Student Data Protection

Policy Series: 3000 Students

Policy No. 3650

Purpose:

The purpose of this policy is to ensure that the District collects, maintains, and uses student data in a manner that supports educational services and complies with applicable laws. The District is committed to protecting the privacy, security, and confidentiality of all student information and will implement safeguards and procedures to prevent unauthorized access, disclosure, or misuse of student data. For more information, please view our data privacy page on our Student Services website: https://provo.edu/student-services/student-data-privacy/

Definitions:

1. "Aggregate Data" means data that:
    a. Are totaled and reported at the group, cohort, school, school district, region, or state level with at least 10 individuals in the level;
    b. Do not reveal personally identifiable student data; and
    c. Are collected in accordance with state board rule.

2. "Biometric Identifier"
    a. Biometric identifier means a:
        i. Retina or iris scan;
        ii. Fingerprint;
        iii. Human biological sample used for valid scientific testing or screening; or
        iv. Scan of hand or face geometry.
    b. "Biometric identifier" does not include:
        i. A writing sample;
        ii. A written signature;
        iii. A voiceprint;
        iv. A photograph;
        v. Demographic data; or
        vi. A physical description, such as height, weight, hair color, or eye color.

3. "Biometric Information" means information, regardless of how the information is collected, converted, stored, or shared:

a. Based on an individual's biometric identifier; and
b. Used to identify the individual.

4. "Cyber security framework" means:
    a. the cyber security framework developed by the Center for Internet Security found at http://www.cisecurity.org/controls/; or
    b. a comparable IT security framework.
5. "Data Breach" means an unauthorized release of or unauthorized access to personally identifiable student data that is maintained by an education entity.

6. "Data Governance Plan" means a comprehensive plan for managing education data that:
    a. Incorporates reasonable data industry best practices to maintain and protect student data and other education-related data;
    b. describes the role, responsibility, and authority of an education entity data governance staff member;
    c. Provides for necessary technical assistance, training, support, and auditing;
    d. Describes the process for sharing student data between the District and another person;
    e. Describes the process for an adult student or parent to request that data be expunged including how to respond to requests for expungement;
    f. describes the data breach response process; and
    g. Is published annually and available on the District's website.

7. "Destroy" means to remove data or a record:
    a. In accordance with current industry best practices; and
    b. rendering the data or record irretrievable in the normal course of business of the District or a third-party contractor.

8. "Disclosure" means permitting access to, revealing, releasing, transferring, disseminating, or otherwise communicating all or any part of any individual record orally, in writing, electronically, or by any other communication method.

9. "Expunge" means to seal or permanently delete data so as to limit its availability to all except authorized individuals.

10. "Metadata Dictionary" means any tool, document, or display that:
    a. Defines and discloses all personally identifiable student data collected and shared by the education entity;
    b. comprehensively lists all recipients with whom the education entity has shared personally identifiable student data, including:
        i. The purpose for sharing the data with the recipient;
        ii. The justification for sharing the data, including whether sharing the data was required by federal law, state law, or a local directive; and

iii. How sharing the data is permitted under federal or state law; and;

c. Without disclosing personally identifiable student data, is displayed on the education entity's website.

11. "Optional Student Data" means student data that is neither necessary student data nor data which the District is prohibited from collecting (as described in Prohibited Collection of Student Data, below).
    a. "Optional student data" includes:
        i. Information that is related to an IEP or needed to provide special needs services but is not "necessary student data";
        ii. Biometric information; and
        iii. Information that is not necessary student data but is required for a student to participate in a federal or other program.

12. "Significant data breach" means a data breach where:
    a. An intentional data breach successfully compromises student records;
    b. A large number of student records are compromised;
    c. Sensitive records are compromised, regardless of number; or
    d. The surrounding circumstances make the breach significant as determined by the District.

District Responsibilities

The District shall annually provide training regarding the confidentiality of student data to any employee with access to education records as defined in FERPA.

The District shall designate an individual to act as a student data manager to fulfill the responsibilities of a student data manager described in *Requirements for Student Data Manager*, below.

If possible, the District shall designate a records officer pursuant to the Government Records Access and Management Act as defined in Utah Code § 63G-2-103(27), as the student data manager.

The District shall also:

1. designate a District Information Security Officer.
2. The District shall implement a cyber security framework.

The District shall create and maintain a District:
1. Data governance plan; and
2. Metadata dictionary.

By November 15 annually, the District shall provide the State Superintendent with the following:

1. The name and contact information of the District's Information Security Officer and its Student Data Manager;
2. Evidence that the District has implemented:
    a. Privacy requirements outlined in:
        i. Utah Code Title 53E, Chapter 9, Part 2, Student Privacy;
        ii. Utah Code Title 53E, Chapter 9, Part 3, Student Data Protection;
        iii. Utah Code Title 63A, Chapter 19, Government Data Privacy Act;
        iv. FERPA; and
        v. 20 U.S.C. 1232h, Protection of Pupil Rights Amendment; and
    b. Other privacy practices identified by the State Superintendent; and
    c. A cybersecurity framework.

