STUDENT DATA COLLECTION NOTICE

Necessary Student Data

Necessary student data means data required by state statute or federal law to conduct the regular activities of the school.

- Student Name, Date of birth, and Sex
- Parent and student contact information and Custodial parent information
- A student identification number (including the student’s school ID number and the state-assigned student identifier, or SSID)
- Local, state, and national assessment results or an exception from taking a local, state, or national assessment
- Courses taken and completed, credits earned, and other transcript information
- Course grades and grade point average
- Grade level and expected graduation date or graduation cohort
- Degree, diploma, credential attainment, and other school information
- Attendance and mobility
- Drop-out data
- Immunization record or an exception from an immunization record
- Race, Ethnicity, or Tribal affiliation
- Remediation efforts
- An exception from a vision screening required under Section 53G-9-404 or information collected from a vision screening described in Utah Code Section 53G-9-404
- Information related to the Utah Registry of Autism and Development Disabilities (URADD), described in Utah Code Section 26-7-4
- Student injury information
- A disciplinary record created and maintained as described in Utah Code Section 53E-9-306
- Juvenile delinquency records
- English language learner status
- Child find and special education evaluation data related to initiation of an IEP

Optional Student Data

We may only collect optional student data with written consent from the student’s parent or from a student who has turned 18.

- Information related to an IEP or needed to provide special needs services
- Biometric information used to identify the student
- Information required for a student to participate in an optional federal or state program (e.g., information related to applying for free or reduced lunch)

Certain sensitive information on students collected via a psychological or psychiatric examination, test, or treatment, or any survey, analysis, or evaluation will only be collected with parental consent. You will receive a separate consent form in these cases. See our Protection of Pupil Rights Act (PPRA) notice for more information.
Prohibited Collections
We will not collect a student’s social security number or criminal record, except as required by Utah Code Section 78A-6-112(3).

Data Sharing
We will only share student data in accordance with the Family Educational Rights and Privacy Act (FERPA), which generally requires written parental consent before sharing student data. FERPA includes several exceptions to this rule, where we may share student data without parental consent. For more information on third parties receiving student information from us, see our Metadata Dictionary.

Student data will be shared with the Utah State Board of Education via the Utah Transcript and Records Exchange (UTREx). For more information about UTREx and how it is used, please visit the Utah State Board of Education’s Information Technology website.

Benefits, Risks, and Parent Choices
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. Parents are given the following choices regarding student data:

- **Choice to request to review** education records of their children and request an explanation or interpretation of the records (see our annual FERPA notice for more information)
- **Choice to contest the accuracy** of certain records (see our annual FERPA notice for more information), potentially leading to the correction, expungement, or deletion of the record
- **Choice to opt into certain data collections** (see the section above on optional data collections)
- **Choice to opt out of certain data exchanges**
  - Information that has been classified as directory information (see our directory information notice for more information)
  - Parents of students with an IEP may have their information shared with the Utah Registry of Autism and Developmental Disabilities (URADD). If included in this data exchange, parents will receive a separate notice within 30 days of the exchange, informing them of their right to opt out, per Utah Code Section 53E-9-308(6)(b)
- **Choice to file a complaint** if you believe the school or its agents are violating your rights under FERPA or Utah’s Student Data Protection Act. If you have a complaint or concern, we recommend starting locally and then escalating to the state and US Department of Education

<table>
<thead>
<tr>
<th>Your local school district or charter school</th>
<th>(insert contact information of the LEA data manager here)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Utah State Board of Education</td>
<td>Report your concern with the <a href="#">USBE hotline</a></td>
</tr>
<tr>
<td>The US Department of Education</td>
<td>Report your concern <a href="#">here</a></td>
</tr>
</tbody>
</table>

Storage and Security
In accordance with Board Rule R277-487-3(14), we have adopted a cybersecurity framework called the [CIS Controls](#).
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 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 cause 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 availability to all except authorized individuals.

10. "Metadata Dictionary" means a record 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 compromised, regardless of number; or
   d. The surrounding circumstances make the breach significant as determined by the District.

*Utah Code § 53F-9-301 (2019)*


---

**District Responsibilities**

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

District employees shall annually submit a certified statement to the District's student data manager, which certifies that the employee has completed the District's required student privacy training and understands student privacy requirements.

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(24), as the student data manager.

The District shall designate a District Information Security Officer:

   Data governance plan; and

The District shall implement a cyber security framework.
The District Shall create and maintain a District:

1. Data governance plan, and

   By October 1 annually, the District shall enter all student data elements shared with third parties into the State Board’s metadata dictionary.

   By October 1 annually, The District shall provide the State Superintendent with evidence that the District has implemented a cyber security framework and the name and contact information of the District Information Security Officer.

   The District shall provide the State Superintendent with a copy or link to the District’s data governance plan by October 1 annually.

   The District shall publicly post the its definition of directory information as defined in FERPA and describe how a student data manager may share personally identifiable information that is directory information. By October 1 annually, the District shall provide the State Superintendent with a copy of or a link to the District’s definition of directory information.

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

\textit{Utah Code § 53E-9-303 (2019)}
\textit{Utah Admin. Rules R277-487-3 (March 13, 2019)}

**Student Data Ownership and Access**—

A student owns the student’s personally identifiable student data.

The District shall allow a student or student’s parent (or in the absence of a parent and individual who is acting as the student’s parent) to access the student’s student data which is maintained by the District.

\textit{Utah Code § 53E-9-304 (2019)}

**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 FE “Right to Amend Records.”


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 or legal guardian, 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—

Beginning with the 2017-18 school year, the District may not collect a student’s:

1. Social Security number; or
2. Criminal record, except as required in Utah Code § 78A-6-112 (Minor taken into custody by peace officer, private citizen, or probation officer).


Student Data Disclosure Statement—

Beginning with the 2017-18 school year, 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**.

_Utah Code § 53E-9-305(2) (2019)_

**Student Data Disclosure Statement Recipients**—

Beginning with the 2017-18 school year, 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.

_Utah Code § 53E-9-305(4) (2019)_

**Optional Student Data Collection**—

Beginning with the 2017-18 school year, 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.

_Utah Code § 53E-9-305(5) (2019)_

**Student Biometric Identifier and Biometric Information Data Collection**—
Beginning with the 2017-18 school year, the District may collect a student’s biometric identifier or biometric information into a cumulative record only 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. §§ 1232(g) 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 from a cumulative record for the District as described in this section; and

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 in accordance with 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 Human Services if:

1. In the custody of or under the guardianship of, the Department of 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 C. F.R. § 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.

*Utah Code § 53E-9-308 (2019)*
**General Non-Disclosure Assurances**

All student data used by NSSD is protected as defined by FERPA and Utah statute. All NSSD staff must sign a NSSD Employee and Volunteer Non-Disclosure Agreement to verify acknowledgement, receipt, and intent to adhere to this Data Governance Policy.

All NSSD employees will do the following:

- Complete student data privacy and security training;
- Consult with NSSD internal data officers when creating or disseminating reports containing data;
- Use password-protected computers/devices when accessing any student-level or staff-level records;
- Refuse to share individual passwords for personal computers or data systems with anyone without authorized access;
- Log out of any data system/portal and close the browser after each use;
- Store sensitive data on appropriate, secured location;
- Keep printed reports with PII in a locked location while unattended;
- Use a secure document destruction service provided at NSSD when disposing of such records;
- Refuse to share personally identifying data during public presentations, webinars, etc., if users need to demonstrate child/staff level data;
- Redact any PII information when sharing sample reports with general audiences in accordance with guidance provided by the student data manager;
- Take steps to avoid disclosure of PII in reports, such as aggregating, data suppression, rounding, recording, blurring, perturbation, etc.;
- Delete files containing sensitive data after using them on computers, or move them to secured servers or personal folders accessible only by authorized parties;
- **NOT** use email to send screenshots, text, or attachments that contain PII or other sensitive information. If users receive an email containing such information, they must delete the screenshots/text when forwarding or replying to these messages. If there is any doubt about the sensitivity of the data the Student Data Privacy manager should be consulted;
- Use secure methods when sharing or transmitting sensitive data as approved by NSSD.
- Share within secured server folders is appropriate for NSSD’s internal file transfer;
• NOT transmit child/staff-level data externally unless expressly authorized in writing by the data owner and then only transmit data via approved methods;
• Limit use of individual data to the purposes, which have been authorized within the scope of job responsibilities.

**Data Breach Protocols**

NSSD shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, NSSD staff shall follow industry best practices in responding to the breach. Furthermore, NSSD shall follow best practices for notifying affected parties, including students, in the case of an adult student, or parents or legal guardians, if the student is not an adult student.

• Concerns about security breaches must be reported immediately to the Superintendent or Director of Educational Technology who will collaborate with appropriate NSSD administrators to determine whether a security breach has occurred.
• If the NSSD administrative team determines that one or more employees or contracted partners have substantially failed to comply with this policy and other relevant privacy policies, the team will determine appropriate consequences, which may include termination of employment or a contract and further legal action.
• Concerns about security breaches that involve the Director of Educational Technology must be reported directly to the Superintendent.
• Concerns about security breaches that involve the Superintendent must be reported directly to the President of NSSD’s Board of Education.
• NSSD will provide and periodically update, in keeping with industry best practices, resources for Utah LEAs in preparing for and responding to security breaches.

**Data Disclosure Protocols**

This plan establishes the protocols and procedures for sharing data maintained by NSSD consistent with the disclosure provisions of the Federal Family Educational Rights and Privacy Act (FERPA) and Utah’s SDPA.

• NSSD will provide parents with access to their child’s educational records, or an eligible student access to his or her own educational records, within 45 days of receiving an official request.
• NSSD is not required to and will not provide information to parents or an eligible student concerning another student, the financial records of parents, and confidential letters of recommendation if the student has waived the right to access.
• NSSD is not required to provide data that it does not maintain, nor is NSSD required to create education records in response to an eligible student’s request.
• Publicly released reports shall not include PII and shall use aggregate data in such a manner that re-identification of individual students is not possible.
• NSSD has clearly defined in its communication policy and in registration materials for parents what data is determined to be directory information.
• NSSD notifies parents in writing at registration about directory information which includes PII and offers parents an opportunity to opt out of the directory. If a parent does not opt out, the release of the information as part of the directory is not a data breach or an unauthorized data disclosure.
• NSSD provides a disclosure statement to parents or guardians of NSSD students that meets the following criteria:
  o A prominent, stand-alone document;
  o Annually updated and published on NSSD’s website;
  o States the necessary and optional student data that NSSD collects;
  o States that NSSD will not collect student data prohibited by the Utah Student Data Protection Act;
  o States that NSSD will not share legally collectible data without authorization;
  o States that students and parents are responsible for the collection, use, or sharing of student data as described in Section 53A-1-1405 which states that a student owns his/her personally identifiable student data and that a student may download, export, transfer, save, or maintain the student’s data, including documents;
  o Describes how NSSD may collect, use, and share student data;
  o Includes the following statements: “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.”
  o Describes in general terms how NSSD stores and protects student data; and
  o States a student’s rights related to his/her data.

DATA SECURITY & PRIVACY TRAINING
• NSSD will provide a range of training opportunities for all NSSD staff, including volunteers, with authorized access to student educational data or confidential educator records in order to minimize the risk of human error and misuse of information.
• NSSD will also require all employees and volunteers to sign both the Employee Responsible Use Agreement, which describes the permissible uses of technology and information, and NSSD’s Confidentiality Agreement, which prohibits employees’ disclosure of confidential personally identifiable information.
• NSSD will also provide targeted security and privacy training for data stewards and IT staff, as well as for any other groups that collect, store, or disclose data.
• Participation in the training is required and documented.

**RECORD RETENTION & EXPUNGEMENT**

NSSD staff shall retain and dispose of student records in accordance with Section 63G-2-604, 53A-1-14-7, and shall comply with active retention schedules for student records per the Utah Division of Archive and Record Services.

• In accordance with 53A-1-1407, NSSD shall expunge student data that is stored upon the request of a student, if the student is at least 23 years old.
• NSSD may expunge medical records and behavioral test assessments.
• NSSD will not expunge student records of grades, transcripts, or records of a student’s enrollment or assessment information except as allowed by law.
• NSSD will collaborate with Utah State Archives and Records Services in updating data retention schedules. Student-level discipline data will be expunged after three years.

**QUALITY ASSURANCES AND TRANSPARENCY REQUIREMENTS**

The quality of data is a function of accuracy, completeness, relevance, consistency, reliability, appropriate accessibility, and data interpretation and use. This policy is structured to encourage the effective and appropriate use of educational data. NSSD acknowledges that adherence to compliance and data-driven decision making guide what data is collected, reported, and analyzed at the school.

• Where possible, data are collected at the lowest level available (at the student/teacher level); no aggregate data collections are necessary if the aggregate data can be derived or calculated from the detailed data;
• For all data collections, NSSD establishes clear guidelines for data collection and the purpose of the data request;
• NSSD’s State-level data are audited by external, independent auditors yearly as a check on accuracy or to investigate the source of any anomalies;
• Before releasing high-risk data, the Superintendent and Director of Educational Technology must complete a review of the reliability, validity, and presentation of the data, and must follow all protocols in this policy related to appropriate disclosure.

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.

Utah Admin. Rules R277-487-3 (March 13, 2019)