

Table of Contents

TITLE 1 – CHAPTER 7 – ADMINISTRATIVE POLICIES AND PROCEDURES

PRIVACY POLICY

1.7.1 BACKGROUND	1.7.3
1.7.2 COMPLIANCE WITH STATE LAW	1.7.4
1.7.3 DEFINITIONS	1.7.4
1.7.4 GOVERNANCE	1.7.6
1.7.4.1 Chief Administrative Officer (CAO)	1.7.6
1.7.4.2 Appointed Records Officers (AROs)	1.7.6
1.7.5 Records Series	1.7.7
1.7.5.1 Records and Records Series	1.7.7
1.7.6 Awareness & Training	1.7.7
1.7.6.1 Departmental Data Privacy Training	1.7.7
1.7.6.2 District-Specific Training	1.7.8
1.7.6.3 Appointed Records Officer Training and Certification	1.7.8
1.7.7 Identify	1.7.8
1.7.7.1 Inventorying	1.7.8
1.7.8 Transparency	1.7.9
1.7.8.1 Website Privacy Policy	1.7.9
1.7.8.2 Privacy Notice	1.7.9
1.7.9 Individual Requests	1.7.10
1.7.10 Processing	1.7.10
1.7.10.1 Minimum Data Necessary	1.7.10
1.7.10.2 Record and Data Sharing or Selling Policy	1.7.11
1.7.10.3 Retention and Disposition of Records Containing Personal Data	1.7.11
1.7.11 Information Security	1.7.12
1.7.11.2 Incident Response	1.7.12
	1.7.1

1.7.11.3 Breach Notification 1.7.12

1.7.12 Surveillance 1.7.13

1.7.12.1 Covert Surveillance 1.7.13

1.7.12.2 Cookies, Fingerprinting, Key Loggers, and Tracking Technologies 1.7.13

TITLE 1 – CHAPTER 7 – ADMINISTRATIVE POLICIES AND PROCEDURES

PRIVACY POLICY

1.7.1 BACKGROUND

A. Policy:

This chapter of the Administrative Policies and Procedures Manual shall be known as the Kearns Improvement District (“District”) Privacy Policy (the “Policy”).

B. Purpose:

This Policy documents the 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) and in alignment with the records management and data governance requirements of both the Government Records Access and Management Act (“GRAMA”) and the Division of Archives and Records Service (“DARS” or “Archives”) and establishes guidelines for protecting privacy rights and the handling of personal information and data that may be collected, used, and/or secured by the District.

C. Guiding Principles:

This Policy consolidates privacy practices, outlines governance roles and responsibilities, and ensures compliance with generally applicable records management, data protection, and data privacy obligations. It is designed to safeguard individual privacy rights, promote transparency, maintain the integrity and security of personal data, and ensure accountability. This Policy is meant to guide further alignment of the District with the State Data Privacy Policy as detailed in Utah Code § 63A-19-102.

D. Scope:

This Policy applies to all District employees involved in the management, creation, and maintenance of records or who have access to personal data as part of their job duties. As provided in Utah Code § 63A-19-401.4, this Policy also applies to all contractors that process or have access to personal data as part of the contractor’s duties under an agreement with the District.

1.7.2 COMPLIANCE WITH STATE LAW

A. **State Law to Govern:**

In the event of any inconsistency or conflict between the Policy and any provision of the Utah Code that is applicable to the District, including but not limited to the Government Data Privacy Act (“GDPA”), (Title 63A, Chapter 19, particularly Part 4, excluding § [63A-19-401.1](#)), GRAMA (Title 63G, Chapter 2), and the Governmental Immunity Act of Utah (Title 63G, Chapter 7), to the extent specifically applicable to the District, the Utah Code provision shall control.

1.7.3 DEFINITIONS

Words and phrases in this Policy that are defined in Utah Code § 63A-19-101 shall have the same definition in the Policy. Other words and phrases may be defined throughout the Policy.

- A. **Classification, classify** and their derivative forms mean determining whether a record series, record, or information within a record is public, private, controlled, protected, or exempt from disclosure under [Utah Code § 63G-2-201\(3\)](#).
- B. **Cookie** means “Technology that records a user’s information and activity when the user accesses websites. Cookies are used by website owners, third parties, and sometimes threat actors to gather user data.”¹
- C. **Data breach** means— “the unauthorized access, acquisition, disclosure, loss of access, or destruction of personal data held by a governmental entity, unless the governmental entity concludes, according to standards established by the Cyber Center, that there is a low probability that personal data has been compromised.”²
- D. **Designation, designate** and their derivative forms mean indicating, based on a governmental entity's familiarity with a record series or based on a governmental entity's review of a reasonable sample of a record series, the primary classification that a majority of records in a record series would be given if classified and the classification that other records typically present in the record series would be given if classified.³

