| Official Policies and Procedures<br>of the<br>Utah State Board of Education | |
|---|---|
| **Effective/Revision Date:** 2/13/2018 | |
| **Policy Title: USBE Data Governance Plan** | |

# 1 PURPOSE

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, from acquisition, to use, to disposal. The Utah Board of Education (USBE) takes seriously its moral and legal responsibility to protect student privacy and ensure data security. Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401, requires that USBE adopt a Data Governance Plan.

# 2 SCOPE AND APPLICABILITY

This policy is applicable to all employees, temporary employees, and contractors USBE. The policy must be used to assess agreements made to disclose data to third parties. This policy must also be used to assess the risk of conducting business. In accordance with USBE policy and procedures, this policy will be reviewed and adjusted on an annual basis or more frequently, as needed. This policy is designed to ensure only authorized disclosure of confidential information. The following 8 subsections provide data governance policies and processes for USBE:

1. Data Advisory Groups
2. Non-Disclosure Assurances for Employees
3. Data Security and Privacy Training for Employees
4. Data Disclosure
5. Data Breach
6. Record Retention and Expungement
7. Data Quality
8. Transparency

Furthermore, this USBE Data Governance Plan works in conjunction with the USBE Information Security Policy, which

- Designates USBE as the steward for all confidential information maintained within USBE.
- Designates Data Stewards' access for all confidential information.

- Requires Data Stewards to maintain a record of all confidential information that they are responsible for.
- Requires Data Stewards to manage confidential information according to this policy and all other applicable policies, standards, and plans.
- Complies with all legal, regulatory, and contractual obligations regarding privacy of USBE data. Where such requirements exceed the specific stipulation of this policy, the legal, regulatory, or contractual obligation shall take precedence.
- Provides the authority to design, implement, and maintain privacy procedures meeting USBE standards concerning the privacy of data in motion, at rest, and processed by related information systems.
- Ensures that all USBE board members, employees, contractors, and volunteers comply with the policy and undergo annual privacy training.
- Provides policies and process for

    - Systems administration
    - Network security
    - Application security
    - Endpoint, server, and device security
    - Identity, authentication, and access management
    - Data protection and cryptography
    - Monitoring, vulnerability, and patch management
    - High availability, disaster recovery, and physical protection
    - Incident responses
    - Acquisition and asset management, and
    - Policy, audit, e-discovery, and training.

# 3 DATA ADVISORY GROUPS

## 3.1 STRUCTURE

USBE has a three-tiered data governance structure to ensure that data are protected at all levels of Utah's educational system.

## 3.2 GROUP MEMBERSHIP

Membership in the groups require board approval. Group membership is for two years.

## 3.3 INDIVIDUAL AND GROUP RESPONSIBILITIES

Table 1 outlines individual USBE staff responsibilities, whereas Table 2 outlines advisory group responsibilities.

3.3.1 Table 1. Individual USBE Staff Responsibilities

| Role | Responsibilities |
|---|---|
| **Chief Privacy Officer** | 1. Acts as the primary point of contact for state student data protection administration in assisting the board to administer this part;<br>2. ensures compliance with student privacy laws throughout the public education system, including:<br>a. providing training and support to applicable board and LEA employees; and<br>b. producing resource materials, model plans, and model forms for local student data protection governance, including a model student data disclosure statement;<br>3. investigates complaints of alleged violations of this part;<br>4. reports violations of this part to:<br>a. the board;<br>b. an applicable education entity; and<br>c. the student data policy advisory group; and<br>5. acts as a state level student data manager. |
| **IT Systems Security Manager** | 1. Acts as the primary point of contact for state student data security administration in assisting the board to administer this part;<br>2. ensures compliance with security systems laws throughout the public education system, including:<br>a. providing training and support to applicable USBE employees; and<br>b. producing resource materials, model plans, and model forms for LEA systems security;<br>3. investigates complaints of alleged violations of systems breaches;<br>4. provides an annual report to the board on USBE's systems security needs |
| **Data and Statistics Coordinator** | 1. Monitors, improving and training of the data management;<br>2. provides bi-annual data quality training to USBE staff that handle student data;<br>3. coordinates Data Stewards from each section within USBE to review data requests;<br>4. works closely with IT staff to ensure data quality;<br>5. ensures the proper level of data redaction techniques for publicly posted reports, reports in the Data Gateway, and data that are shared with external entities and researchers;<br>6. ensures proper access levels for the Data Gateway for USBE and LEA employees;<br>7. documents the name(s), date, and all data elements shared;<br>8. manages Data Quality Processes; and<br>9. ensures appropriate public reporting of data. |
| **Data Stewards** | 1. Acts as the point of contact for data related issues in each department or section within USBE;<br>2. coordinates with Data/IT and program areas; and<br>3. documents specific internal rules and process data content, context, and associated business rules. |

