	RULES AND REGULATIONS	Privacy Program
	Revised Date:	Article: VIII Section: 802.00
	Effective Date: 1/13/2026	Pages: 5
	Kevin Ward Board Chairman	Britt Clark Fire Chief

I. PURPOSE

The purpose serves to document Weber Fire District's privacy program, which includes policies, practices, and procedures for the processing of personal data in accordance with Utah Code § 63A-19-401(2)(a). This policy aligns with the records management and data governance requirements provided in both GRAMA and DARS. Where applicable, this policy will refer to a more specific or detailed policy, procedure, or guidance developed by Weber Fire District.

II. POLICY

Weber Fire District is committed to safeguarding individual privacy rights, ensuring transparency, and maintaining accountability in the handling of personal data. The District will:

- Consolidate privacy practices across all divisions.
- Assign governance roles and responsibilities for data privacy and records management.
- Ensure compliance with applicable state and federal data protection, privacy, and records obligations.
- Protect the integrity and security of personal data while promoting trust and accountability.
- Align the District practices with the Utah State Data Privacy Policy, as outlined in Utah Code § 63A-19-102.

This policy applies to all District employees and contractors who manage, create, maintain, or have access to personal data.

III. PROCEDURES

1. Governance

- One or more individuals shall be designated A Chief Administrative Officer(s) to fulfill the duties as outlined in Utah Code § 63A-12-103.
- CAOs shall appoint Appointed Records Officers (AROs) to fulfill responsibilities for records management, scheduling, classification, designation, access, privacy, and preservation.

- Designations and appointments must be reported to the Utah Division of Archives and Records Services (Archives) within 30 days of appointment.
- The designation of, and responsibilities assigned to, a CAO(s) and ARO(s) shall be reviewed and confirmed by the District on an annual basis.

2. Records Series

- Each should create, maintain, designate, and classify records and records series in compliance with DARS and GRAMA in addition to correlated guidance issued by Archives.
- CAO(s) shall be responsible for submitting proposed retention schedule for each type of material defined as a record under GRAMA to the State Archivist for review and approval by the Records Management Committee (RMC).
- Upon approval by the RMC, the District shall maintain and dispose of records in strict accordance with the approved retention schedule. In instances where the District has not received an approved retention schedule for a specific type of record, the general retention schedule maintained by the state archivist shall govern the retention and disposition of those records.
- Privacy annotations are required for all record series containing personal data pursuant to Utah Code § 63A-12-115. They shall be conducted and reported in accordance with additional requirements provided by Archives via administrative rule.
  A. Privacy annotations shall include:
     I. The legal authority under which personal data is processed.
     II. The purposes and uses for the personal data; and
     III. The types of personal data that may be processed within the record series.

3. Awareness & Training

- All employees with access to personal data must complete Data privacy training within 30 days of hire and annually thereafter. In addition to the general privacy training the District may create and require employees to complete agency-specific privacy training tailored to unique privacy needs, practices, and requirements of the agency.
- CAO(s) shall ensure that AROs successfully complete annual GRAMA and records management training and maintain certification through Archives annually.
  A. AROs who handle GRAMA transparency responsibilities are required to complete the GRAMA transparency training and obtain certification from Archives in accordance with Utah Code § 63A-12-110.

B. AROs specializing in records management or privacy are required to complete both records management and GRAMA transparency training, as well as obtain the corresponding certifications.

4. Inventorying & Impact Assessments

- The CAO(s) of the District shall maintain a comprehensive inventory.
  - A. All IT systems that may process state or federal data which the state owns or is responsible for, using the standard process that DTS provides.
  - B. All records, record series that contain personal data and the types of personal data included in the records and records series.
  - C. All processing activities, the inventory of which shall include:
    - I. Non-compliant processing activities-pursuant to the GDPA-that were implemented prior to May 1, 2024, and a prepared strategy for bringing the non-compliant processing activity into compliance by no later than January 1, 2027, and
    - II. All processing activities implemented after May 1, 2024, with documentation confirming compliance status.
- The CAO(s) shall ensure that the District completes a Privacy Impact Assessment (PIA) for all IT systems that may process personal data prior to initiating new IT systems or processing activities as required under DTS Information Security Policy 5000-0002. And must maintain a copy of completed assessments for a period of four years.

