



Government Data Non-Student Data Privacy
Policy Series: 7000 Community

Policy No. 7400

Purpose

The board of education recognizes the importance of protecting the privacy of personal data collected and maintained by the district. This policy establishes standards for the collection, processing, use, sharing, protection, and management of personal data in accordance with the Government Data Privacy Act. This policy applies to personal data collected by the district relating to individuals other than students and is intended to promote transparency, accountability, and responsible data stewardship while ensuring compliance with applicable state and federal law.

Policy Application

This policy does not apply to student data or education records, which are governed by Policy 3650, Student Data Protection; Policy 3200, Student Records; Policy 3210 the Family Educational Rights and Privacy Act (FERPA); and other applicable federal and state laws.

This policy applies to all personal data collected or processed by the district concerning individuals other than students.

The district shall apply this policy to all new processing activities. For processing activities implemented before May 7, 2025, the district shall identify and document any processing activities that are not compliant with the Government Data Privacy Act, develop a strategy to bring those activities into compliance, and include that information in the district's annual privacy report no later than July 1, 2027.

Definitions:

1. *Data breach* means the unauthorized access, acquisition, disclosure, destruction, or loss of access to personal data maintained by the district, unless the district determines,

40 using standards established by the Utah Cyber Center, that there is a low probability that
41 personal data has been compromised.

- 42
- 43 2. *High-risk processing activity* means processing of personal data that may significantly
44 affect an individual's privacy interests because of the nature, sensitivity, amount, or use
45 of the information.
- 46
- 47 3. *Personal data* means information that is linked or can reasonably be linked to an
48 identified or identifiable individual.
- 49
- 50 4. *Process, processing, or processing activity* means any operation performed on personal
51 data, including collecting, recording, organizing, storing, retrieving, using, disclosing,
52 transferring, modifying, restricting, deleting, or destroying personal data.
- 53
- 54 5. *Sell* means exchanging personal data for monetary consideration and does not include
55 fees authorized under the Government Records Access and Management Act
56 (GRAMA).

57

58

59 **Privacy Program**

60

61 The district shall establish and maintain a comprehensive privacy program designed to ensure
62 compliance with the Government Data Privacy Act.

63

64 The privacy program shall include policies, procedures, administrative safeguards, technical
65 safeguards, employee training, privacy notices, risk assessments, and annual reporting
66 sufficient to protect personal data maintained by the district.

67

68 The district may satisfy the requirement to establish a privacy program through completion of
69 the annual privacy reporting requirements established by this policy.

70

71

72 **Collection and Processing of Personal Data**

73

74 The district shall collect, use, maintain, and process only the minimum amount of personal data
75 reasonably necessary to accomplish a lawful governmental purpose.

76

77 Personal data shall be used only for the purposes identified in the privacy notice provided to the
78 individual at the time the information is collected unless otherwise authorized by law.

79

80 The district shall not establish, maintain, or use covert surveillance of individuals except as
81 expressly authorized by law.

82

83 The district shall not sell personal data except where expressly authorized or required by law.

The district shall not share personal data except as authorized by the Government Records Access and Management Act (GRAMA), the Government Data Privacy Act, or other applicable law.

Annual Privacy Report

On or before December 31 of each year, the superintendent or designee shall prepare an annual privacy report describing the district's privacy program.

The report shall include:

- Whether the district has implemented a privacy program;
- Privacy practices currently implemented by the district;
- Strategies for improving the district's privacy program;
- Any high-risk processing activities conducted by the district;
- Categories of personal data the district shares, sells, or purchases;
- The legal authority for sharing, selling, or purchasing personal data;
- The categories of persons or entities with whom personal data is shared, sold, or purchased;
- The percentage of district employees who completed required privacy training; and
- Any identified non-compliant processing activities together with the district's plan for achieving compliance.

Legal References:

[20 U.S.C. § 1232g](#)

[20 U.S.C. § 1232h](#)

[Utah Code Title 63A, Chapter 19 – Government Data Privacy Act](#)

[Utah Code § 63A-16-110](#)

[Utah Code § 63A-19-101](#)

[Utah Code § 63A-19-401](#)

[Utah Code § 63A-19-401.2](#)

[Utah Code § 63A-19-401.3](#)

[Utah Code § 63A-19-401.4](#)

[Utah Code § 63A-19-402](#)

[Utah Code § 63A-19-403](#)

[Utah Code § 63A-19-405](#)

[Utah Code § 63A-19-406](#)

[Utah Code § 63G-2-301](#)

Board Approved: