

Weber Mosquito Abatement District

Data Privacy Policy

I. Authority

This policy is established pursuant to the Government Data Privacy Act (Utah Code § 63A-19-101 et seq.), the Government Records Access and Management Act (GRAMA, Utah Code § 63G-2-101 et seq.), and the Utah Division of Archives and Records Services provisions for records management (Utah Code § 63A-12-100 et seq.). It aligns with state requirements for data privacy, records management, and data governance.

II. Purpose

The purpose of this policy is to document the Weber Mosquito Abatement District's ("District") privacy program, including its practices and procedures for handling personal data in compliance with the Government Data Privacy Act. This policy is designed to safeguard individual privacy rights, promote transparency, maintain the security and integrity of personal data, and ensure accountability in the District's operations. This policy will guide the District's current and future personal data practices and ensure they remain in alignment with applicable law.

III. Scope

This policy applies to all District employees and officials who create, manage, or have access to records containing personal data as part of their duties. It also applies to any contractors or service providers that may access or process personal data on the District's behalf to the same extent as District employees. The policy covers all personal data that the District collects and processes.

IV. Definitions

- A. Personal Data:** For purposes of this policy, "personal data" means information that is linked or reasonably linkable to an identified or identifiable individual. In practice, this includes information such as an individual's name, contact details, and any other information that could be used to identify them.

V. Personal Data Collection and Use

The District collects personal data only in limited circumstances in order to carry out its mission of mosquito abatement. The types of personal data and their uses are as follows:

- A. Service Request Information:** Individuals who request mosquito spraying services provide personal contact information to the District. This includes the individual's name, service address, telephone number, and (if the request is submitted through the District's website) an email address. The District collects this information either through an online request form on its website or via phone request. This personal data is used only for the

purpose of scheduling and performing mosquito abatement services at the requested location and for any necessary follow-up communication.

B. Surveillance Footage: The District operates security cameras at its facilities to protect District property, equipment, and personnel. These surveillance cameras may record video of individuals (e.g. employees, visitors, or members of the public) when they are on or around District premises. The video footage is used solely for security and safety purposes, such as monitoring facilities and investigating any security incidents.

C. Cookies: The District's website does not use cookies, analytics tools, advertising trackers, or any other website tracking technologies. No user data is collected or stored automatically when you browse the website.

The categories listed above represent the only personal data the District currently collects. The District does not collect any sensitive personal information such as social security numbers, financial information, biometric identifiers, or medical data, etc., as those are outside the scope of the District's services.

VI. Data Minimization and Use Limitation

The District only collects the personal data that is reasonably required to accomplish a clearly defined purpose, and no more. Personal data will be processed and used only for the purpose for which it was collected and for closely related operational purposes. In accordance with Utah law, personal data provided by an individual will only be used for the purposes identified in the privacy notice given to that individual. If the District ever needs to process personal data for a purpose other than what was originally disclosed, it will first update this policy and the relevant privacy notices to reflect the new use and ensure ongoing compliance.

VII. Privacy Notices and Transparency

In compliance with the Government Data Privacy Act, the District provides clear privacy notices to individuals at the point of data collection, and maintains a public privacy notice on its website:

A. Personal Data Collection Notice: Whenever the District requests or collects personal data from an individual, the District will provide a privacy notice to that individual at the time of collection. This notice will inform the individual about how their personal data will be used and managed. Specifically, if the personal data being collected is not classified as a public record under GRAMA, the notice will describe:

- i. the purposes for which the data is being collected and intended to be used;
- ii. any consequences for refusing to provide the data (for instance, the District may be unable to fulfill a spray request without a service address or contact info);
- iii. the classes of recipients with whom the District may share the data (for example, that the data will be used internally by District staff and not shared

with outside entities, and affirming that the District does not sell personal data); and

- iv. the record series in which the data will be maintained (i.e. the District's "Service Request" records series under its retention schedule).

This privacy notice will be provided in a manner consistent with Utah Code § 63A-19-402(3) – for example, the text of the notice may be included on the website where the service request form is submitted, or if collected by phone, the phone system will direct callers to the written notice available on the District's website. Where the personal data processing serves a public safety or security purpose (such as the operation of the District's surveillance cameras), the District may satisfy the notice requirement by posting a clear privacy notice about those activities on its website.

The District will also, upon request, provide an individual with the applicable privacy notice for any personal data that the individual previously provided.

