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

POLICY REVIEW AND OVERSIGHT COMMITTEE MEETING AGENDA

Thursday, November 12, 2026, 5:00 PM

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

BOARD OF DIRECTORS

Director Gregory Young, Chair
Director Daniel Jenkins

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@wvwd.org.

If you require additional assistance, please contact administration@wvwd.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. Updates to the Policy Review and Oversight Committee
2. Approve Minutes of the October 13, 2026, Policy Review & Oversight Committee Meeting PG. 4
3. Artificial Intelligence ("AI") Acceptable Use Policy PG. 6
4. Adopt Resolution 2026-XX - A Resolution of the Board of Directors of the West Valley Water District Amending the Public Records Act Request Policy PG. 36
5. Adopt Resolution 2026-XX - A Resolution of the Board of Directors of the West Valley Water District Establishing an Electronic Signature Policy PG. 47
6. Adopt Resolution 2026-XX - A Resolution of the Board of Directors of the West Valley Water District Establishing a Litigation Hold Policy PG. 56

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 November 5, 2026, by 6:00 pm., in compliance with the provisions of the Brown Act.

Brandon Yoshida

Brandon Yoshida, Board Secretary

Date Posted: November 5, 2026

MINUTES
POLICY REVIEW AND OVERSIGHT COMMITTEE MEETING
of the
WEST VALLEY WATER DISTRICT
OCTOBER 13, 2026

I. CALL TO ORDER

Chair Young called the Policy Committee Meeting of the West Valley Water District to order at 5:00 p.m.

Attendee Name	Present	Absent	Arrived
Gregory Young	☑	☐	
Daniel Jenkins	☑	☐	
John Thiel	☑	☐	
Linda Jadeski	☑	☐	
Jon Stephenson	☑	☐	

II. PUBLIC PARTICIPATION

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

III. DISCUSSION ITEMS

1. Minutes of the September 22, 2026 Policy Review & Oversight Committee Meeting

The Committee approved the Minutes as presented.

2. Updates to the Policy Review and Oversight Committee

Assistant General Jadeski reported that the Board Secretary will bring forth a litigation hold policy to the next committee meeting.

3. Artificial Intelligence (“AI”) Acceptable Use Policy

Director of Technical Services Jon Stephenson provided a summary of the policy. The Committee requested that legal counsel review the policy for applicability to the Board of Directors, then bring it back to the Safety and Technology Committee before returning it to the Policy Review & Oversight Committee.

IV. ADJOURN

Chair Young adjourned the meeting at 5:24 p.m.

ATTEST:

_____
Brandon Yoshida, Board Secretary

STAFF REPORT

DATE: November 12, 2026

TO: Policy Review and Oversight 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:

10/05/26 - Special Safety and Technology Committee Meeting
10/13/26 - Special Policy Review and Oversight Committee Meeting
11/02/26 - Regular Safety and Technology Committee Meeting

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 2026-17, 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.

The policy was reviewed by the Safety and Technology Committee as well as the Policy Review and Oversight Committee. One clarification was requested regarding the Scope of the policy. Specifically, whether the policy applies to the Board of Directors. The language in the Scope was updated to clarify that, "The use of AI by elected officials in connection with official District business will be governed separately under the Board Policies and Procedures Manual." The proposed update to the Board Policies and Procedures Manual is forthcoming.

Staff did also make one additional change in Section D. Guidelines for Use. Microsoft CoPilot was listed as the only authorized AI tool because it is currently the only AI tool for which the District has an account. Language was added to clarify that " Access to other AI tools such as ChatGPT, Claude, Gemini, and Grok may also be granted through District-issued accounts."

A redline version of the policy that was presented at the last meeting is included as **Attachment A**. A clean version is included as **Attachment B**.

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. 2026-17 adopting the AI Acceptable Use Policy.

Attachments

Attachment_A-AI_Acceptable_Use_Policy_Redlines.pdf
Attachment_B-AI_Acceptable_Use_Policy_Clean.pdf

ATTACHMENT A

REDLINE VERSION

RESOLUTION NO. 2026-17

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. 2026-17

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**"). The use of AI by elected officials in connection with official District business will be governed separately under the Board Policies and Procedures Manual.

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. Access to other AI tools such as ChatGPT, Claude, Gemini, and Grok may also be granted through District-issued accounts. 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.

ATTACHMENT B

CLEAN VERSION

RESOLUTION NO. 2026-17

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. 2026-17

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 employees, temporary staff, interns, and volunteers, and any other persons working under the District's direction or supervision ("**District Personnel**"). The use of AI by elected officials in connection with official District business will be governed separately under the Board Policies and Procedures Manual.

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. Access to other AI tools such as ChatGPT, Claude, Gemini, and Grok may also be granted through District-issued accounts. 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.

STAFF REPORT

DATE: November 12, 2026

TO: Policy Review and Oversight Committee

FROM: Brandon Yoshida, Board Secretary

SUBJECT: Adopt Resolution 2026-XX - A Resolution of the Board of Directors of the West Valley Water District Amending the Public Records Act Request Policy

---

STRATEGIC GOAL:

Strategic Goal 8 - Deliver Superior Customer Service; C. Provide Easy and Transparent Access to Public Records and Information.

MEETING HISTORY:

May 7, 2020 - Regular Board of Directors Meeting

BACKGROUND:

In 2023, the California Public Records Act was re-codified from Government Code Sections 6250 et seq. to Government Code Sections 7920.000 et seq. As a result, references to the former Government Code sections within the District's policy and Public Records Act Request Form/Website Page require updating to reflect the current statutory citations.

DISCUSSION:

The proposed revisions are administrative in nature and ensure that the District reflects the correct procedures in accordance with the California Public Records Act and the 2023 re-codification. No substantive changes to the District's existing procedures or practices for processing public records requests are proposed at this time.

The attached Resolution and Policy were reviewed and approved by the District's General Counsel.

FISCAL IMPACT:

None.

REQUESTED ACTION:

It is respectfully recommended that the Policy Review & Oversight Committee:

1. Forward the recommendation to the Board of Directors to adopt Resolution 2026-XX - A Resolution of the Board of Directors of the West Valley Water District Amending the Public Records Act Request Policy.

Attachments

Resolution_Policy-Public_Records_Request_11-12-2026.pdf

WEST VALLEY WATER DISTRICT
BOARD OF DIRECTORS
RESOLUTION NO. 20XX-XXXX

A RESOLUTION OF THE BOARD OF DIRECTORS OF THE WEST VALLEY WATER DISTRICT AMENDING THE PUBLIC RECORDS ACT REQUEST POLICY

The Board of Directors of the West Valley Water District (hereafter referred to as the "Board of Directors") does resolve as follows:

WHEREAS, the West Valley Water District ("District") originally adopted its Public Records Act Request Policy in May of 2020; and

WHEREAS, in 2023, the California Public Records Act was re-codified from Government Code Sections 6250 et seq. to Government Code Sections 7920.000 et seq.; and

WHEREAS, as a result, references to the former Government Code sections within the District's policy and Public Records Act Request Form/Website Page require updating to reflect the current statutory citations; and

WHEREAS, the District desires to amend and restate the Policy to update statutory citations and clarify the District's procedures for receiving, evaluating, and producing public records requests.

NOW, THEREFORE, THE BOARD OF DIRECTORS OF THE WEST VALLEY WATER DISTRICT FINDS, DETERMINES, ORDERS AND RESOLVES AS FOLLOWS:

SECTION 1. RECITALS. The foregoing recitals are true and correct and are incorporated herein by reference.

SECTION 2. BOARD OF DIRECTORS ACTION. Approve and adopt the amended and restated West Valley Water District Public Records Act Request Policy, as attached hereto as "Exhibit A".

SECTION 3. AUTHORIZATION. The General Manager or designee may make non-substantive administrative updates to keep statutory citations current, provided those updates do not materially change the Policy. Substantive amendments require approval by the Board of Directors.

SECTION 4. EFFECTIVE DATE. This Resolution shall become effective upon adoption by the Board of Directors, unless otherwise specified herein.

SECTION 5. SEVERABILITY. If any section, subsection, paragraph, sentence, clause, or phrase of this Resolution is declared by a court of competent jurisdiction to be unconstitutional or otherwise invalid, such decision shall not affect the validity of the remaining portions of this Resolution.

SECTION 6. CERTIFICATION. The Board Secretary shall certify to the adoption of this Resolution.

PASSED, APPROVED AND ADOPTED this XXth day of Month, 2026.

_____
Kelvin Moore, President

ATTEST:

_____
Brandon Yoshida, Board Secretary

I, Brandon Yoshida, Board Secretary of the West Valley Water District, do hereby certify that the foregoing resolution was adopted by the Board of Directors of the West Valley Water District on the XXth day of MONTH, 2026, and was passed by the following vote:

AYES:
NOES:
ABSTAIN:
ABSENT:

_____
Brandon Yoshida, Board Secretary

EXHIBIT A

Purpose

To establish District policy and guidelines concerning accessibility of District records.

Background

In enacting the California Public Records Act, the State Legislature declared that access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state.

A. The term "District" shall mean West Valley Water District.

B. The term "public records" includes any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by the District regardless of physical form or characteristics.

C. The term "writing" means handwriting, typewriting, printing, photo-stating, photographing, photocopying, electronic mail, facsimile, and every other means of recording upon any form of communication or representation, including letters, words, pictures, sounds, symbols, or combination thereof and all papers, maps magnetic or paper tapes, photographic films and prints, magnetic or punch cards, discs, drums and other documents regardless of the manner in which the record has been stored.

D. The term "person" includes any natural person, corporation, partnership, limited liability company, firm or association.

E. The term "requester" shall mean a person, or representative of a person, who has submitted a request for records to the District by mail, fax, e-mail, telephone or in person. Policy Public records of the West Valley Water District ("District") shall be open to inspection during normal office hours at the District's headquarters located at 855 W. Base Line Road, Rialto, California. A "public record" includes any writing containing information relating to the conduct of the public's business that is prepared, owned, used, or retained by the District, regardless of physical form or characteristics, except as otherwise provided by law.

Procedure

A. A request must reasonably describe an identifiable record or records.
When a request is unclear, the District shall, to the extent reasonable under the circumstances, assist the requester in identifying records responsive to the request or its stated purpose, describe the information technology and physical location in which responsive records may be found, and suggest ways to overcome practical barriers to access. (Gov. Code, § 7922.600.)

B. Any person may obtain a copy of any identifiable public record unless exempt from public disclosure. The District may make a request form available for convenience, but a request may be made orally or in writing and use of a form is not required. A request may be directed to the Board Secretary or another person designated to coordinate Public Records Act responses. An employee who receives a request shall promptly route it to that person. Media requests may also be referred to the District's designated media contact, but that referral does not alter the District's response obligations. Written requests reduce any misunderstandings between the requester and the District's staff, which allows District's staff to respond to records requests in a timely manner and with greater efficiency. However, the District will not deny a request for records solely because it is not submitted in writing.

C. The requester should specify the records to be inspected/copied with sufficient detail to enable the District to identify the particular records. If the request seems ambiguous or unfocused, District staff will make a reasonable effort to obtain additional clarifying information from the requester that will help identify the record or records. Upon request, an exact copy shall be provided unless impracticable to do so.

D. Notice of Decision ("NOD"): Within ten (10) calendar days from receipt of such request, the District Clerk or designee shall determine whether the request, in whole or in part, seeks copies of disclosable public records in the possession of the agency and shall promptly notify the person making the request of the determination and the reasons thereof. If the Board Secretary is uncertain whether a record is exempt from disclosure, the Board Secretary shall consult with the District's General Counsel during the initial ten-day period. The public-interest balancing test in Government Code section 7922.000 applies when no express exemption governs. If the District determines that a request seeks disclosable records, the notice shall also state the estimated date and time when the records will be made available. In unusual circumstances, the time to make the determination may be extended by written notice stating the reasons for the extension and the date on which the determination is expected. The extension may not exceed fourteen (14) calendar days. Any extension of time will not last more than fourteen (14) calendar days. A response to a written request for inspection or copies of public records that includes a determination that the request is denied, in whole or in part, shall be in writing.

E. Unusual circumstances means the following, but only to the extent reasonably necessary to the proper processing of the particular request:

    a. The need to search for and collect the requested records from field facilities or other establishments that are separate from the office processing the request.

    b. The need to search for, collect, and appropriately examine a voluminous amount of separate and distinct records that are demanded in a single request.

c. The need for consultation, which shall be conducted with all practicable speed, with another agency having substantial interest in the determination of the request or among two or more components of the agency having substantial subject matter interest therein.

F. If a record contains information exempt from disclosure, the District shall provide any reasonably segregable nonexempt portion after redacting the exempt information. Any withholding shall be supported by an applicable express exemption or, when applicable, the public-interest balancing test in Government Code section 7922.000.

G. In-person inspection of physical records shall ordinarily occur at the District office. No physical record may be removed from the District's premises, and a District representative shall be present during in-person inspection. This procedure does not limit access to electronic records or the District's obligation to provide records in an electronic format when required by law.

H. The public records policy of the District shall at all times be subject to the California Public Records Act ("Act") as it may be amended from time to time, and if there is any conflict between the Act and this policy, the Act shall prevail.