¹ Cybersecurity & Infrastructure Security Agency, Project Upskill Glossary. Last visited 1/8/2026 at: <https://www.cisa.gov/resources-tools/resources/project-upskill-glossary>

² Utah Code § 63A-19-101(11)

³ [Utah Code § 63G-2-103\(8\)](#)

- E. Device fingerprinting** means collecting attributes of a user's device configurations to create a trackable profile for the device.
- F. Individual** means a human being.⁴
- G. Key logger** means “a program designed to record which keys are pressed on a computer keyboard...”⁵
- H. Personal data** means information that is linked or can be reasonably linked to an identified individual or an identifiable individual.⁶
- I. Processing activity** means any operation or set of operations performed on personal data, including collection, recording, organization, structuring, storage, adaptation, alteration, access, retrieval, consultation, use, disclosure by transmission, transfer, dissemination, alignment, combination, restriction, erasure, or destruction.⁷
- J. Record** means the same as that term is defined at [Utah Code § 63G-2-103\(25\)](#).⁸
- K. Record series** means a group of records that may be treated as a unit for purposes of designation, description, management, or disposition.⁹
- L. Records officer** means the individual or individuals appointed by the Chief Administrative Officer to work with Archives in the care, maintenance, scheduling, designation, classification, disposal, and preservation of records.¹⁰
- M. Schedule, scheduling**, and their derivative forms mean the process of specifying the length of time each record series should be retained by a governmental entity for administrative, legal, fiscal, or historical purposes and when each record series should be transferred to state Archives or be destroyed.¹¹

⁴ [Utah Code § 63G-2-103\(15\)](#)

⁵ National Institute of Standards and Technology, Computer Security Resource Center, Glossary. Last visited 1/8/2026, at: https://csrc.nist.gov/glossary/term/key_logger

⁶ [Utah Code § 63A-19-101\(24\)](#)

⁷ [Utah Code § 63A-19-101\(27\)](#)

⁸ Only the citation to the definition of “record” is provided here due to the length of the definition.

⁹ [Utah Code § 63G-2-103\(26\)](#)

¹⁰ [Utah Code §§ 63G-2-103\(27\)](#) and 63A-12-103(2)

¹¹ [Utah Code § 63G-2-103\(28\)](#)

1.7.4 GOVERNANCE

1.7.4.1 Chief Administrative Officer (CAO)

- A. Unless the District Board of Trustees designates the General Manager to be the Chief Administrative Officer (“CAO”), the General Manager shall designate an individual to serve as CAO of the District to fulfill the duties outlined in [Utah Code § 63A-12-103](#).
- B. The designation of a CAO shall be reported to Archives within 30 days after the designation.
- C. The designation of a CAO shall be reviewed and confirmed by the District on an annual basis.

1.7.4.2 Appointed Records Officers (AROs)

- A. The CAO shall appoint one or more individuals to serve as records officers in fulfilling the duties of working with Archives and the Office of Data Privacy in the care, maintenance, scheduling, disposal, classification, designation, access, privacy, and preservation of records.¹²
- B. The CAO may assign responsibility for records officer duties to one or more records officers as the CAO deems appropriate.
- C. The appointment of a records officer shall be reported to Archives within 30 days of the appointment.
- D. If responsibility for the duties of appointed records officers are divided between more than one records officer, such specification should be reported to Archives along with the appointment.
- E. The appointment of, and responsibilities assigned to, a records officer shall be reviewed and confirmed by the District on an annual basis.

¹² [Utah Code § 63A-12-103\(2\)](#)

1.7.5 Records Series

1.7.5.1 Records and Records Series

- A.** The District shall create and maintain records and records series in accordance with the requirements provided by DARS and in GRAMA in addition to correlated guidance issued by Archives.
- B.** The District shall appropriately designate and classify records and records series in accordance with requirements provided by DARS and in GRAMA.
- C.** The CAO may submit a proposed retention schedule for each type of material defined as a record under GRAMA to the state archivist for review and final approval by the Records Management Committee (“RMC”).
- D.** 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 in which event the general retention schedule shall be deemed to have been adopted by reference as the District’s approved retention schedule.

1.7.6 Awareness & Training

1.7.6.1 Departmental Data Privacy Training

- A.** The CAO shall ensure that all employees that have access to personal data as part of the employees’ work duties complete a data privacy training program within 30 days after beginning employment and at least once in each calendar year thereafter.
- B.** The CAO is responsible for monitoring completion of data privacy training by such employees.

