights, accessibility, intellectual property, and records requirements; vendor and subcontractor practices; public transparency; monitoring; and continuity and exit planning.

Higher-risk uses require written approval from the Director of Technical Services and the affected department, with Legal, Human Resources and Risk Management, procurement, records management, communications, or other review as appropriate. Higher-risk uses include those involving non-public Personal Information or Sensitive Data; employment or customer decisions; public-facing autonomous interactions; AI-assisted code proposed for deployment in a production environment; or water quality, critical infrastructure, operational technology, SCADA, safety, financial, or other consequential functions.

IT will maintain an inventory of approved AI Systems, configurations, owners, vendors, use cases, data categories, integrations, and review dates. Approval of a tool does not authorize every use case, integration, or category of data.

D. Guidelines for Use

- AI Users may use an Authorized AI Tool for an approved use case without notifying a supervisor each time, unless the applicable department requires notice. A new tool, use case, integration, automated action, or data category requires prior written approval from the Director of Technical Services or designee. Supervisors must coordinate with IT to ensure appropriate personnel training, review, and safeguards.
- Microsoft Copilot is an Authorized AI Tool only when accessed through a District-issued account and in the configuration approved by the Director of Technical Services or designee. Any other AI System, account, plug-in, extension, integration, or material feature requires prior written approval.
- In order to ensure the accuracy and reliability of AI System outputs, AI Users must review and verify all AI-assisted work and information before relying on or distributing it.
- AI Users may not use an AI System to request, create, revise, reproduce, distribute, or otherwise use content in a manner that infringes third-party intellectual property or publicity rights. AI Users may not assume that AI output is original, licensed, accurate, or free of restrictions
- Material use of Generative AI in public-facing work product must be disclosed when required by law, contract, District policy or procedure, or direction from a supervisor or department head. Routine use for brainstorming, grammar, formatting, or editing does not by itself require disclosure. AI-generated output may not be cited as authority for an underlying factual, legal, technical, or policy proposition. If the AI-generated output itself is being evaluated or documented, it may be quoted or cited as the subject of that evaluation, but the underlying proposition must still be verified against an authoritative source.
- AI Users may access an Authorized AI Tool only with the District-approved account and configuration and apply available privacy controls. AI Users may not assume that privacy settings, opt-outs, chat deletion, or private-browsing modes prevent a provider or third party from retaining or using submitted data. Before submitting District Data, AI Users must confirm that the tool, use case, and applicable data category have been approved. AI Users may not submit credentials, authentication information, secrets, or any other information prohibited from submission under this Policy. Other Sensitive Data may be submitted only if the Director of Technical Services or designee has approved that category of Sensitive Data for use with the Authorized AI Tool and appropriate contractual, technical, and administrative safeguards are in place.
- If an AI System has or may have produced, enabled, or contributed to an inaccurate, unauthorized, unsafe, biased, misleading, noncompliant, or harmful outcome, or to a privacy, confidentiality, cybersecurity, records, or intellectual-property incident, AI Users must stop

using the AI System or take reasonable steps to contain the incident when safe to do so, preserve relevant information, and immediately notify their supervisor and the District's IT Department. AI Users must also notify the District's Human Resources and Risk Manager when the event involves an employee, applicant, injury, claim, or other risk matter, and Legal when legal rights, obligations, investigations, or potential liability may be affected.

- The District is subject to the California Public Records Act and applicable records-retention requirements. Accordingly, an AI-related prompt, input, output, summary, log, or AI-assisted work product may constitute a public record when it relates to District business and is prepared, owned, used, or retained by the District.
- When AI content is saved to a District system, incorporated into a District record, used to materially support a District decision, retained in the ordinary course of business, or subject to a legal hold, it must be managed under the District's records-retention, Public Records Act, confidentiality, and legal-hold requirements. AI Users may not assume that AI-related material is private or exempt from disclosure solely because an AI tool was used.
- AI Users must manage AI-related records in accordance with the District's records-retention schedule and Public Records Act procedures. Routine or transitory AI interactions, such as brainstorming, editing, formatting, or drafting assistance, must be handled consistently with those requirements.
- Only the Director of Technical Services or designee may approve Authorized AI Tools; IT will manage and maintain an inventory of approved tools and use cases.
- Only AI integrations, plug-ins, extensions, agents, and automated actions approved in writing by the Director of Technical Services or designee may be enabled on, connected to, or permitted to access District systems, accounts, files, code repositories, operational technology, or District Data.
- The District may require one or more categories of AI Users to complete mandatory AI, cybersecurity, privacy, public-records, records-retention, or role-specific training before using an Authorized AI Tool and when material requirements change.
- The District must suspend, limit, or discontinue an AI System that is no longer effective, safe, lawful, secure, or useful. If abrupt cessation would materially disrupt District services, the General Manager or designee may approve a controlled phaseout. Any transition plan must address service continuity, records-retention and legal holds, data export or return, deletion, vendor and user access, integrations, and replacement processes.

