STUDENT DATA PROTECTION FEC

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. "**Cumulative Record**" means physical or electronic information that the District intends:
    a. To store in a centralized location for 12 months or more; and
    b. For the information to follow the student through the public education system.
5. "**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. Provides for necessary technical assistance, training, support, and auditing;

c. Describes the process for sharing student data between the District and another person;

d. Describes the process for an adult student or parent to request that data be expunged; and

e. Is published annually and available on the District's website.

6. "**Metadata Dictionary**" means a complete list of student data elements and other education-related data elements, that:

   a. Defines and discloses all data collected, used, stored, and shared by the District, including:

      i. Who uses a data element within the District and how a data element is used within the District;

      ii. If a data element is shared externally, who uses the data element externally and how a data element is shared externally;

      iii. Restrictions on the use of a data element; and

      iv. Parent and student rights to a data element;

   b. Designates student data elements as either

      i. necessary student data or

      ii. optional student data;

   c. Designates student data elements as required by state or federal law; and

   d. Without disclosing student data or security information, is displayed on the District's website.

7. "**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.

Utah Code § 53A-1-1402 (2016)

District Responsibilities—

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(25), as the student data manager.

The District shall create and maintain a District:

1. Data governance plan; and
2. Metadata dictionary.

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

Utah Code § 53A-1-1404 (2016)

Student Data Ownership—

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

A student may download, export, transfer, save, or maintain the student's student data, including a document.

Utah Code § 53A-1-1405 (2016)

Notification in Case of Breach—

If there is a release of a student's personally identifiable student data due to a security 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.

Utah Code § 53A-1-1405 (2016)

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).

Utah Code §53A-1-1406(2) (2016)

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 Act.

Utah Code § 53A-1-1406(3) (2017)

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 § 53A-1-1406(4) (2017)

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 § 53A-1-1406(5) (2017)

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 disclosure statement that is separate from a student data disclosure statement 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 a data authorization to collect the biometric identifier or biometric information from an individual described in **Student Data Disclosure Statement Recipients**, above.

Utah Code § 53A-1-1406(6) (2017)

Sharing Student Data—

Beginning with the 2017-18 school year, the District may not share a student's personally identifiable student data 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).

Utah Code § 53A-1-1409 (2016)

Requirements for Student Data Manager—

Beginning with the 2017-18 school year, 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 § 53A-1-1403.

Utah Code § 53A-1-1409 (2016)

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. The Department of 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 Human Services to receive the student's personally identifiable student data; and
3. The Department of Human Services maintains and protects the student's personally identifiable student data.

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. Submit the request to the District's external research review process; and
2. Fulfill the instructions that result from the review process.

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 § 53A-1-1409 (2016)

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:
    - A prominent, stand-alone document;
    - Annually updated and published on NSSD's website;
    - States the necessary and optional student data that NSSD collects;
    - States that NSSD will not collect student data prohibited by the Utah Student Data Protection Act;
    - States that NSSD will not share legally collectible data without authorization;
    - 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;
    - Describes how NSSD may collect, use, and share student data;
    - 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."
    - Describes in general terms how NSSD stores and protects student data; and
    - 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.

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 §§ 53A-1-1410 and 53A-1-1411.

Utah Code § 53A-1-1410 (2016)