UTAH STATE BOARD OF EDUCATION POLICY
Policy Number: 3006
Policy Name: USBE Data Governance Plan
Date Approved: February 6, 2025

By this policy, the Utah State Board of Education (USBE) establishes the following policy and procedures:

1. Data governance is an organizational approach to data and information management that is formalized as a set of policies and procedures that encompass the full life cycle of data. USBE takes seriously its moral and legal responsibility to protect student privacy and ensure data security. Utah's student Data Protection Act (SDPA), Sections 53E-9-301, et seq., requires that USBE adopt a Data Governance Plan.

2. This policy is applicable to all USBE employees, State Board Members (the Board and supporting staff) temporary employees, and USBE contractors. The policy must be used to assess agreements made to disclose student data to third parties. This policy must also be used to assess the risk of conducting business as it pertains to confidential information as defined in USBE Internal Policy 05-01, Acceptable Use of Information Technology Resources. This policy is designed to help ensure only authorized disclosure of confidential information.

3. Furthermore, this USBE Data Governance Plan works in conjunction with USBE Information Security Policies

4. The Superintendent shall implement a Student Data Protection Advisory Group as described in Section 53E-9-304 and Board Policy 5003.

5. The Superintendent shall review a request for educator data consistent with Title 63G, Chapter 2, Government Records Access and Management Act, and Rule R277-312.

6. Table 1 outlines individual USBE employee responsibilities.

Table 1. Individual USBE employee Responsibilities

Role	Responsibilities
Director of Privacy	Fulfills the role described in Section 53E-9-302(4).
Chief Information Security Officer	Fulfills the role described in USBE Internal Policy 05.02 Information Security.
Records Officer	Fulfills the duties of the Records Officer, as defined in Section 63G-2-103(24).
Records Steward	Departmental/section point of contact for the Records Officer, meets bi-annually with the Records Officer (Fall and Spring), and updates record schedules.
Data and Statistics Director	1. Monitors and trains data stewards on data management; 2. provides bi-annual data quality training to USBE staff that handle student data; 3. coordinates Data Stewards from each section within USBE to review data requests; 4. works closely with IT staff to ensure data quality; 5. helps ensure the proper level of data redaction for publicly posted reports, reports in the Data Gateway, and data that are shared with external entities and researchers; 6. helps ensure proper access levels for the Data Gateway for USBE and LEA employees; 7. documents the names(s), date, and all data elements shared; 8. manages Data Quality Processes; and 9. helps ensure appropriate public reporting of data.
Data Stewards	1. Act as the point of contact for data-related issues in each department or section within USBE; 2. Coordinate with Data and Statistics/IT and program areas; and 3. Document specific internal rules and processes related to data content, context, and associated business rules.

Data Governance Specialist	1. Supports the day-to-day stewardship effort through leadership, program management, and measurement of the USBE data governance effort. 2. Liaises with Data Governors and Data Stewards to implement and maintain data governance.

Data Security and Privacy Training

1. The Superintendent will provide a range of training opportunities for all USBE employees, including volunteers, contractors, and temporary employees with access to confidential information, in order to minimize the risk of human error and misuse of information.

   a. All employees will annually complete the standard information security awareness course provided online by the USBE Information Technology (IT) section under the direction of the Chief Information Security Officer.

   b. Upon receiving access to USBE networks or technology, all new USBE employees, temporary employees, and contracted partners must comply with Internal Policy 05-01 Acceptable Use of Information Technology Resources, which describes the permissible uses of USBE technology and information. All employees will annually certify to their supervisor that they will comply with this policy.

   c. All employees, temporary employees, and contracted partners that are granted access to personally identifiable information, will be given an additional training on privacy and confidentiality fundamentals no less than annually under the direction of the Director of Privacy.

   d. The Director of Privacy shall monitor completion of required privacy trainings and report completion rates to Section Directors and the Board.

   e. Employees that do not comply with Internal Policy 05-01 Acceptable Use of Information Technology Resources, will be referred to their direct supervisor and the director of human resources to determine what remediation or consequences are necessary and appropriate.

f. Contracted partners who have been granted access to confidential information who are found to be in non-compliance with the USBE Non-Disclosure Agreement (NDA) shall receive consequences up to and including removal of access to USBE's network; if this access is required for completion of the contract, the contractor may be found in breach of contract and subject to dismissal and other penalties as outlined in the contract.

Right to Review, Inspect, and Request Amendment of Records

1. USBE will allow access to inspect and review a student's education records held by USBE to the student's parent, legal guardian, or individual acting in the place of a parent or to a student who has turned 18 years of age in accordance with FERPA regulation 34 CFR 99.10(a)(2).

a. Access will be allowed within 45 days of receiving an official request.
b. Parents and eligible students should direct all requests to the Director of Privacy.
c. USBE will respond to reasonable request for explanation or interpretation of the records.
d. Should a parent or eligible student request records held by the LEA, USBE will direct the request to the relevant LEA.
e. USBE is not required to provide data that it does not maintain, nor is USBE required to create education records in response to a request.

Student Data Disclosure

1. USBE may only disclose student data consistent with the disclosure provisions of:

a. the federal Family Educational Rights and Privacy Action, 20 USC § 1232g and 34 CFR Part 99;

b. Utah's Student Data Protection Act, Sections 53E-9-301, et seq.;

c. the National School Lunch Act, 42 USC § 1758 and 7 CFR 245.6;

d. the Individuals with Disabilities Education Act, 20 USC §§ 1401, et seq., and

e. other pertinent federal and state law.

2. This data disclosure policy:

a. establishes a framework for compliance to federal or state reporting requirements;

b. allows contracted vendors to perform services that USBE would otherwise perform;

c. increases knowledge about Utah public education;

d. provides valuable information to external partners; and

e. facilitates transparency.

3. All data disclosures must be approved by USBE.

4. As used herein, the following definitions apply:

a. "Internal student data" means:

i. personally identifiable student data;

ii. de-identified student-level data; or

iii. aggregate student data, which do not have disclosure avoidance techniques applied in accordance with USBE policy and procedure.

b. "Over the shoulder review" means visual inspection of data on USBE systems facilitated by agency staff at the Utah State Board of Education office.

c. "Public-ready student data" means:

i. aggregate student data, which have disclosure avoidance techniques applied in accordance with USBE policy and procedure; or

ii. data otherwise considered public under GRAMA.

5. The Records Officer will share information that currently appears on the USBE website or that has previously appeared publicly on USBE's website, but has been archived, in accordance with Title 63G, Chapter 2 Government Records Access and Management Act (GRAMA).

6. The Director of Data and Statistics and Director of Privacy shall review and may approve requests for public-ready student data from the public consistent with this policy.

8. The Director of Privacy, Board legal counsel, and the Director of Purchasing shall review and may approve a request from a USBE-contracted vendor for internal student data, which are needed to perform the vendor's contracted services at the time the contract is reviewed consistent with this policy.

9. The Director of Data and Statistics, the Director of Privacy, and Board legal counsel shall review and may approve a request for internal student data required for auditing agencies, federal reporting, or evaluating and conducting studies that are required by federal or state law consistent with this policy.

10. A data steward shall review and may approve an LEA request for internal student data concerning the LEA's students consistent with this policy.

11. If an LEA requests internal student data concerning students outside of the LEA for the purpose of auditing or challenging the validity of USBE data, the following applies:

a. The request shall be in writing.

b. The Director of Data and Statistics and the Director of Privacy shall review and may approve the request.

c. If the request is for financial data, approval from the Deputy Superintendent of Operations is also required.

d. All approvals shall be in writing.

e. Upon approval:

i. an LEA may conduct an over-the-shoulder review of data in-person at the USBE building;

ii. No data sharing agreement is required where internal student data are not disclosed in an over-the-shoulder review of data; and

iii. No student PII or de-identified student data may be exported during an over-the-shoulder review.

12. The Law and Licensing Committee shall review and make a recommendation to the Board for approval of discretionary (non-state or federally mandated) requests for internal student data considering whether the request:

a. helps Utah students; and

b. advances the Board's strategic plan.

13. Discretionary requests for internal student data for the purposes of conducting research that will use PII must be submitted using the Data and Statistics Data Request form.

14. If a data request has been approved, the Director of Data and Statistics will work with the requestor and is responsible for ensuring that the data are delivered securely, and that data quality and privacy assurances are followed.

15. The Director of Data and Statistics is responsible for entering any disclosed student data into USBE's Metadata Dictionary within a month of the disclosure.

16. Educator and LEA staff data will be disclosed in accordance with GRAMA.

Data Incidents and Breaches

1. Establishing a plan for responding to a data breach, complete with clearly defined roles and responsibilities, will promote better response coordination, and help USBE shorten its incident response time. Prompt response is essential for minimizing the risk of any further data loss and, therefore, plays an important role in mitigating any negative consequences of the breach, including potential harm to affected individuals

2. a. In the event of a data breach or inadvertent disclosure of personally identifiable information, USBE employees shall follow the USBE Incident Response Plan.

b. USBE shall notify affected parties in accordance with Subsections 53E-9-304(2) and 63A-19-405.

c. Concerns about security breaches must be reported immediately to the Chief Information Security Officer, who will collaborate with appropriate members of the USBE executive team to determine whether a security breach has occurred.

3. If the USBE data breach response team determines that one or more employees or contracted partners have substantially failed to comply with USBE's IT Security Policy and relevant privacy policies, the Chief Information Security Officer will notify their direct supervisor and the director of human resources to determine what remediation and consequences are necessary and appropriate, which may include termination of employment, termination of a contract, or further legal action.

4. Concerns about security breaches that involve the Chief Information Security Officer shall be reported immediately to the Superintendent.

Record Retention and Destruction

1. A fundamental concept of the Public Records Management Act, Section §63A-12-105, is that records created by government are the property of the State. Their care, maintenance, and release are governed by statute and are not subject to the discretion of the government employees. Adherence to records retention laws promote preservation of records of enduring value, quality access to public information, data security, and data privacy.

2. a. USBE shall retain, expunge, and dispose of student records in accordance with Section 63G-2-604, 53E-9-306, R277-487 and shall comply with active retention schedules for student records per Utah Division of Archive and Record Services.

b. Intentional inappropriate destruction of records is a class B misdemeanor.

c. Employees who intentionally and inappropriately destroy records may be subject to disciplinary action including suspension or discharge.

a. The Superintendent shall appoint a Records Officer.

3. Each director or supervisor of a USBE section, department, or program shall designate a departmental records steward to be the point of contact for the Records Officer and be responsible for updating record schedules and being familiar with records retention requirements.

4. a. In the Fall (September-November) and Spring (March-May) of each year the Records Officer shall review departmental records management and retention policies and practices.

b. The Records Officer shall provide annual training to the Departmental Records Stewards.

c. The Records Officer shall provide records management and retention onboarding for new USBE employees, as part of the USBE “On Boarding” training.

5. The Records Officer shall create a policy to oversee USBE's deletion/purge process to ensure document destruction or transfer of data to State Archives as instructed by the appropriate retention schedules.

Transparency

Annually, USBE will publicly post USBE data collections and disclosures of student personally identifiable information via the USBE Metadata Dictionary as described in Utah's Student Data Protection Act, Section 53E-9-301.

Annual Review

The Superintendent shall review the Data Governance Plan with the Law and Licensing Committee at least annually.