Government Data Privacy

Policy Application—

This policy does not apply to student data, which is governed by Policy FED Student Data Protection, Policy FE Student Records, and the Family Educational Rights and Privacy Act ("FERPA") and related provisions under 20 U.S.C. §§ 1232g and 1232(h). This policy implements the Government Data Privacy Act (Utah Code Title 63A, Chapter 19) and applies to personal data of individuals other than students which is collected and held by the District. This policy applies to all new processing activity (as defined below) implemented by the District. For any processing implemented by the District before May 7, 2025, the District shall, as soon as reasonably practicable but no later than July 1, 2027, identify and document any non-compliant processing activity, prepare a strategy for bringing it into compliance with the Governmental Data Privacy Act, and include that information in the annual privacy program report.

Utah Code § 63A-19-401(1)(b), (2)(a)(iii), (iv) (2025)

Definitions—

As used in this policy:

1. "Personal data" means information that is linked or can be reasonably linked to an identified individual or an identifiable individual.
2. "Process," "processing," or "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.
3. "High-risk processing activities" means processing of personal data by the District that may have a significant impact on an individual's privacy interests, based on factors that include:
   a. the sensitivity of the personal data processed;
   b. the amount of personal data being processed;
   c. the individual's ability to consent to the processing of personal data; and
   d. risks of unauthorized access or use.

   Such activities may include use of facial recognition technology, automated decision making, profiling, genetic data, biometric data, or geolocation data as those terms are defined in Utah Code § 63A-19-101.
4. "Sell" means an exchange of personal data for monetary consideration by the District to a third party. It does not include a fee charged by the District for

access to a record under GRAMA or assessed in accordance with an approved fee schedule.

5. “Data breach” means the unauthorized access, acquisition, disclosure, loss of access, or destruction of personal data held by the District, unless the District concludes, according to standards established by the Utah Cyber Center, that there is a low probability that personal data has been compromised.

Utah Code § 63A-19-101(11), (17), (24), (27), (33) (2025)

Privacy Program—

The District shall initiate a privacy program before December 31, 2025. The District may meet this requirement by completing the reporting requirement described below in “Annual Report.”

Utah Code § 63A-19-401(2)(a)(i), (b) (2025)

Utah Code § 63A-19-401.3 (2025)

Restrictions on Collection and Dissemination of Personal Data—

The District shall obtain and process only the minimum amount of personal data reasonably necessary to efficiently achieve a specified purpose. The District may only use personal data furnished by an individual for the purposes identified in the privacy notice provided to the individual. The District shall not establish, maintain, or use covert surveillance of individuals unless permitted by law. The District may not sell personal data unless expressly required by law. The District may not share personal data unless expressly permitted by GRAMA or other governing law.

Utah Code § 63A-19-401(1)(b)(ii), (2)(a)(ii), (3) (2025)

Utah Code § 63A-19-402(7) (2025)

Annual Report—

The Superintendent shall annually, before December 31, prepare a report that includes:

1. Whether the District has initiated a privacy program;
2. A description of:
   a. Any privacy practices implemented by the District;
   b. Strategies for improving the District’s privacy program and practices; and
   c. The District’s high-risk processing activities.;
3. A list of the types of personal data that the District currently shares, sells, or purchases;
4. The legal basis for sharing, selling, or purchasing personal data; and
5. The category of individuals or entities:

a. With whom the District shares personal data;

b. To whom the District sells personal data; or

c. From whom the District purchases personal data;

6. The percentage of District's employees that have fulfilled the privacy training requirements; and

7. A description of any non-compliant processing activities identified and the District's strategies for bringing those activities into compliance.

Utah Code § 63A-19-401.3 (2025)

Privacy Notice—

The District shall provide a privacy notice to any individual (or for a minor who is not a student, the individual's legal guardian) from whom the District requests or collects personal data. If the personal data collected by the District would be classified as a public record under Utah Code § 63G-2-301, the privacy notice shall consist of a statement that the individual's personal data may be available to the public as provided by Utah Code § 63G-2-201. Otherwise, the notice shall describe:

1. The intended purposes and uses of the personal data;
2. The consequences for refusing to provide the personal data;
3. The classes of persons and entities:
   a. With whom the District shares personal data or
   b. To whom the District sells personal data; and
4. The record series in which the personal data is or will be included.

The District shall provide the privacy notice by one of the following means:

1. Posting the notice in a prominent place where the District collects the data;
2. Including the notice as part of a document or form used by the District to collect the data; or
3. Including as part of any document or form used by the District to collect personal data, a conspicuous link or QR code that links to an electronic version of the notice.

Upon request, the District shall provide a privacy notice regarding personal data previously furnished by the individual to an individual (or the individual's legal guardian if the individual is a non-student minor).

Utah Code § 63A-19-402 (2025)

Amendment or Correction of Personal Data—

An individual or legal guardian of an individual may request that the District amend or correct personal data about the individual that has been provided to the District. The request shall be in writing and shall specify how the personal data is

inaccurate, misleading, or should otherwise be changed. In evaluating the request, the District may ask for further information from the individual requesting the change. The District shall evaluate the request and determine whether the personal data should be amended or corrected and shall inform the requester in writing of the District's determination. A request does not obligate the District to make the amendment or correction sought.

Utah Code § 63A-19-403 (2024)

Website Domain Requirement—

An "authorized top-level domain" means one of the following suffixes that follow the domain name in a website address: "gov", "edu", and "mil".