1.7.6.2 District-Specific Training

- A. In addition to the general privacy awareness training, the District may create and require employees to complete District-specific privacy training tailored to the unique privacy needs, practices, and requirements of the District.

1.7.6.3 Appointed Records Officer Training and Certification

- A. The CAO shall ensure that, on an annual basis, the appointed records officer(s) shall successfully complete online GRAMA training, including GRAMA transparency training, and obtain certification from Archives in accordance with [Utah Code § 63A-12-110](#).
- B. The CAO shall, on an annual basis, review and confirm the certification status of all appointed records officers.
- C. AROs specializing in records management or privacy are required to complete both records management and GRAMA transparency training and obtain the corresponding certifications.

1.7.7 Identify

1.7.7.1 Inventorying

- A. The CAO shall maintain a comprehensive inventory of:
 - a. All records and record series that contain personal data and the types of personal data included in the records and record series.
 - b. All processing activities, the inventory of which shall include:
 - i. Non-compliant processing activities—pursuant to the GDPR—that were implemented prior to May 1, 2024, and a prepared strategy for

timely bringing the non-compliant processing activity into compliance;¹³ and

- ii. All processing activities implemented after May 1, 2024, with documentation confirming compliance status.

1.7.8 Transparency

1.7.8.1 Website Privacy Policy

- A. The CAO shall ensure that the District's website contains a privacy policy statement that discloses:
 - a. The identity of the website operator;
 - b. How the website operator may be contacted;
 - c. The personal data collected by the District;
 - d. The practices related to disclosure of personal data collected by the District and/or the District's website operator; and
 - e. The procedures, if any, by which a user of the website may request:
 - i. Access to the user's personal data; and
 - ii. Access to correct the user's personal data.
 - f. A general description of the security measures in place to protect a user's personal data from unintended disclosure.

1.7.8.2 Privacy Notice

- A. District employees shall only collect personal data from an individual if, on the day the personal data is collected, the District has provided a privacy notice to an individual asked to furnish personal data that complies with Utah Code §§ [63G-2-601\(2\)](#), [63A-19-402](#), or other governing law, as applicable.

- B. Such a personal data request privacy notice shall generally include¹⁴:

¹³ Compliance is required by no later than January 1, 2027, for any processing activity implemented before May 7, 2025. [Utah Code § 63A-19-401\(2\)\(a\)\(iv\)](#)

¹⁴ Utah Code §§ [63G-2-601\(2\)](#) and [63A-19-402](#).

- a. the record series in which the personal data will be included;
- b. the reasons the person is asked to furnish the information;
- c. the intended purposes and uses for the information;
- d. consequences of refusing to provide the information; and
- e. the classes of persons and entities that currently:
 - i. share the information with the District or
 - ii. receive the information from the District on a regular or contractual basis.

1.7.9 Individual Requests

- A.** The CAO shall ensure that the District has established appropriate processes and procedures that facilitate compliance with applicable governing law for handling the following privacy requests of individuals:
 - a. Individuals' requests to access their personal data;
 - b. Individuals' requests to amend or correct their personal data;
 - c. Individuals' requests for an explanation of the purposes and uses of their personal data; and
 - d. At-risk governmental employee requests to restrict access to their personal data.

- B.** The CAO shall ensure that the District has established processes for public access requests to inspect or copy the District's records, which are not requests from individuals to access their personal data as provided in the District's Records Policy.

- C.** The CAO shall ensure that employees of the District follow established practices with respect to records requests and GRAMA.

1.7.10 Processing

1.7.10.1 Minimum Data Necessary

- A.** The CAO shall ensure that the District obtains and processes only the minimum amount of personal data reasonably necessary to efficiently achieve a specified purpose.¹⁵
- B.** The CAO shall see to it that the District’s data collection practices are reviewed regularly to ensure compliance with the data minimization requirement.

1.7.10.2 Record and Data Sharing or Selling Policy

- A.** The District will only share or disclose personal data when there is appropriate legal authority to do so. The sale of personal data is prohibited unless required by law.
- B.** Data sharing must comply with GRAMA or any other governing law, including sharing data with governmental entities, contractors, private providers, or researchers. Compliance with GRAMA or any other governing law is contingent upon the purpose of the sharing, the parties involved, and the nature of the records.
- C.** The CAO is to report annually to the Chief Privacy Officer regarding the District’s personal data sharing and selling activities, including types of data shared, the legal basis for sharing, and the entities receiving the data.
- D.** All contracts involving personal data must incorporate appropriate privacy protection terms. Written agreements for data sharing are recommended to ensure compliance with applicable laws and regulations.