I. In addition to maintaining public records for public inspection during office hours, the District may comply with a request by posting any public record on its Internet Website and direct a member of the public to the location on the Internet Website where the public record is posted. However, if a member of the public requests a copy because the member cannot access or reproduce a record posted on the District's website, the District shall promptly provide a copy. If a requested record is in an electronic format, the District shall make it available in that format when required by Government Code section 7922.570, subject to applicable law.

Production of Records Requests and Fees

Upon any request for a copy of public records which reasonably describes an identifiable record or information produced therefrom and which is not otherwise exempt from disclosure, and after payment of any fees, the District shall make the records promptly available, subject to applicable fees. The fees will cover the direct cost of duplication (see District Copy Cost Schedule). Upon request, an exact copy shall be provided unless impracticable to do so.

District Copy Cost Schedule

A. Requested documents can be viewed at the West Valley Water District's office at no charge.
B. The District may charge fees covering the direct costs of duplication, or a statutory fee when applicable. A charge for paper copies may not exceed the direct cost of duplication.

C. Charges for reproducing blueprints, maps, oversized documents, or similar materials shall be limited to the direct cost of duplication, unless a statutory fee applies.

D. Electronic records shall be provided in an electronic format when required by law. The charge for producing an electronic copy shall be limited to the direct cost of producing that copy. Costs for data compilation, extraction, or programming may be charged only when authorized by Government Code section 7922.575.

STAFF REPORT

DATE: November 12, 2026

TO: Policy Review and Oversight Committee

FROM: Brandon Yoshida, Board Secretary

SUBJECT: Adopt Resolution 2026-XX - A Resolution of the Board of Directors of the West Valley Water District Establishing an Electronic Signature Policy

---

STRATEGIC GOAL:

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

Strategic Goal 7 – Realize Health, Safety, and Regulatory Compliance; B. Establish Compliance Programs for Staff.

MEETING HISTORY:

None.

BACKGROUND:

The District currently does not have a formal Electronic Signature Policy establishing guidelines for the use, acceptance, and management of electronic signatures. As the District continues to utilize electronic documents and digital workflows, establishing consistent practices for electronic signatures will help support efficient administrative operations and compliance with regulatory statues.

DISCUSSION:

The proposed Electronic Signature Policy establishes guidelines and requirements for the use and acceptance of electronic signatures in accordance with applicable regulatory statues. The policy addresses signature authentication, verification, and security to help ensure electronic signatures are reliable and legally recognized. Adoption of the policy will provide a consistent framework for the Support Services Division while allowing for the continued use of traditional handwritten signatures when appropriate.

The attached Resolution and Policy were reviewed and approved by the District's General Counsel.

FISCAL IMPACT:

None.

REQUESTED ACTION:

It is respectfully recommended that the Policy Review & Oversight Committee:

1. Forward the recommendation to the Board of Directors to adopt Resolution 2026-XX - A Resolution of the Board of Directors of the West Valley Water District Establishing an Electronic Signature Policy.

Attachments

Resolution_Policy-Electronic_Signature_11-12-2026.pdf

WEST VALLEY WATER DISTRICT
BOARD OF DIRECTORS
RESOLUTION NO. 20XX-XXXX

A RESOLUTION OF THE BOARD OF DIRECTORS OF THE WEST VALLEY WATER DISTRICT, ESTABLISHING AN ELECTRONIC SIGNATURE POLICY

The Board of Directors of the West Valley Water District (hereafter referred to as the "Board of Directors") does resolve as follows:

WHEREAS, the West Valley Water District ("District") recognizes the use of electronic signatures as a means of facilitating efficient administrative operations and document processing; and

WHEREAS, the District desires to establish consistent guidelines and requirements for the use and acceptance of electronic signatures in accordance with applicable statutory regulations; and

WHEREAS, establishing an Electronic Signature Policy will establish standards for the authentication, verification, security, and retention of electronically signed documents; and

WHEREAS, the Board of Directors finds that adopting an Electronic Signature Policy will establish a defined guideline for the District to use when evaluating electronic signatures.

NOW, THEREFORE, THE BOARD OF DIRECTORS OF THE WEST VALLEY WATER DISTRICT FINDS, DETERMINES, ORDERS AND RESOLVES AS FOLLOWS:

SECTION 1. RECITALS. The foregoing recitals are true and correct and are incorporated herein by reference.

SECTION 2. BOARD OF DIRECTORS ACTION. Approve the West Valley Water District's Electronic Signature Policy to follow best business practices and establish a formal guideline, as attached hereto as "Exhibit A"

SECTION 3. AUTHORIZATION. The General Manager or designee may establish administrative procedures to implement the Policy, provided they are consistent with the Policy and applicable law. Material amendments to the Policy require approval by the Board of Directors.

SECTION 4. EFFECTIVE DATE. This Resolution shall become effective upon adoption by the Board of Directors, unless otherwise specified herein.

SECTION 5. SEVERABILITY. If any section, subsection, paragraph, sentence, clause, or phrase of this Resolution is declared by a court of competent jurisdiction to be unconstitutional or otherwise invalid, such decision shall not affect the validity of the remaining portions of this Resolution.

SECTION 6. CERTIFICATION. The Board Secretary shall certify to the adoption of this Resolution.

PASSED, APPROVED AND ADOPTED this XXth day of Month, 2026.

_____
Kelvin Moore, President

ATTEST:

_____
Brandon Yoshida, Board Secretary

I, Brandon Yoshida, Board Secretary of the West Valley Water District, do hereby certify that the foregoing resolution was adopted by the Board of Directors of the West Valley Water District on the XXth day of MONTH, 2026, and was passed by the following vote:

AYES:
NOES:
ABSTAIN:
ABSENT:

_____
Brandon Yoshida, Board Secretary

EXHIBIT A

PURPOSE

The purpose of this Electronic Signature Policy “Policy” is to establish guidelines for when an electronic signature may replace a handwritten "wet" signature, to encourage the use of paperless, electronic documents, as appropriate, to reduce the turnaround time on approval and full execution of documents, and to comply with the requirements of California Government Code section 16.5, the California Uniform Electronic Transactions Act (Civ. Code, § 1633.1 et seq.), the federal E-SIGN Act, and applicable regulations.

Electronic signatures shall not be used when prohibited by law or when applicable execution requirements cannot be satisfied electronically. Nothing in this policy supersedes legal requirements for particular documents or transactions.

DEFINITIONS

A “wet signature”, for purposes of this Policy, is a handwritten signature executed with an ink pen.

A “digital signature” means an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature. A digital signature is a type of “electronic signature.”

An “electronic signature” is defined as “any sound, symbol, or process attached to or associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record.”

An “electronic record” means a record created, generated, sent, communicated, received, or stored by electronic means.

SCOPE

This Policy applies to all signatures used in processing independent contracts and requests for proposals, as well as internal communications, external correspondence, and other official activities, unless noted otherwise below. By affixing an electronic signature to a document in a manner consistent with this Policy, it will satisfy the District’s requirement for signing a document.

This Policy does not address the validity of electronic signatures from third parties, but instead establishes a policy for District staff and Board Members to execute internal and external documents on behalf of the District via electronic signature, provided electronic signatures are allowable by law for the subject document and are acceptable by the third party receiving the executed District document.

This policy does not supersede laws specifically requiring a wet signature. Furthermore, this policy does not limit the right or option to conduct the transaction on paper or non-electronic forms or the right to have documents provided or made available on paper. Use of an electronic signature does not independently authorize any person to approve, execute, or bind the District to a document, and does not alter existing approval or delegation requirements.

The General Manager or designee may adopt administrative procedures and approve electronic-signature methods consistent with this Policy and applicable law, including Government Code section 16.5 and regulations adopted under that section.

REQUIREMENTS OF ELECTRONIC SIGNATURE

The use of electronic signatures is permitted and shall have the same force and effect as the use of a "wet" or manual signature if all the following criteria are met:

- The electronic signature is unique to the person using it.
- The electronic signature is capable of verification.
- The electronic signature is under the sole control of the person using it.
    1. Email notifications requesting electronic signatures must not be forwarded.
    2. These requirements prohibit the use of proxy signatures.
- The electronic signature is linked to the data in such a manner that if the data is changed after the electronic signature is affixed, the electronic signature is invalidated. For any digital signature used with a public entity, the technology must also be acceptable under Title 2, Division 7, Chapter 10 of the California Code of Regulations.

PROHIBITED USES OF ELECTRONIC SIGNATURES

Electronic signatures may not be used on the following documents:

- Documents or transactions that require a signature to be witnessed, attested to, notarized or acknowledged.
- Documents or transactions that require a wet signature, including but not limited to transfers of interests in real property, deeds and all recorded documents.
- Documents that summarize the actions taken by the Board of Directors, that in line with the Records Retention Schedule, are maintained in paper format indefinitely by the District such as: Minutes, Resolutions & Ordinances.
- Use of electronic signature technology that does not conform to the requirements set forth in this Policy.

STAFF REPORT

DATE: November 12, 2026

TO: Policy Review and Oversight Committee

FROM: Brandon Yoshida, Board Secretary

SUBJECT: Adopt Resolution 2026-XX - A Resolution of the Board of Directors of the West Valley Water District Establishing a Litigation Hold Policy

---

STRATEGIC GOAL:

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

Strategic Goal 7 – Realize Health, Safety, and Regulatory Compliance; B. Establish Compliance Programs for Staff.

MEETING HISTORY:

None.

BACKGROUND:

The District currently does not have a formal Litigation Hold Policy in place to establish procedures for preserving records and information related to pending or anticipated litigation, claims, investigations, other legal matters, etc.

DISCUSSION:

The proposed Litigation Hold Policy establishes a consistent process for identifying, issuing, and implementing litigation holds. The policy outlines the responsibilities of District staff to ensure potentially relevant records and electronically stored information are properly preserved. It also establishes procedures for issuing notices, tracking, coordinating with the Technical Services Department, and suspending routine records destruction when necessary.

Adoption of the policy will provide the District with a formal framework to ensure records subject to a litigation hold are appropriately preserved and remain available for General Counsel's review. While the District's Records Retention Schedule addresses the preservation of records, a standalone Litigation Hold Policy provides a more comprehensive framework as it establishes responsibilities and roles to ensure proper procedures are followed.

The attached Resolution and Policy were reviewed and approved by the District's General Counsel.

FISCAL IMPACT:

None.

REQUESTED ACTION:

It is respectfully recommended that the Policy Review & Oversight Committee:

1. Forward the recommendation to the Board of Directors to adopt Resolution 2026-XX - A Resolution of the Board of Directors of the West Valley Water District Establishing a Litigation Hold Policy.

Attachments

Resolution_Policy-Litigation_Hold_11-12-2026.pdf

WEST VALLEY WATER DISTRICT
BOARD OF DIRECTORS
RESOLUTION NO. 20XX-XXXX

A RESOLUTION OF THE BOARD OF DIRECTORS OF THE WEST VALLEY WATER DISTRICT, ESTABLISHING A LITIGATION HOLD POLICY

The Board of Directors of the West Valley Water District (hereafter referred to as the "Board of Directors") does resolve as follows:

WHEREAS, the West Valley Water District ("District") does not have an established Litigation Hold Policy; and

WHEREAS, the District recognizes the importance of preserving records and information related to pending or reasonably anticipated litigation, claims, investigations, and other legal matters; and

WHEREAS, the District desires to follow best business practices and establish a formal process for identifying, issuing, implementing, monitoring, and releasing litigation holds; and

WHEREAS, the Board of Directors finds that adopting a Litigation Hold Policy will establish consistent procedures and clearly define responsibilities for the preservation of District records and information; and

NOW, THEREFORE, THE BOARD OF DIRECTORS OF THE WEST VALLEY WATER DISTRICT FINDS, DETERMINES, ORDERS AND RESOLVES AS FOLLOWS:

SECTION 1. RECITALS. The foregoing recitals are true and correct and are incorporated herein by reference.

SECTION 2. BOARD OF DIRECTORS ACTION. Approve the West Valley Water District's Litigation Hold Policy to follow best business practices and establish a formal process, as attached hereto as "Exhibit A".

SECTION 3. AUTHORIZATION. The General Manager or designee may establish administrative procedures to implement the Policy, provided they are consistent with the Policy and applicable law. Material amendments to the Policy require approval by the Board of Directors.

SECTION 4. EFFECTIVE DATE. This Resolution shall become effective upon adoption by the Board of Directors, unless otherwise specified herein.

SECTION 5. SEVERABILITY. If any section, subsection, paragraph, sentence, clause, or phrase of this Resolution is declared by a court of competent jurisdiction to be unconstitutional or otherwise invalid, such decision shall not affect the validity of the remaining portions of this Resolution.

SECTION 6. CERTIFICATION. The Board Secretary shall certify to the adoption of this Resolution.

PASSED, APPROVED AND ADOPTED this XXth day of Month, 2026.

_____
Kelvin Moore, President

ATTEST:

_____
Brandon Yoshida, Board Secretary

I, Brandon Yoshida, Board Secretary of the West Valley Water District, do hereby certify that the foregoing resolution was adopted by the Board of Directors of the West Valley Water District on the XXth day of MONTH, 2026, and was passed by the following vote:

AYES:
NOES:
ABSTAIN:
ABSENT:

_____
Brandon Yoshida, Board Secretary

EXHIBIT A

PURPOSE

The purpose of this Litigation Hold Policy and Procedure ("Policy") is to create a consistent process for identifying, issuing, implementing, monitoring, and releasing litigation holds.