### 3.3.2 Table 2. Advisory Group Responsibilities

| Group | Members | Responsibilities |
|---|---|---|
| **Policy Advisory**<br><br>Meets approximately 2-3 times a year | • Legislator(s)<br>• Board Member(s)<br>• Board Employee(s)<br>• LEA representative(s)<br>• Chief Privacy Officer<br>• Deputy Superintendent | Discuss and make recommendation to the board regarding:<br>1. enacted or propose legislation, and<br>2. state and local student data protection policies across the state<br>a. that reviews and monitors the state student data governance plan; and<br>b. that performs other tasks related to student data protection as designate by the board |
| **Data Governance Advisory**<br><br>Meets approximately 6-10 times a year | • Chief Privacy Officer<br>• Other board employees<br>• Data and Statistics Coordinator<br>• USBE attorney(s)<br>• USBE IT Employee(s) | Performs duties related to state and local student data protection, including:<br>1. Overseeing data collection and usage by board program offices; and<br>2. Preparing and maintaining the board's student data governance plan under the direction of the student data policy advisory group. |
| **Data User Advisory**<br><br>Meets approximately 6-10 times a year | • Local-level student data users<br>• 3-5 LEA Officials who work with Data Privacy<br>• Chief Privacy Officer | Provides feedback and suggestions on practicality of actions proposed by student data policy advisor and governance groups that affect LEAs. |

# 4 EMPLOYEE NON-DISCLOSURE ASSURANCES

Employee non-disclosure assurances are intended to minimize the risk of human error and misuse of information.

## 4.1 SCOPE

All USBE board members, employees, contractors, and volunteers must sign and obey the USBE Employee Non-Disclosure Agreement (See Appendix A), which describes the permissible uses of state technology and information.

## 4.2 NON-COMPLIANCE

Non-compliance with the agreements shall result in consequences up to and including removal of access to USBE's network; if this access is required for employment, employees and contractors may be subject to dismissal.

## 4.3 DATA SECURITY AND PRIVACY TRAINING

### 4.3.1 Purpose

USBE will provide a range of training opportunities for all USBE staff, including volunteers, contractors, and temporary employees with access to student educational data or confidential educator records, in order to minimize the risk of human error and misuse of information.

### 4.3.2 Scope

All USBE board members, employees, and contracted partners.

### 4.3.3 Compliance

Employees that do not comply may not be able to use USBE networks or technology.

### 4.3.4 Policy

1. Upon receiving access to USBE networks and/or technology, all new USBE board members, employees, and contracted partners must sign and follow the USBE Employee Acceptable Use Policy, which describes the permissible uses of state technology and information. New employees that do not comply may not be able to use USBE networks or technology.
2. Within the first week of employment, all USBE board members, employees, and contracted partners also must sign and obey the USBE Employee Non-Disclosure Agreement, which describes appropriate uses and the safeguarding of student and educator data.
3. All current USBE board members, employees, and contracted partners are required to participate in an annual Security and Privacy Fundamentals Training Curriculum.
4. USBE requires a targeted Security and Privacy Training for Data Stewards and IT staff for other specific groups within USBE that collect, store, or disclose data. The Chief Privacy Officer will identify these groups and will determine the annual training topics for these targeted groups based on USBE training needs.
5. Participation in the training as well as a signed copy of the Employee Non-Disclosure Agreement will be annually monitored by supervisors. Supervisors and the board secretary will annually report all USBE board members, employees, and contracted partners who do not have these requirements completed to the Chief Privacy Officer.

# 5 DATA DISCLOSURE

## 5.1 PURPOSE

USBE discloses data consistent with the disclosure provisions of the federal Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g and34 CFR Part 99, and Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401, as well as other pertinent federal and state law. Data disclosure ensures

compliance of federal and/or state reporting requirements, allows contracted vendors to perform services that USBE would otherwise perform, increases knowledge about Utah public education, provides valuable information to external partners, and increases transparency. This policy establishes the protocols and procedures for sharing data maintained by USBE.

## 5.2 Student or Student's Parent or Legal Guardian Access

Parents are advised that the records maintained by USBE are provided to USBE by the school district in which their student is/was enrolled, and access to their student's record can be obtained from the student's school district. In accordance with FERPA regulations 20 U.S.C. § 1232g (a)(1) (A) (B) (C) and (D), LEAs will provide parents with access to their child's education records, or an eligible student access to his or her own education records (excluding information on other students, the financial records of parents, and confidential letters of recommendation if the student has waived the right to access), within 45 days of receiving an official request. LEAs and USBE is not required to provide data that it does not maintain, nor is USBE required to create education records in response to an eligible student's request.

## 5.3 Data Disclosure

All data disclosures must be approved by the USBE Board.

Internal data requests include:

Contracted third-party vendors who perform services USBE would otherwise perform,

- Federal or state mandated program reports, audits or evaluations,
- USBE Board approved research or evaluation of a federal or state funded program.

Data requests that are not internal are considered external. The following table outlines how data requests are presented to the Board. The full Board must approve a data request in order for data to be disclosed.

Table 3. Data Request Presentations to the Board

| | **Internal Data Request** | **External Data Request** |
|---|---|---|
| **Student-level Data** | Consent Calendar | Law and Licensing Committee |
| **Not student-level Data** | Consent Calendar | Consent Calendar |

Prior to being placed on either the consent calendar or the agenda for the Law and Licensing Committee, both USBE assistant attorney general and Chief Privacy Officer shall review the data request. If the data disclosure is related to procurement, then USBE's Purchasing Director must also review the contract.

Data requests for the purposes of conducting research must be submitted using this form: http://www.schools.utah.gov/data/Data-Request/ResearcherProposal.aspx

If a data request has been board approved, the Coordinator of Data and Statistics will works with the requestor and is responsible for ensuring that the data are appropriately delivered securely and that

data quality and privacy assurances are followed. The Coordinator of Data and Statistics is responsible for entering any disclosed student personally identifiable information into USBE's Metadata Dictionary within a month of the disclosure.

# 6 DATA BREACH

## 6.1 PURPOSE

Establishing a plan for responding to a data breach, complete with clearly defined roles and responsibilities, will promote better response coordination and help educational organizations shorten their 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.

## 6.2 POLICY

USBE shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, USBE staff shall follow industry best practices outlined in the USBE IT Security Policy for responding to the breach. Further, USBE 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 IT security manager who will collaborate with appropriate members of the USBE executive team to determine whether a security breach has occurred. 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, they will identify appropriate consequences, which may include termination of employment or a contract and further legal action. Concerns about security breaches that involve the IT Security Manager must be reported immediately to the Superintendent.

USBE will provide and periodically update, in keeping with industry best practices, resources for Utah LEAs in preparing for and responding to a security breach. USBE will make these resources available on its website.

# 7 RECORD RETENTION AND EXPUNGEMENT

## 7.1 PURPOSE

Records retention and expungement policies promote efficient management of records, preservation of records of enduring value, quality access to public information, and data privacy.

## 7.2 SCOPE

USBE board members and staff.

## 7.3 Policy

The USBE, staff, Utah LEAs and schools shall retain and dispose of student records in accordance with Section 63G-2-604, 53A-1-1407, and shall comply with active retention schedules for student records per Utah Division of Archive and Record Services.

In accordance with 53A-1-1407, the USBE shall expunge student data that is stored upon request of the student if the student is at least 23 years old. The USBE may expunge medical records and behavioral test assessments. USBE will not expunge student records of grades, transcripts, a record of the student's enrollment or assessment information. USBE staff will collaborate with Utah State Achieves and Records Services in updating data retention schedules.

USBE maintained student-level discipline data will be expunged after three years.

# 8 QUALITY ASSURANCES AND TRANSPARENCY REQUIREMENTS

## 8.1 Purpose

Data quality is achieved when information is valid for the use to which it is applied, is consistent with other reported data and users of the data have confidence in and rely upon it. Good data quality does not solely exist with the data itself, but is also a function of appropriate data interpretation and use and the perceived quality of the data. Thus, true data quality involves not just those auditing, cleaning and reporting the data, but also data consumers. Data quality at is addressed in five areas:

### 8.1.1 Data Governance Structure

The USBE data governance policy is structured to encourage the effective and appropriate use of educational data. The USBE data governance structure centers on the idea that data is the responsibility of all USBE sections and that data driven decision making is the goal of all data collection, storage, reporting and analysis. Data driven decision making guides what data is collected, reported and analyzed.

### 8.1.2 Data Requirements and Definitions

Clear and consistent data requirements and definitions are necessary for good data quality. On the data collection side, the USBE communicates data requirements and definitions to LEAs through the Data Clearinghouse Update Transactions documentation (see http://www.schools.utah.gov/computerservices/Data-Clearinghouse.aspx). The USBE also communicates with LEA IT staff regularly, at monthly Data Warehouse Group meetings and at biannual Data Conferences. Where possible, USBE program specialists are invited to these meetings and the same guidance is given to the appropriate LEA program directors.

On the data reporting side, the production and presentation layers provide standard data definitions and business rules. Data Stewards coordinate data releases through the Data Stewards Group meetings. All data released includes relevant data definitions, business rules, and are date stamped. Further, Data and Statistics produces documentation, trainings and FAQs on key statistics and reports, such as AYP, graduation rate and class size.

### 8.1.3 Data Collection

Data elements should be collected only once—no duplicate data collections are permitted. Where possible, data is collected at the lowest level available (i.e. at the student/teacher level). Thus, there are no aggregate data collections if the aggregate data can be derived or calculated from the detailed data.

For all new data collections, USBE provides to LEAs clear guidelines for data collection and the purpose of the data request. The USBE also notifies LEAs as soon as possible about future data collections. Time must be given to LEAs in order for them to begin gathering the data needed.

### 8.1.4 Data Auditing

Data and Statistics Data Analysts perform regular and ad hoc data auditing. They analyze data in the warehouse for anomalies, investigate the source of the anomalies, and work with IT and/or LEAs in explaining and/or correcting the anomalies. Data Analysts also work with School Finance to address findings from the Auditors.

### 8.1.5 Quality Control Checklist

Checklists have been proven to increase quality (See Appendix C). Therefore, before releasing data, Data Stewards and Data Analysts must successfully complete the data release checklist in three areas: reliability, validity and presentation.

# 9 DATA TRANSPARENCY

Annually, USBE will publicly post:

- USBE data collections
- Metadata Dictionary as described in Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401

# 10 APPENDIX

## Appendix A. USBE Employee Non-Disclosure Agreement

All student data utilized by USBE is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and Utah statute. This policy outlines the way USBE staff is to utilize data and protect personally identifiable and confidential information. A signed agreement form is required from all USBE staff to verify agreement to adhere to/abide by these practices and will be maintained by the Chief Privacy Officer.

**As an employee of the Utah State Board of Education, I hereby affirm that:** (Initial)

_____ I have readthe Employee Non-Disclosure Assurances attached to this agreement form and read and reviewed Data Governance Plan USBE policies. These assurances address general procedures, data use/sharing, and data security.

_____ I will abide by the terms of the USBE's policies and its subordinate process and procedures;

_____ I grant permission for the manual and electronic collection and retention of security related information, including but not limited to photographic or videotape images, of your attempts to access the facility and/or workstations; and

**Trainings**

_____ I have completed USBE's Data Security and Privacy Fundamentals Training.

_____ I will complete USBE's Data Security and Privacy Fundamentals Training within 30 days.

**Using USBE Data and Reporting Systems**

_____ I will use a password-protected computer when accessing data and reporting systems, viewing child/staff records, and downloading reports.

_____ I will not share or exchange individual passwords, for either personal computer(s) or USBE system user accounts, with USBE staff or participating program staff.

_____I will log out of and close the browser after each use of USBE data and reporting systems.

_____I will only access data in which I have received explicit written permissions from the data owner.

_____I will not attempt to identify individuals, except as is required to fulfill job or volunteer duties, or to publicly release confidential data;

**Handling Sensitive Data**

_____ I will keep sensitive data on password-protected state-authorized computers.

_____ I will keep any printed files containing personally identifiable information in a locked location while unattended.

_____ I will not share child/staff-identifying data during public presentations, webinars, etc. I understand that dummy records should be used for such presentations.

_____ I will delete files containing sensitive data after working with them from my desktop, or move them to a secured USBE server.

**Reporting & Data Sharing**

_____ I will not redisclose or share any confidential data analysis except to other authorized personnel without [USBE]'s express written consent.

_____ I will not publicly publish any data without the approval of the Superintendent.

_____ I will take steps to avoid disclosure of personally identifiable information in state-level reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.

_____ I will not use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If I receive an email containing such information, I will delete the screenshots/text when forwarding or replying to these messages.

_____ I will not transmit child/staff-level data externally unless explicitly authorized in writing.

_____ I understand that when sharing child/staff-identifying data with authorized individuals, the only approved methods are phone calls or USBE's Secure File Transfer Protocol (SFTP). Also, sharing within secured server folders is appropriate for USBE internal file transfer.

_____ I will immediately report any data breaches, suspected data breaches, or any other suspicious activity related to data access to my supervisor and the USBE Information Security Officer. Moreover, I acknowledge my role as a public servant and steward of child/staff information, and affirm that I will handle personal information with care to prevent disclosure.

**Consequences for Non-Compliance**

_____ I understand that access to the USBE network and systems can be suspended based on any violation of this contract or risk of unauthorized disclosure of confidential information;

_____ I understand that failure to report violation of confidentiality by others is just as serious as my own violation and may subject me to personnel action, including termination.

**Termination of Employment**

_____ I agree that upon the cessation of my employment from USBE, I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone outside of USBE without the prior written permission of the Chief Information Officer of USBE.

Print Name: _____

Signed: _____

Date: _____

# Appendix B. Protecting PII in Public Reporting

Data Gateway Statistical Reporting Method for Protecting PII

Public education reports offer the challenge of meeting transparency requirements while also meeting legal requirements to protect each student's personally identifiable information (PII). Recognizing this, the reporting requirements state that subgroup disaggregation of the data may not be published if the results would yield personally identifiable information about an individual student. While the data used by the Utah State Board of Education (USBE ) and local education agencies (LEAs) is comprehensive, the data made available to the public is masked to avoid unintended disclosure of personally identifiable information at summary school, LEA, or state-level reports.

This is done by applying the following statistical method for protecting PII.

1. Underlying counts for groups or subgroups totals are not reported.
2. If a reporting group has 1 or more subgroup(s) with 10 or fewer students.
    - The results of the subgroup(s) with 10 or fewer students are recoded as "N<10"
    - For remaining subgroups within the reporting group
        1. For subgroups with 300 or more students, apply the following suppression rules.
            1. Values of 99% to 100% are recoded to ≥99%
            2. Values of 0% to 1% are recoded to ≤1%
        2. For subgroups with 100 or more than but less than 300 students, apply the following suppression rules.
            1. Values of 98% to 100% are recoded to ≥98%
            2. Values of 0% to 2% are recoded to ≤2%
        3. For subgroups with 40 or more but less than 100 students, apply the following suppression rules.
            1. Values of 95% to 100% are recoded to ≥95%
            2. Values of 0% to 5% are recoded to ≤5%
        4. For subgroups with 20 or more but less than 40 students, apply the following suppression rules.
            1. Values of 90% to 100% are recoded to ≥90%
            2. Values of 0% to 10% are recoded to ≤10%
            3. Recode the percentage in all remaining categories in all groups into intervals as follows (11-19,20-29,…,80-89)
        5. For subgroups with 10 or more but less than 20 students, apply the following suppression rules.
            1. Values of 80% to 100% are recoded to ≥80%
            2. Values of 0% to 20% are recoded to ≤20%
            3. Recode the percentage in all remaining categories in all groups into intervals as follows (20-29,30-39,…,70-79)

## Appendix C. Quality Control Checklist Reliability (results are consistent)

1. Same definitions were used for same or similar data previously reported **or** it is made very clear in answering the request how and why different definitions were used
2. Results are consistent with other reported results **or** conflicting results are identified and an explanation provided in request as to why is different
3. All data used to answer this particular request was consistently defined (i.e. if teacher data and student data are reported together, are from the same year/time period)
4. Another USBE data steward could reproduce the results using the information provided in the metadata

Validity (results measure what are supposed to measure, data addresses the request)

5. Request was clarified
6. Identified and included all data owners that would have a stake in the data used
7. Data owners approve of data definitions and business rules used in the request
8. All pertinent business rules were applied
9. Data answers the intent of the request (intent ascertained from clarifying request)
10. Data answers the purpose of the request (audience, use, etc.)
11. Limits of the data are clearly stated
12. Definitions of terms and business rules are outlined so that a typical person can understand what the data represents

Presentation

13. Is date-stamped
14. Small n-sizes and other privacy issues are appropriately handled
15. Wording, spelling and grammar are correct
16. Data presentation is well organized and meets the needs of the requester
17. Data is provided in a format appropriate to the request
18. A typical person could not easily misinterpret the presentation of the data

**ADA Compliant 03/08/2018**