B. Website Privacy Notice: The District maintains its own official website, and in accordance with Utah Code § 63A-19-402.5, the District provides a website privacy notice accessible on the site's homepage. This website privacy notice informs users about the following key points:

- i. the identity of the governmental entity operating the website (the Weber Mosquito Abatement District);
- ii. how to contact the District for any questions or concerns (e.g. phone number, email, or mailing address for the District's office);
- iii. how a user can access personal data or other information the District may have about them, request correction or amendment of their personal data, and how to file a complaint with the state Data Privacy Ombudsperson regarding the District's data practices; and
- iv. instructions for an "at-risk" government employee (as defined in Utah Code § 63G-2-303) on how they may request that their personal information be classified as a private record under GRAMA.

These two notices may be combined for the sake of convenience and will be available via a clear link on the website's homepage, so that users can easily find this information.

Through these measures, the District ensures that individuals are informed about how their personal data will be used and protected at the time they engage with the District. The District's goal is to be transparent about its data practices and to provide individuals with confidence that their personal information is handled lawfully and responsibly.

VIII. Data Sharing and Disclosure

The District does not share personal data with any third parties. Personal information collected by the District (such as service request details) is used internally and only shared with District

personnel who need the information to perform their duties (for example, field technicians who need to know service addresses). The District will only share personal data with outside entities where there is a clear legal obligation to do so. Such circumstances might include complying with a lawful public records request under GRAMA (after appropriate review and redaction of private information), responding to a court order or subpoena, or coordinating with other government agencies for a legitimate governmental purpose.

The District does not sell personal data under any circumstances. Selling personal data is strictly prohibited.

The District currently does not utilize any third-party data processors or contractors for handling its personal data, there are no routine disclosures to outside vendors. If the District were to engage a contractor or partner in the future that involves personal data processing, the District would ensure that appropriate privacy protections and contractual terms are in place, consistent with the requirements of the Government Data Privacy Act.

IX. Data Retention and Disposal

The District retains and disposes of records containing personal data in accordance with an approved records retention schedule. All personal data collected by the District is part of an official record series with a defined retention period.

Personal data provided through mosquito spray service requests is maintained for 2 years from the date of collection, after which the records are destroyed or deleted in accordance with the District's retention schedule.

Surveillance video recordings are treated as transient records and are retained only until any related security issue or incident has been resolved. If no incident occurs, the footage is overwritten or erased after a short operational period (consistent with the Utah General Retention Schedule for surveillance recordings).

If an individual's personal data needs to be retained longer due to an ongoing matter (such as a pending GRAMA request, audit, or legal hold), the District will retain it as required, but once those obligations are satisfied, the data will be disposed of without delay.

X. Data Security and Breach Notification

The District implements reasonable administrative, technical, and physical safeguards to ensure that personal data is protected against unauthorized access, use, alteration, or destruction.

Examples of these safeguards include: restricting access to personal data only to those District personnel who need it for their job duties (access controls and staff confidentiality obligations); maintaining secure passwords and user authentication for electronic systems; using updated anti-malware software and secure network practices for District IT resources; and physically securing paper records or devices that contain personal information. The District follows industry best practices to guard against data breaches or other security incidents.

In the event of a security incident or data breach involving personal data, the District will promptly take steps to contain and investigate the incident in accordance with its incident response procedures. A “data breach” is defined generally as any unauthorized access, acquisition, disclosure, or loss of personal data held by the District. If the District discovers a data breach that affects personal data, it will fulfill all notification obligations required under the Government Data Privacy Act and other applicable laws.

If a data breach is discovered that involves 500 or more individuals’ personal data, the District will notify the Utah Cyber Center (Utah Department of Technology Services) and the Utah Office of the Attorney General without unreasonable delay (and no later than five days after discovery of the breach).

For any data breach (regardless of size), the District will document the incident internally by creating an internal incident report and will cooperate fully with state authorities (such as the Cyber Center) to mitigate the breach and prevent future incidents.

If a data breach is likely to result in harm or affects the privacy of individuals, the District will provide timely notice to the affected individuals or their legal guardians. Such notice to individuals will be given after the District has determined the scope of the breach and secured its systems, and it will be provided without unreasonable delay, consistent with the requirements of Utah Code § 63A-19-406. The breach notification to individuals will include information about what happened, the types of personal data involved, steps the District is taking to address the breach, and advice on what the individuals can do to protect themselves. Notification may be provided via written letters, electronic means, or other methods most likely to reach the affected persons.