5. Transparency

- Website Privacy Policy
  - A. The website privacy policy shall be created by the CAO(s) and published on the District's website as outlined in Utah Code § 63A-12-103 and Utah Admin. Code R895-8. and disclose data practices, security measures, and user rights.
    - I. Website privacy policy statement shall disclose:
      1. The identity of the District website operator.
      2. How the District website operator may be contacted.
      3. The personal data collected by the District entity.
      4. The practices related to the disclosure of personal data collected by the District and/or the District's website operator; and
      5. The procedures, if there are any, by which a user of the District may request:
         - a. Access to the user's personal data; and
         - b. Access to correct the user's personal data.
    - II. A general description of the security measures in place to protect a user's personal data from unintended disclosure.
- Privacy Notice

A. Employees shall only collect the minimum amount of personal data reasonably necessary to efficiently complete the intended purpose.
B. Individuals must receive a privacy notice when asked to provide personal data that complies with Utah Code §§ 63G-2-601(2), 63A-19-402, 63D-2-103(2)-(3), or other governing law, as applicable.

6. Individual Requests

- Procedures must allow individuals to access, amend, or restrict access to their personal data.
- GRAMA requests must be handled in accordance with applicable law.

7. Processing Standards

- Only the minimum amount of personal data necessary shall be collected and processed.
- Data may only be shared with appropriate legal authority; the sale of personal data is prohibited unless required by law.
- Records must be retained and disposed of according to the approved retention schedules.

8. Information Security

- The District follows the DTS Cybersecurity Incident Response Plan>
- Data breaches must be reported in accordance with Utah Code § 63A-19-405 and 406.
- Additional division-specific breach notification policies may be required for compliance with federal law (e.g. HIPAA).

9. Surveillance & Tracking Technologies

- Covert surveillance is prohibited unless permitted by law.
- Use of cookies, fingerprinting devices, key loggers, or other tracking technologies requires explicit authorization and documented justification.
- Any authorized tracking must be disclosed in the District's privacy policy, with user consent obtained as required.

III. DEFINITIONS

Key terms used in this policy include:

- **Personal Data:** Information that is linked or can reasonably be linked to an identified or identifiable individual.
- **Processing Activity:** Any operation performed on personal data, including collection, storage, access, use, sharing, or destruction.
- **Record/Record Series:** As defined in Utah Code § 63G-2-103(25).
- **Records Officer (ARO)**: Individual appointed to manage records and privacy responsibilities in coordination with Archives.

- **Classification/Designation/Schedule**: Determinations of access level, categorization, and retention timelines for records under GRAMA.
- **Data Breach:** Unauthorized access, disclosure, or loss of personal data unless determined to have low probability of compromise.
- **Cookie, Fingerprinting Device, Key Logger:** Technologies for user tracking or monitoring, subject to restrictions under this policy.

IV. FORMS AND EXHIBITS

- Privacy Program Requirements - Utah Code § 63A-19-401
- Government Data Privacy Act (GDPA) - Utah Code § 63A-19-101 *et seq.*
- Division of Archives and Records Services (DARS) - Utah Code § 63A-12-100 *et seq.*
- Management of Records and Access to Records at – Utah Administrative Code § R13-2.
- GRAMA Classification Requirements - Utah Code § 63G-2-201
- Privacy Impact Assessments – Utah Privacy; Utah Code § 63A-12-103; Utah Administrative Code § R895-8
- Division of Technology Services (DTS) – DTS Information Security Policy 5000-0002
- Weber Fire District Rules and Regulations (GRAMA) – Rules 800.00 Records Management
- Weber Fire District Privacy Notice(s)
  - Form 802.00 A Request for Privacy Notice
  - Form 802.00 B Request to Amend Corrected Records
  - Form 802.00 C Request At Risk Employee Classification