HEATHER GLEN COMMUNITY SERVICES DISTRICT

POLICY TITLE: **Privacy and Data Protection Policy**
POLICY NUMBER: **2440**
ADOPTED BY BOARD OF DIRECTORS: **03/27/2025**
PROPOSED AMENDMENT ADOPTION: **9/24/2026**; will supersede previous policy 03/27/25

2440.1 - Purpose and Scope

The Heather Glen Community Services District ("District") is committed to protecting personal, confidential, and sensitive information collected or maintained in connection with District operations and services.

This policy establishes requirements for the collection, use, access, disclosure, storage, retention, protection, and lawful disposition of such information in accordance with applicable federal and state law and District policy.

This policy shall be administered in conjunction with the California Public Records Act Policy and Procedures, Records Retention and Management Policy, Contractors and Consultants Policy, and other applicable District policies.

Nothing in this policy creates an exemption from public disclosure that does not otherwise exist under law.

2440.2 - Privacy Policy

2440.2.1 Data Collection

The District collects and processes personal information only for lawful, legitimate, and specified purposes related to District operations and the provision of water, sewer, road maintenance, and other District services, as applicable. The District collects personal information, including:

- **Contact Information:** Name, mailing address, phone number, and email address.
- Account Information: Service address, account number, payment history, and billing details.
- **Usage Data:** Water consumption data, sewer usage (for those receiving sewer services), and related service information.
- **Emergency Contact Information (optional):** Name and contact details of a designated emergency contact person.

The District will:

- Collect data only for specific administrative and operational purposes.
- Limit data collection to the minimum necessary to fulfill the stated purposes.
- Obtain consent from individuals for the collection and use of personal data when required by law.

- Use personal information only for lawful District purposes reasonably related to District operations, services, administration, financial management, legal compliance, or other authorized governmental purposes.

2440.2.2 Data Use

The District may use personal information for the following authorized purposes:

- **Service Provision:** To establish and maintain district water, sewer, and road services, as applicable. For those receiving water service only, this will be limited to water service provision.
- **Billing and Payments:** To issue bills, process payments, and manage your account.
- **Customer Support:** To address service inquiries, issues, or requests.
- **Legal Compliance:** To meet local, state, and federal regulations.
- **Communication:** To provide account updates, service notices, service disruption information, policy notices, and other communications related to District operations and services.

2440.2.3 Individual Access and Correction

Individuals may contact the District to request access to or correction of information concerning their own District account or services, subject to applicable law, identity verification requirements, District record-retention requirements, and other legal obligations.

The District will make reasonable efforts to correct inaccurate account or contact information when appropriate.

Requests to delete District records are subject to the **Records Retention and Management Policy**, applicable law, pending public records requests, litigation holds, audits, investigations, and other legal preservation requirements. The District shall not destroy a record solely because an individual requests deletion when retention of the record is required or authorized by law or District policy.

Requests for public access to District records shall be processed under the **California Public Records Act Policy and Procedures**.

2440.2.4 Data Protection and Security

The District shall use reasonable administrative, technical, and physical safeguards appropriate to the nature of the information maintained and the systems used by the District.

Safeguards may include, as appropriate:

- Access controls and account-security measures;
- Use of encryption or other appropriate security measures;

- Limiting access to persons with a legitimate District business need;
- Secure storage and transmission practices;
- Appropriate backup and recovery measures;
- Periodic review of access and security practices; and
- Privacy and information-security guidance or training for Directors, contractors, consultants, and other persons with authorized access to District information.

No information system can be guaranteed to be completely secure. The District shall take reasonable measures to reduce foreseeable risks and respond appropriately to suspected or confirmed security incidents.

2440.2.5 Disclosure and Third-Party Service Providers

The District may disclose personal or confidential information to contractors, consultants, governmental agencies, financial institutions, service providers, or other persons when reasonably necessary for authorized District purposes or when required or permitted by law.

The District does not sell or rent customer personal information.

Contractors or service providers that receive or maintain protected District information shall be subject to appropriate confidentiality, information-security, record-retention, incident-notification, and return-or-disposal requirements through their contract, agreement, terms of service, or other appropriate written arrangement.

Disclosure of District records in response to a public records request shall be governed by the **California Public Records Act Policy and Procedures** and applicable law.

Utility customer information shall be protected in accordance with applicable law.

2440.3 - Third-Party Data Protection Requirements

Contractors, consultants, service providers, and other third parties that access, process, store, or maintain personal, confidential, or sensitive District information shall protect that information consistent with applicable law, their contractual obligations, and District policy.

When appropriate based on the nature and sensitivity of the information involved, District agreements should address:

- Permitted use of District information;
- Confidentiality and restrictions on unauthorized disclosure;
- Appropriate information-security safeguards;
- Access limitations;
- Security-incident and data-breach notification;

- Cooperation with District investigations or legally required notifications;
- Preservation and production of District records;
- Return of District records upon termination; and
- Secure deletion of duplicate information when authorized and when no retention obligation applies.

District records shall not be destroyed by a contractor or service provider contrary to the **Records Retention and Management Policy**, a pending public records request, litigation hold, audit, investigation, or other legal preservation requirement.

2440.3.1 Security Incidents and Data Breach Notification

Suspected unauthorized access, acquisition, use, loss, or disclosure of protected District information shall be reported promptly to the General Manager / Board Secretary.

The District shall evaluate suspected security breaches and provide notifications required by applicable law, including Civil Code §1798.29. Required notifications shall be made within the time and in the manner prescribed by law.

Contractors and service providers with access to protected District information shall be required, where appropriate, to promptly notify the District of suspected or confirmed security incidents affecting District information and to reasonably cooperate with the District's response.

2440.4 - Compliance and Enforcement

Directors, contractors, consultants, and other authorized users of District information shall promptly report known or suspected privacy or information-security incidents to the General Manager / Board Secretary.

The District may provide privacy and information-security guidance or training as appropriate.

Failure to comply with this policy may result in contractual remedies, restriction or termination of access to District systems or information, termination of a contract when authorized, or other lawful corrective action.

2440.5 - Review and Updates

This policy shall be reviewed periodically and updated as necessary to reflect changes in applicable law, District operations, technology, information-security practices, or related District policies.

2440.6 - Contact Information

For questions or concerns regarding the District's privacy policy or data protection practices, please contact the District at heatherglencsd@gmail.com.

2440.7 – Relationship to Public Records and Record Retention
Protection of personal or confidential information under this policy shall be administered consistently with the California Public Records Act Policy and Procedures and the Records Retention and Management Policy.

This policy does not independently make a District record confidential or exempt from disclosure. Records shall be withheld or redacted from public disclosure only when authorized or required by applicable law.

Likewise, the fact that information is confidential or exempt from public disclosure does not authorize its destruction before expiration of the applicable retention period or other legal preservation requirement.