E. Acceptable Use of AI Systems

AI Users are permitted to use an Authorized AI Tool as follows:

- Drafting, editing or publishing a public-facing communication, report, or media message, so long as a qualified personnel verify the material facts, citations, tone, legal and policy content, accessibility, and authorization before release.
- Drafting, editing, or reviewing an email, memorandum, or report, so long as any District Data input into the tool is nonconfidential or falls within a data category approved for use with that tool, and AI Users review the resulting AI-assisted content before use.
- Summarizing District Data, so long as it is non-confidential or falls within a data category approved for use with that tool, and AI Users verify the summary against the source material.
- Assisting with analyzing District Data, so long as the information is non-confidential or falls within a data category approved for use with that tool, and AI Users verify the methodology and results.
- Translating District Data from English into another language, so long as a person sufficiently proficient in the target language reviews the translated output before use, particularly translations involving emergency, safety, legal, technical, public-notice, or other sensitive or high-risk subject matter,
- Supporting the District's accessibility efforts, such as closed captioning or text-to-speech, so long as the output is tested and does not replace any legally-required accessibility review.
- Creating graphic designs, concept illustrations, or other layout suggestions, so long as AI Users comply with all District branding, intellectual property, privacy, and likeness requirements.
- Assisting with research, so long as AI Users verify all propositions, quotations, and citations using authoritative primary sources where reasonably available.
- Automating low-risk administrative tasks within an approved process, so long as the automation does not independently make a High-Impact Decision, commit District funds, alter customer accounts, communicate externally, affect a safety- or mission-critical system, or otherwise perform an action requiring specific approval under this Policy.
- Writing or troubleshooting code in a District-approved development environment. Actual API keys, passwords, access tokens, system credentials, and other secrets may not be entered into the AI System. Non-public source code or information about District systems, internal network architecture, or known security weaknesses may be entered only if the Director of Technical Services or designee has approved that type of information for use with the AI System. Before implementation, qualified personnel must review and appropriately test AI-assisted code for functionality and security. AI-assisted code may not hardcode or expose actual credentials or secrets, disclose non-public District system or network information to unauthorized persons or systems, or be deployed in production or used to access, control, or modify SCADA, industrial

control, water treatment, or water distribution systems without specific prior written approval from the Director of Technical Services or designee.

- Any other use expressly approved in writing by the relevant department head and the Director of Technical Services or designee and conducted in compliance with this Policy.

F. Prohibited Use of AI Systems

- Entering, pasting, uploading, transmitting, connecting, or otherwise making District Data, including Sensitive Data, available to an AI System that is not an Authorized AI Tool, whether through a prompt, file attachment, data integration, or other input method, unless the Director of Technical Services or designee has approved the tool, use, and applicable data category in writing
- Making or materially supporting a High-Impact Decision unless the proposed use has undergone the required risk review, received all written approvals required under this Policy, and is subject to meaningful, independent review by a qualified person who independently evaluates the relevant inputs and AI output and makes the final decision. AI output may not be the sole basis for a High-Impact Decision.
- Creating or distributing a deepfake, disinformation, impersonation, or materially deceptive or manipulative synthetic content. This prohibition does not apply to synthetic content that is created for an expressly authorized legitimate District purpose, appropriately controlled, clearly labeled when necessary to avoid deception, and not intended to deceive.
- Deploying or using AI in a manner that could compromise the District's data security or privacy, or otherwise pose an unreasonable risk to District systems, District Data, critical infrastructure, water quality, service continuity, public safety or the environment.
- Using AI to evade or circumvent access controls, procurement requirements, records-retention schedules, legal holds, Public Records Act procedures, confidentiality restrictions, accessibility requirements, or other District policies or legal obligations.
- Using AI for social scoring or to rank or classify a person based on behavior, socioeconomic status, personal characteristics, or unrelated data in a manner that affects access to District services, employment, other opportunities, or legal rights.
- Using AI to exploit a person's age, disability, economic circumstances, or other vulnerability, or to manipulate a person through deceptive, subliminal, or materially misleading techniques.
- Using AI in a manner that unlawfully discriminates or relies on a proxy for a protected characteristic.

- Relying on AI as the final source of legal, engineering, financial, employment, water-quality, safety, cybersecurity, or other technical or professional judgment or advice without review and approval by qualified personnel
- Using AI to operate, control, or make autonomous changes to water treatment, water distribution, SCADA, industrial control, emergency response, public safety, financial transaction, or customer account systems without specific prior written approval and tested safeguards.
- Using real-time or covert biometric identification or emotion-inference technology involving employees, applicants, customers, or members of the public, except when specifically authorized after appropriate privacy, security, civil-rights and other legal review.

IV. POLICY ENFORCEMENT

Any District Personnel who violates this Policy may face suspension or termination of AI system access, and other corrective or disciplinary action, up to and including termination, consistent with applicable law, personnel rules and District policies.

The District may also refer AI Users to the appropriate governmental authorities for any known or suspected unlawful conduct.