1.7.10.3 Retention and Disposition of Records Containing Personal Data

- A.** District employees shall maintain, archive, and dispose of records—which includes all personal data—in accordance with an approved retention schedule.¹⁶

¹⁵ [Utah Code § 63A-19-401\(2\)\(a\)\(ii\)](#).

¹⁶ Utah Code §§ [63G-2-604\(1\)](#) and [63A-19-404](#).

- B. District employees shall comply with all other applicable laws, rules and regulations related to retention or disposition of specific personal data held by the District.

1.7.11 Information Security

1.7.11.2 Incident Response

- A. The District will adopt and follow a **Cybersecurity Incident Response Plan** to manage and address all security incidents, including data breaches, and privacy violations.
- B. District employees shall report all suspected security incidents, including non-IT incidents such as unauthorized access to physical records, to the **General Manager**. Any additional District-specific response measures for non-IT incidents are the responsibility of the CAO to develop and implement as appropriate.
- C. The CAO shall ensure compliance with all other applicable laws, rules and regulations related to incident response and breach notification of specific personal data held by the District.

1.7.11.3 Breach Notification

- A. The District is required to provide notice to an individual, or the legal guardian of an individual, if the individual's personal data is affected by a data breach in accordance with [Utah Code § 63A-19-406](#).
- B. The District is required to notify the Utah Cyber Center and the Utah State Attorney General's Office of a data breach affecting 500 or more individuals in accordance with [Utah Code § 63A-19-405](#). If the District experiences a data breach affecting fewer than 500 individuals, the District must create an internal incident report in accordance with [Utah Code § 63A-19-405\(5\)](#). These requirements are in addition to any other reporting requirement to which the District may be subject.
- C. The CAO may be subject to other breach notification requirements, such as those required for compliance with federal regulations, laws or other governing requirements (e.g., HIPAA or 42 CFR Part 2) and any District specific breach

notification policies and procedures that meet the requirements of applicable governing laws and regulations.

1.7.12 Surveillance

1.7.12.1 Covert Surveillance

- A. District employees may not establish, maintain, or use undisclosed or covert surveillance of individuals unless permitted by law.¹⁷
- B. District employees are responsible for engaging with appropriate leadership for review—to include legal counsel where pertinent—of any activity that may be considered a type of surveillance.
- C. The CAO shall ensure that surveillance activities are documented.

1.7.12.2 Cookies, Fingerprinting, Key Loggers, and Tracking Technologies

The District is committed to transparency and privacy protection for individuals that visit the District’s website with regard to the use of any tracking technologies, including but not limited to cookies, device fingerprinting, key loggers, and other similar methods for monitoring or collecting information from website users.

A. Cookies

The use of cookies on the District website and digital services must comply with applicable privacy and security policies. Cookies should be limited to essential operational purposes, and any use of tracking or third-party cookies for analytics or similar functions must clearly be disclosed to users, with an option to consent when required by law.

B. Device Fingerprinting

¹⁷ [Utah Code § 63A-19-401\(3\)\(a\)](#).

Device fingerprinting is prohibited unless explicitly authorized by the CAO and when the legal basis or appropriate justification for such processing is documented. The purpose and extent of fingerprinting must be clearly defined, documented, and disclosed to website users in a privacy notice or statement that complies with applicable legal requirements.

C. Key Loggers

Key loggers are prohibited without specific authorization from the CAO and a documented justification. Key loggers may only be used when there is a clearly defined operational need that complies with security standards and legal requirements, including an appropriate website user notice when required.

D. Other Tracking Technologies

The use of other tracking technologies, such as web beacons, pixel tags, or similar tools, is prohibited unless explicitly authorized by the CAO, and the legal basis for such tracking is documented. Disclosure of these technologies must be included in user-facing privacy statements, with user consent obtained when required by law.

E. User Notification and Consent

The District must ensure that users are informed about the use of tracking technologies. A clear website privacy statement must explain the types of data collected, the purpose of the tracking, and how users can manage their preferences or consent. Any updates to tracking practices must promptly be reflected in the privacy statement.

F. Data Security and Retention

Data collected through authorized tracking technologies must be securely stored, with access limited to authorized personnel. Retention of this data must align with approved retention schedules, and the data should only be retained as long as reasonably necessary for the defined operational purpose.

Approved the 13th day of January 2026

A handwritten signature in dark ink, appearing to read "Cheryle A. Hatch", written over a horizontal line.

Cheryle A. Hatch

Chair

ATTEST:

A handwritten signature in blue ink, appearing to read "F. Greg Anderson", written over a horizontal line.

F. Greg Anderson

General Manager/CEO

4926-2550-5158, v. 9