XI. Training and Compliance

Maintaining compliance with data privacy requirements is an ongoing effort, and the District assigns general responsibilities to ensure adherence to this policy and applicable laws:

- A. Employee Training:** All District employees who have access to personal data as part of their job duties are required to complete data privacy training as mandated by the Government Data Privacy Act. New employees must complete the approved privacy training within 30 days of starting employment, and all relevant employees must undergo refresher privacy training at least annually thereafter.
- B. Chief Administrative Officer:** The District’s Executive Director will designate a Chief Administrative Officer (CAO) for privacy and records. The CAO is responsible for oversight of the District’s records management and data privacy program. The CAO’s duties include implementing this policy, ensuring compliance with the Government Data Privacy Act, and coordinating with state oversight bodies (such as the State Archives and the Utah Office of Data Privacy) as needed. The CAO will

also ensure that the District inventories its personal data processing activities and that any new processing activity is reviewed for compliance prior to implementation.

- C. Records Officer:** The CAO may appoint another employee to be the Records Officer, or the CAO may fulfill the responsibilities of the Records Officer. The Records Officer is responsible for the day-to-day management of District records, including classification of records, maintaining the retention schedule, and handling records requests. The Records Officer serves as the liaison with the Utah Division of Archives and Records Services for records scheduling, retention, and disposition matters.
- D. Privacy Issues/Data Requests:** Employees must immediately report to the CAO/Records Officer any potential privacy issues, such as if personal data is requested by an outside party or if a possible security incident is detected, so that proper procedures can be followed.
- E. Privacy Program Reporting:** The District's CAO shall prepare an annual privacy program report as required by Utah Code § 63A-19-401.3. Such a report (due by the end of each calendar year) will include information such as whether the District has formally initiated its privacy program, a summary of the District's privacy practices, any improvements made or planned, the types of personal data the District shares (if any), and the percentage of employees who have completed the required privacy training.

XII. Policy Updates and Review

The District will review and update this policy as needed to reflect any changes in law, technology, or District practices. At a minimum, the policy will be reviewed annually to ensure it remains accurate and effective. Updates to the policy will be approved by the District's governing board. Any material changes will be communicated to District personnel and, where appropriate, noted in the District's public-facing privacy notice.

Weber Mosquito Abatement District

Website Privacy Notice and Personal Data Collection Notice

Effective Date: January 1, 2026

Contact: For questions or concerns about this notice or your personal data, please contact us at:

Weber Mosquito Abatement District

505 W. 12th Street, Ogden, UT 84404

Phone: (801) 392-1630

Email: keith@webermad.org

1. About This Website

This website is operated by the Weber Mosquito Abatement District, a local government entity in the State of Utah. The District is responsible for mosquito control services within its jurisdiction.

2. Personal Data Collected

The District collects personal data only when it is necessary to provide services or fulfill legal duties. We do not collect personal data from individuals who are simply visiting this website.

You may choose to provide the following information when submitting a Spray Service Request:

- Name
- Service address
- Telephone number
- Email address (if submitted online)

This information is used solely for scheduling mosquito abatement services and communicating with the requestor. It is retained for two years in accordance with the District's approved records retention schedule.

3. Website Tracking and Cookies

The District's website does not use cookies, analytics tools, advertising trackers, or any other website tracking technologies. No user data is collected or stored automatically when you browse the website.

4. Security Camera Disclosure

The District uses security cameras at its physical facilities to enhance public safety and protect District assets and personnel. These cameras may record video footage of individuals entering or moving around District property.

- Footage is used only for security purposes and is not routinely monitored.

- Recordings are retained only as long as necessary to resolve any security concern, and are automatically deleted thereafter unless required for an investigation or legal obligation.
- Access to footage is strictly limited to authorized personnel.

This surveillance serves a public safety purpose and is conducted in accordance with Utah Code § 63A-19-402(5).

5. Use and Sharing of Data

The District uses personal data only for the purposes identified above.

We do not sell personal data under any circumstances.

We do not share your data with any third parties except:

- When required by law (e.g., court order or GRAMA request),
- For internal operational needs (e.g., scheduling services), or
- When necessary to protect public safety.

6. Your Privacy Rights

You have the right to:

- **Access** the personal data we maintain about you.
- **Request corrections** to your personal data.
- **Request an explanation** of how your personal data is used.

To exercise these rights, please contact us using the information listed above. We will respond in accordance with applicable Utah law.

7. Privacy for At-Risk Government Employees

If you are an at-risk government employee (as defined in Utah Code § 63G-2-303), you may request to have your personal data classified as a private record. Contact the District to make this request or for more information.

8. Changes to This Notice

This notice may be updated to reflect changes in the District's privacy practices or applicable law. The most recent version will always be posted on this page.