A litigation hold serves as a directive to preserve District records and information that may be relevant to pending or reasonably anticipated litigation, claims, investigations, or other legal matters.

A litigation hold suspends the District's ordinary destruction, deletion, alteration, or disposition of records that fall within the scope of the hold.

The purpose of a litigation hold is to ensure that potentially relevant information is preserved and remains available for review and, when legally required, discovery.

POLICY

The District shall take reasonable steps to preserve records and electronically stored information when the District becomes aware of pending or reasonably anticipated litigation or another circumstance requiring preservation of information.

When a litigation hold is issued, all District personnel and other individuals who possess or control information within the scope of the hold shall comply with the hold and preserve the identified information until the hold is formally released or otherwise modified by the District’s General Counsel.

A litigation hold takes precedence over the District's otherwise applicable records retention and destruction schedule for records within the scope of the hold. The District's normal records retention schedule shall continue to apply to records that are outside the scope of the litigation hold.

SCOPE

This policy applies to:

- All District departments and divisions
- All District employees
- Members of the Board of Directors, when acting in their official capacity
- Temporary and part-time employees
- Interns and other District personnel
- Consultants and contractors, when applicable

DEFINITIONS

"Litigation Hold" - A written directive issued by or at the direction of District's General Counsel requiring the preservation of specified records and information because of pending, threatened, or reasonably anticipated litigation, a claim, investigation, or other legal matter.

"Electronically Stored Information (ESI)" means information stored or maintained in electronic form.

"District's General Counsel" means the attorney or attorneys authorized by the District to provide legal advice to the District.

RESPONSIBILITIES

District's General Counsel shall have primary responsibility for the legal determination regarding litigation holds:

- Determine when a litigation hold is necessary
- Determine the scope of the hold
- Identify the subject matter and time period covered by the hold
- Identify, or assist in identifying, affected departments and custodians
- Prepare or approve the Litigation Hold notice
- Determine what categories of records and ESI must be preserved
- Provide direction regarding collection, preservation, and production of records
- Modify or expand the hold when necessary
- Monitor the legal status of the matter
- Determine when the litigation hold may be released
- Issue a written release or modification of the hold

The General Manager shall ensure that District departments provide the personnel and technical support needed to implement litigation holds. The Board Secretary shall coordinate administrative steps, and department directors and managers shall ensure that their personnel comply with hold notices and preservation instructions. District's General Counsel shall resolve legal questions concerning the scope and administration of a hold.

The Board Secretary shall:

- Maintain a confidential Litigation Hold Log
- Coordinate distribution of hold notices
- Track acknowledgments
- Coordinate with affected departments
- Coordinate with Information Technology regarding preservation of ESI
- Coordinate with Human Resources when personnel changes affect custodians
- Maintain documentation demonstrating implementation of the hold

- Conduct periodic administrative follow-up regarding outstanding acknowledgments
- Notify District's General Counsel of compliance issues or newly identified custodians

The Board Secretary shall not independently determine what records are legally responsive or whether a hold should be released. Those determinations belong to District's General Counsel.

Department Directors and Managers shall:

- Identify employees and other custodians who may possess information within the scope of a hold
- Communicate the hold to affected personnel
- Assist in identifying physical and electronic records
- Ensure that employees do not destroy or alter records subject to the hold
- Coordinate with IT and the Board Secretary as necessary
- Immediately notify the Board Secretary, Human Resources, or the District's General Counsel of personnel changes or other circumstances that may affect preservation

PROCEDURE

A litigation hold process may be initiated when the District becomes aware of:

- Filed litigation
- A summons or complaint
- A subpoena
- A claim against the District
- A demand letter
- A threatened lawsuit
- An investigation
- An incident that the District's General Counsel determines creates a reasonable anticipation of litigation
- Another circumstance requiring preservation of District records

District personnel who become aware of circumstances that may reasonably require a litigation hold shall promptly notify their supervisor and/or District's General Counsel.

DETERMINATION AND SCOPE OF HOLD

Upon learning of pending or reasonably anticipated litigation, District's General Counsel shall determine whether a litigation hold is appropriate.

If a hold is required, District's General Counsel shall determine the scope of the hold.
The scope should identify, as appropriate:

- Legal matter or case name
- Case number, if applicable
- General subject matter
- Relevant claims or issues
- Relevant date range
- Departments involved
- Individual custodians
- Types of records
- Electronic systems
- Email accounts
- Network locations
- Cloud applications
- Mobile devices
- Text messaging or other communication platforms
- Physical records
- Other sources of potentially relevant information

Not every litigation hold will require preservation of every type of record or information. The scope should be reasonably designed for the circumstances of the matter. The District's General Counsel shall provide guidance on the scope.