Beginning July 1, 2025, the District shall use an authorized top-level domain for the District website and for District email addresses. If the use of an authorized top-level domain by the District is otherwise prohibited, the District shall transition to an authorized top-level domain within 15 months.

Utah Code § 63A-16-110 (2025)

Website Notice Requirement—

A "user" is an individual who accesses a District website.

"User data" means any information about a user that is automatically collected by a District website when a user accesses the website. It includes information that identifies:

1. A user as having requested or obtained specific materials or services from a District website;
2. Internet sites visited by a user;
3. The contents of a user's data-storage device;
4. Any identifying code linited to a user of a District website; and
5. A user's IP or Mac address or session ID.

"Website tracking technology" means any tool used by a District website to monitor a user's behavior or collect user data.

Utah Code § 63A-19-101(37), (38), (39) (2025)

Each District website shall include notice to users of:

1. The District as the entity responsible for the website;
2. How to contact the District;
3. The method by which a user may:
4. Seek access to the user's personal data or user data;
5. Request to correct or amend the user's personal data or user data;

6. File a complaint with the state Data Privacy Ombudsperson; and
7. How an at-risk government employee may request that the employee's personal information be classified as private under Utah Code § 63G-2-302.

Each District website shall also provide notice of:

1. Any website tracking technology that is used to collect user data on the website;
2. What user data is collected by the website;
3. All intended purposes and uses of the user data;
4. The classes of persons and governmental entities with whom the District shares user data or to whom the District sells user data; and
5. The record series in which the user data is included.

These notices shall be provided by prominently posting the notice on the homepage of the website or by prominently posting a link to a separate webpage containing the notices.

Utah Code § 63A-19-402.5 (2025)

Data Breach Notification to Individuals—

The District shall give notice to an individual affected by a data breach after the District determines the scope of the breach and after restoring the reasonable integrity of the affected system, if necessary. (This notice is not required to be given if the personal data involved in the data breach would be classified as a public record under Utah Code § 63G-2-301 and the District prominently posts notice of the data breach on the homepage of its website.) The notice shall be given without unreasonable delay, except that the District shall delay giving notice at the request of a law enforcement agency that determines that notice may impede a criminal investigation. In that case, the notice shall be given when the law enforcement agency informs the District that notice will no longer impede the criminal investigation.

The notice shall include:

1. A description of the data breach;
2. The individual's personal data that was or may have been accessed;
3. Steps the District is taking or has taken to mitigate the impact of the data breach;
4. Recommendations to the individual on how to protect themselves from identity theft and other financial losses; and
5. Any other language required by the Utah Cyber Center.

Unless the District reasonably believes that giving notice would pose a threat to the safety of an individual or unless the individual has designated a preferred method of communication from the District, the District shall provide notice by:

1. Mail or (if reasonably available and allowed by law), email; and
2. One of the following (if the individual's contact information is reasonably available and the method is allowed by law):
    a. Text message, with a summary of the data breach notice and instructions for accessing the full notice; or
    b. Telephone message, with a summary of the data breach notice and instructions for accessing the full notice.

If the data breach affects more than 500 individuals and the District is unable to obtain an individual's contact information to provide notice by one of these methods, the District shall also provide notice of the data breach in a manner that is reasonably calculated to have the best chance of being received by the affected individual or the legal guardian of the individual, such as through a press release, posting on appropriate social media accounts, or publishing notice in a newspaper of general circulation.

Utah Code § 63A-19-406 (2025)

Data Breach Notification to Utah Cyber Center and Attorney General—

The District shall give notice to the Utah Cyber Center and the Utah Attorney General of a data breach that affects 500 or more individuals. The District shall inform the Utah Cyber Center of a data breach that affects fewer than 500 individuals but compromises the security, confidentiality, availability, or integrity of the computer systems used or information maintained by the District. The notice shall be given without unreasonable delay but in any event no later than five days after discovery of the breach.

The notice shall include:

1. The date and time the data breach occurred;
2. The date the data breach was discovered;
3. A short description of the data breach that occurred;
4. The means by which access was gained to the system, computer, or network;
5. The person who perpetrated the data breach;
6. Steps the District is taking or has taken to mitigate the impact of the data breach; and
7. Any other details requested by the Utah Cyber Center.

If this information is not available within five days of discovering the breach, the District shall provide as much of the information as is available and supplement with additional information as soon as it becomes available.

If the data breach affects 500 or more individuals, the District shall also inform the Utah Cyber Center and the Utah Attorney General of the type of personal data involved in the breach and the total number of individuals affected by the breach, including the total number of Utah residents affected.

For any data breach that affects fewer than 500 individuals, the District shall as soon as practicable create an internal incident report containing the information required for a notice to the Utah Cyber Center and shall include additional information in this report as it becomes available. These internal incident reports shall be maintained and provided upon request to the Utah Cyber Center. The District shall also provide an annual report to the Utah Cyber Center which logs all the District data breach incidents affecting fewer than 500 individuals.

Utah Code § 63A-19-405 (2025)

Contractor Obligations—

Any contractor that enters into or renews a contact with the District and whose duties under the contract include processing personal data shall comply with this policy, except such contractors are not subject to the data privacy training requirements. The District's contract with such a contractor shall include this requirement.

Utah Code § 63A-19-401.4 (2025)

Staff Training—

Each employee of the District shall complete a data privacy training program created by the Utah Office of Data Privacy within 30 days after beginning employment and at least once in each calendar year. The District shall ensure that each employee completes this required training.

Utah Code § 63A-19-401.2 (2025)