The District shall establish an external research review process to evaluate requests for data for the purpose of external research or evaluation. (See Policy 4495.)

Student Data Ownership and Access

A student owns the student's personally identifiable student data. The District shall allow a student or a student's parent (or in the absence of a parent an individual who is acting as the student's parent) to access the student's student data which is maintained by the District.

Data Retention

The District shall classify all student data which it collects under an approved records retention schedule. The District shall retain and dispose of all student data in accordance with an approved records retention schedule.

If no existing retention schedule governs student disciplinary records collected by the District:

1. The District may propose to the State Records Committee a retention schedule of up to one year if collection of the data is not required by federal or state law or Board rule; or
2. The District may propose to the State Records Committee a retention schedule of up to three years if collection of the data is required by federal or state law or State Board rule, unless a longer retention period is prescribed by federal or state law or State Board rule.

The District's retention schedules shall take into account the District's administrative need for the data. Unless the data requires permanent retention, the District's retention schedules shall require destruction or expungement of student data after the administrative need for the data has passed.

A parent or adult student may request that the District amend, expunge, or destroy any record not subject to an approved retention schedule and believed to be inaccurate, misleading, or in

violation of the privacy rights of the student. The District shall process such a request following the same procedures outlined to amend a student education record under FERPA, as set out in Policy 3210 Compliance with FERPA.

Notification in Case of Breach

If there is a release of a student's personally identifiable student data due to a significant data breach, the District shall notify:

1. The student, if the student is an adult student; or
2. The student's parent, if the student is not an adult student.

Within 10 business days of the discovery of a significant data breach (either by the District or by third parties), the District shall report the significant data breach to the State Superintendent.

Prohibited Collection of Student Data

The District may not collect a student's:

1. Social Security number; or
2. Criminal record, except as required in Utah Code § 80-6-103 (Minor taken into custody by peace officer, private citizen, or juvenile probation officer).

Student Data Disclosure Statement

If the District collects student data into a cumulative record it shall, in accordance with this section, prepare and distribute to parents and students a student data disclosure statement that:

1. Is a prominent, stand-alone document;
2. Is annually updated and published on the District's website;
3. States the necessary and optional student data the District collects;
4. States that the District will not collect the student data described in *Prohibited Collection of Student Data,* above;
5. Describes the types of student data that the District may not share without a data authorization;
6. Describes how the District may collect, use, and share student data;
7. Includes the following statement: "The collection, use, and sharing of student data has both benefits and risks. Parents and students should learn about these benefits and risks and make choices regarding student data accordingly.";
8. Describes in general terms how the District stores and protects student data; and
9. States a student's rights under the student data protection statutes.

The notice may also include additional information relating to student and parent privacy, as determined by the District.

Student Data Disclosure Statement Recipients

The District may collect the necessary student data of a student into a cumulative record only if the District provides a student data disclosure statement to:

1. The student, if the student is an adult student; or
2. The student's parent, if the student is not an adult student.

Optional Student Data Collection

The District may collect optional student data into a cumulative record only if it:

1. Provides, to an individual described in *Student Data Disclosure Statement Recipients*, above, a student data disclosure statement that includes a description of:
    a. The optional student data to be collected; and
    b. How the District will use the optional student data; and

2. Obtains a data authorization to collect the optional student data from an individual described in *Student Data Disclosure Statement Recipients*, above.

Student Biometric Identifier and Biometric Information Data Collection

The District may collect a student's biometric identifier or biometric information if the District:

1. Provides, to an individual described in *Student Data Disclosure Statement Recipients*, above, a biometric information collection notice that is separate from a student data collection notice and which states:
    a. The biometric identifier or biometric information to be collected;
    b. The purpose of collecting the biometric identifier or biometric information; and
    c. How the District will use and store the biometric identifier or biometric information; and
2. Obtains written consent to collect the biometric identifier or biometric information from an individual described in *Student Data Disclosure Statement Recipients*, above.

Sharing Student Data

The District may not share a student's personally identifiable student data without written consent, except in conformance with the requirements of this policy and with the Family

Educational Rights and Privacy Act ("FERPA") and related provisions under 20 U.S.C. §§ 1232g and 1232(h).

Requirements for Student Data Manager

The District will designate a student data manager who shall:

1. Authorize and manage the sharing, outside of the District, of personally identifiable student data for the District as described in this section;
2. Act as the primary local point of contact for the state student data officer described in Utah Code § 53E-9-302; and
3. Fulfill other responsibilities described in the District's data governance plan.

Permitted and Prohibited Sharing of Student Data by Student Data Manager

A student data manager may share the personally identifiable student data of a student with the student and the student's parent. Otherwise, a student data manager may only share a student's personally identifiable student data from a cumulative record (including sharing student data with a federal agency) as required by federal law or as follows. Such data may be shared with:

1. A school official;
2. An authorized caseworker, in accordance with this policy, or other representative of the Department of Human Services; or
3. A person to whom the District has outsourced a service or function:
    a. To research the effectiveness of a program's implementation; or
    b. that the District's employees would typically perform.

A student data manager may share a student's personally identifiable student data from a cumulative record with a caseworker or representative of the Department of Health and Human Services if:

1. The Department of Health and Human Services is:
    a. legally responsible for the care and protection of the student; or
    b. providing services to the student; and
2. The student's personally identifiable student data is not shared with a person who is not authorized:
    a. to address the student's education needs; or
    b. by the Department of Health and Human Services to receive the student's personally identifiable student data; and
3. The Department of Health and Human Services maintains and protects the student's personally identifiable student data.

A student data manager may share a student's personally identifiable student data to improve educational outcomes for the student where the student is:

1. In the custody of or under the guardianship of, the Department of Health and Human Services;
2. Receiving services from the Division of Juvenile Justice Services;
3. In the custody of the Division of Child and Family Services;
4. Receiving services from the Division of Services for People with Disabilities; or
5. Under the jurisdiction of the Utah Juvenile Court.

A student data manager may share aggregate data. A student data manager may not share personally identifiable student data for the purpose of external research or evaluation except as follows: If a student data manager receives a request to share data for the purpose of external research or evaluation, the student data manager shall:

1. Verify that the request meets the requirements of 34 CFR § 99.31(a)(6);
2. Submit the request to the District's external research review process; and
3. Fulfill the instructions that result from the review process.

If the student data manager is informed that the State Board of Education intends to share student data collected by the District with the Utah Registry of Autism and Developmental Disabilities, the student data manager shall give notice to the parent of each student whose data is to be shared of the State Board's intention to share the data. This notice shall be provided at least 30 days before the State Board is to share the data. If a parent requests that the State Board not share the data, the student data manager shall relay that request to the State Board.

A student data manager may share personally identifiable student data in response to a subpoena issued by a court.

In accordance with State Board of Education rule, a student data manager may share personally identifiable information that is directory information.

Third Party Contractors

The District may provide a third-party contractor with personally identifiable student data received under a contract with the District strictly for the purpose of providing the contracted product or service within the negotiated contract terms.

When contracting with a third-party contractor, the District shall require the following provisions in the contract:

1. Requirements and restrictions related to the collection, use, storage, or sharing of student data by the third-party contractor that are necessary for the District to ensure compliance with the provisions of the Student Data Protection Act and State Board of Education rules;

2. A description of a person, or type of person, including an affiliate of the third-party contractor, with whom the third-party contractor may share student data;
3. Provisions that govern requests by the District for the deletion of the student data received by the third-party contractor from the District;
4. Except as provided in this policy and if required by the District, provisions that prohibit the secondary use of personally identifiable student data by the third-party contractor; and
5. An agreement by the third-party contractor that, at the request of the District, the District or its designee may audit the third-party contractor to verify compliance with the contract.

A third-party contractor's use of personally identifiable student data shall be in accordance with Utah Code §§ 53E-9-309, 53E-9-310 and FERPA.

If the District contracts with a third-party contractor to collect and have access to the District's student data, the District shall monitor and maintain control of the data.

If the District contracts with a third-party contractor to collect and have access to the District's student data, the District shall notify a student and the student's parent or guardian in writing that the student's data is collected and maintained by the third-party contractor.

Legal References

Utah Code § 53E-9-301 (2023)
Utah Admin. Rules R277-487-2 (July 8, 2025)
Utah Code § 53E-9-303 (2019)
Utah Admin. Rules R277-487-2 (July 8, 2025)
Utah Admin. Rules R277-487-3(1) (July 8, 2025)
Utah Code § 53E-9-304 (2020)
Utah Admin. Rules R277-487-4 (July 8, 2025)
Utah Code § 53E-9-304(2) (2020)
Utah Admin. Rules R277-487-3(3) (July 8, 2025)
Utah Code §53E-9-305(1) (2023)
Utah Code § 53E-9-305(2), (8) (2023)
Utah Code § 53E-9-305(4) (2023)
Utah Code § 53E-9-305(5) (2023)
Utah Code § 53E-9-305(6) (2023)
Utah Code § 53E-9-308 (2023)
Utah Code § 53E-9-308(2) (2023)
Utah Code § 53E-9-308 (2023)
Utah Admin. Rules R277-487-7 (July 8, 2025)
Utah Code § 53E-9-309 (2020)
Utah Code § 53E-9-310 (2019)

Board Approved: