

| 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**

| <b>Role</b>                               | <b>Responsibilities</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Director of Privacy</b>                | Fulfills the role described in Section 53E-9-302(4).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Chief Information Security Officer</b> | Fulfills the role described in USBE Internal Policy 05.02 Information Security.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Records Officer</b>                    | Fulfills the duties of the Records Officer, as defined in Section 63G-2-103(24).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Records Steward</b>                    | Departmental/section point of contact for the Records Officer, meets bi-annually with the Records Officer (Fall and Spring), and updates record schedules.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Data and Statistics Director</b>       | <ol style="list-style-type: none"> <li>1. Monitors and trains data stewards on data management;</li> <li>2. provides bi-annual data quality training to USBE staff that handle student data;</li> <li>3. coordinates Data Stewards from each section within USBE to review data requests;</li> <li>4. works closely with IT staff to ensure data quality;</li> <li>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;</li> <li>6. helps ensure proper access levels for the Data Gateway for USBE and LEA employees;</li> <li>7. documents the names(s), date, and all data elements shared;</li> <li>8. manages Data Quality Processes; and</li> <li>9. helps ensure appropriate public reporting of data.</li> </ol> |
| <b>Data Stewards</b>                      | <ol style="list-style-type: none"> <li>1. Act as the point of contact for data-related issues in each department or section within USBE;</li> <li>2. Coordinate with Data and Statistics/IT and program areas; and</li> <li>3. Document specific internal rules and processes related to data content, context, and associated business rules.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|                                   |                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Data Governance Specialist</b> | <ol style="list-style-type: none"><li>1. Supports the day-to-day stewardship effort through leadership, program management, and measurement of the USBE data governance effort.</li><li>2. Liaises with Data Governors and Data Stewards to implement and maintain data governance.</li></ol>                                                                                       |
| <b><u>Date Governors</u></b>      | <ol style="list-style-type: none"><li>1. <u>Governing body of director-level stakeholders within USBE.</u></li><li>2. <u>Reviews and makes recommendations to the Superintendency on data governance policies and goals.</u></li><li>3. <u>Discusses topics brought forth by staff related to data.</u></li><li>4. <u>Resolves issues escalated by the data stewards.</u></li></ol> |
| <b><u>Superintendent</u></b>      | <ol style="list-style-type: none"><li>1. <u>Designated Chief Administrative Officer (CAO) and fulfills the duties described in Section 63A-12-103.</u></li><li>2. <u>Completes the privacy program report described in Section 63A-19-401.3.</u></li></ol>                                                                                                                          |

### **Data Governance Approval Processes**

1. USBE employees seeking to make changes to USBE data collections shall coordinate with the Data Governance Specialist following processes that have been approved by the Data Governors.
2. As outlined in the relevant standard operating procedures (SOPs), changes to data collections will be approved by:
  - a. the Data Stewards group;
  - b. the Data Governors; and
  - c. the Superintendency.
3. The Data Governance Specialist may guide USBE employees through data governance processes.

### **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

43 with access to confidential information, in order to minimize the risk of human  
44 error and misuse of information.

- 45 a. All employees will annually complete the standard information security  
46 awareness course provided online by the USBE Information Technology  
47 (IT) section under the direction of the Chief Information Security Officer.
- 48 b. Upon receiving access to USBE networks or technology, all new USBE  
49 employees, temporary employees, and contracted partners must comply  
50 with Internal Policy 05-01 Acceptable Use of Information Technology  
51 Resources, which describes the permissible uses of USBE technology  
52 and information. All employees will annually certify to their supervisor that  
53 they will comply with this policy.
- 54 c. All employees, temporary employees, and contracted partners that are  
55 granted access to personally identifiable information, will be given an  
56 additional training on privacy and confidentiality fundamentals no less than  
57 annually under the direction of the Director of Privacy.
- 58 d. The Director of Privacy shall monitor completion of required privacy  
59 trainings. ~~[and report completion rates to Section Directors and the Board]~~  
60 The Superintendent shall report completion rates in the Privacy Program  
61 Report described in Section 63A-19-401.3.
- 62 e. Employees that do not comply with Internal Policy 05-01 Acceptable Use  
63 of Information Technology Resources, will be referred to their direct  
64 supervisor and the director of human resources to determine what  
65 remediation or consequences are necessary and appropriate.
- 66 f. Contracted partners who have been granted access to confidential  
67 information who are found to be in non-compliance with the USBE Non-  
68 Disclosure Agreement (NDA) shall receive consequences up to and  
69 including removal of access to USBE's network; if this access is required  
70 for completion of the contract, the contractor may be found in breach of  
71 contract and subject to dismissal and other penalties as outlined in the  
72 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 Act, 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;

- 105           c. increases knowledge about Utah public education;
- 106           d. provides valuable information to external partners; and
- 107           e. facilitates transparency.
- 108       3. All data disclosures must be approved by USBE.
- 109       4. As used herein, the following definitions apply:
- 110           a. "Internal student data" means:
- 111               i. personally identifiable student data;
- 112               ii. de-identified student-level data; or
- 113               iii. aggregate student data, which do not have disclosure avoidance
- 114 techniques applied in accordance with USBE policy and procedure.
- 115           b. "Over the shoulder review" means visual inspection of data on USBE
- 116 systems facilitated by agency staff at the Utah State Board of Education office.
- 117           c. "Public-ready student data" means:
- 118               i. aggregate student data, which have disclosure avoidance techniques
- 119 applied in accordance with USBE policy and procedure; or
- 120               ii. data otherwise considered public under GRAMA.
- 121       5. The Records Officer will share information that currently appears on the
- 122 USBE website or that has previously appeared publicly on USBE's website, but has
- 123 been archived, in accordance with Title 63G, Chapter 2 Government Records Access and
- 124 Management Act (GRAMA).
- 125       6. The Director of Data and Statistics and Director of Privacy shall review and
- 126 may approve requests for public-ready student data from the public consistent with this
- 127 policy.
- 128       7. The Director of Privacy, Board legal counsel, and the Director of Purchasing
- 129 shall review and may approve a request from a USBE-contracted vendor for internal
- 130 student data, which are needed to perform the vendor's contracted services at the time
- 131 the contract is reviewed consistent with this policy.
- 132       8. The Director of Data and Statistics, the Director of Privacy, and Board legal
- 133 counsel shall review and may approve a request for internal student data required for
- 134 auditing agencies, federal reporting, or evaluating and conducting studies that are
- 135 required by federal or state law consistent with this policy.

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

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

141           a. The request shall be in writing.

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

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

146           d. All approvals shall be in writing.

147           e. Upon approval:

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

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

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

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

157           a. helps Utah students; and

158           b. advances the Board's strategic plan.

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

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

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

15. 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.

5. Employee data access permissions should be based off a user's need to know as stated in Internal Policy 05-08 and approvals will go through the user's direct supervisor and data owner of the system for which the user is requesting access.

## **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,



198 maintenance, and release are governed by statute and are not subject to the discretion  
199 of the government employees. Adherence to records retention laws promote  
200 preservation of records of enduring value, quality access to public information, data  
201 security, and data privacy.

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

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

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

209                 a. The Superintendent shall appoint a Records Officer.

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

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

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

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

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

## 224 225 **Transparency**

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

229

230    **Annual Review**

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

233