ISSUANCE OF LITIGATION HOLD NOTICE

District's General Counsel shall issue or approve a written Litigation Hold notice.

DISTRIBUTION OF HOLD NOTICE

The Board Secretary shall distribute the Litigation Hold notice to identified custodians and responsible managers.

Depending upon the matter, recipients may include:

- Department Directors
- Managers
- Individual employees
- General Manager
- IT personnel
- Human Resources
- Records management personnel

Recipients shall be required to acknowledge receipt of the Litigation Hold notice.

PRESERVATION OF RECORDS

Upon receipt of a Litigation Hold notice, custodians shall immediately preserve potentially relevant records, suspend routine destruction or deletion of affected records, preserve electronic and physical records, and avoid altering potentially relevant information.

ELECTRONIC RECORDS AND INFORMATION TECHNOLOGY

When a litigation hold involves ESI, the Board Secretary shall coordinate with Information Technology and District's General Counsel. IT shall assist, as directed, with identifying and preserving information located within District-controlled systems. Custodians shall also preserve District-business records within their possession or control on personal devices or accounts when those records are within the scope of the hold. The specific preservation method shall be determined based on the nature of the information and direction from District's General Counsel. The goal should be preservation of information in its native format whenever reasonably possible.

PHYSICAL RECORDS

Physical records within the scope of a litigation hold shall be preserved in their existing location or moved to another secure location as appropriate. Where an original record is necessary for preservation, the original record shall be retained.

If a copy is sufficient, the District may retain a copy while continuing to retain sufficient information to identify the location of the original record.

RECORDS RETENTION SCHEDULE

A litigation hold supersedes the District's ordinary records retention and destruction schedule for records within the scope of the hold.

Records subject to a litigation hold shall not be destroyed solely because their ordinary retention period has expired. Records outside the scope of the hold remain subject to the District's normal retention schedule.

EMPLOYEE SEPARATION OR TRANSFER

When an employee who is subject to a litigation hold resigns, retires, is terminated, transfers departments, or otherwise separates from the District, the employee's

department shall notify the Board Secretary, Human Resources, and/or the District's General Counsel.

The Board Secretary shall coordinate with District's General Counsel and IT to determine whether additional preservation measures are warranted.

Before separation, or promptly after an unanticipated separation, the District shall take reasonable steps to preserve District information in the employee's possession or control that is subject to the hold.

ACKNOWLEDGMENT AND COMPLIANCE

Each recipient of a Litigation Hold notice shall acknowledge receipt and confirm that they understand their obligation to preserve information within its scope.

The Board Secretary shall track outstanding acknowledgments. Failure to acknowledge a notice shall be reported to the responsible Department Director and, when appropriate, the District's General Counsel.

PERIODIC REVIEW AND MONITORING

Litigation holds shall not be considered a one-time notification. District's General Counsel, with administrative assistance from the Board Secretary, should periodically review active holds to determine whether:

- Additional custodians have been identified
- Additional departments are involved
- The scope of the hold has changed
- New electronic systems or information sources have become relevant
- Personnel have separated from the District
- Additional preservation steps are necessary
- If the hold is still necessary

When appropriate, District's General Counsel may issue a supplemental or amended Litigation Hold notice.

LITIGATION HOLD LOG

The Board Secretary shall maintain an access-restricted Litigation Hold Log containing, at minimum:

Field	Information
Litigation Hold Number Assigned	Unique identification number
Matter	Name/description of matter
Counsel	District's General Counsel responsible
Date Initiated	Date hold was issued.
Departments	Departments affected
Notice Date	Date notice distributed
Acknowledgments	Status
Modifications to the Hold	Dates/details, if applicable
Status	Active / Released
Release Date	Date released
Release Authority	District's General Counsel

The Litigation Hold Log shall be maintained with restricted access and in accordance with the District's General Counsel's direction, the District's retention schedule, and applicable law. If disclosure is requested, the District's General Counsel shall evaluate applicable privileges and exemptions. This policy does not create a categorical exemption from disclosure.

RELEASE OF LITIGATION HOLD

Only District's General Counsel may authorize release of a litigation hold. When District's General Counsel determines that the hold is no longer necessary, District's General Counsel shall issue a written Release of Litigation Hold. The Board Secretary shall distribute the release to all affected departments and custodians. After release, records shall again be managed pursuant to the District's applicable records retention schedule unless another legal hold, statutory requirement, or other preservation obligation applies.