UTAH STATE BOARD OF EDUCATION POLICY	
Policy Number:	3006
Policy Name:	USBE Data Governance Plan
Date Approved:	December 5, 2019

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 date. 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. §53E-9-301, 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 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 in USBE Internal Policy 05-01, Acceptable Use of Information Technology Resources. In accordance with USBE policy and procedures, this policy will be reviewed and adjusted on an annual basis or more frequently, as determined by USBE's Student Data Governance Advisory Group. This policy is designed to help ensure only authorized disclosure of confidential information. The following seven subsections provide data governance policies and processes for USBE:
    a. Data Advisory Groups;
    b. Data Security and Privacy Training for the Board, Employees, and Contractors;
    c. Data Disclosure;
    d. Data Breach;
    e. Record Retention and Expungement;

f. Data Quality; and

g. Transparency.

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

3. The Superintendent shall implement a three-tiered data governance structure to ensure that data are protected at all levels of Utah's educational system. These groups are the Policy Advisory, Data Governance Advisory, and Data User Advisory groups (Table 1).

Table 1 Advisory Group Responsibilities

Group	Responsibilities
Student Data Policy Advisory Group	https://www.schools.utah.gov/file/b5209b47-06ec-4a31-b603-2aad05235fdf
Student Data Governance Advisory Group	https://www.schools.utah.gov/file/2fd7d5bf-876e-4e35-9d0f-bfc7ab96442a
Student Data Users Advisory Group	https://www.schools.utah.gov/file/8d2a56ca-e5ce-4e6c-9565-9fb6140ff3cd

a. Membership in a group requires Board approval and is for a two-year term.

b. Table 2 outlines individual USBE employee responsibilities.

Table 2 Individual USBE Employee Responsibilities

Role	Responsibilities
Chief Privacy Officer	Fulfills the role described in U.C.A. 53E-9-302(4).
Chief Information Security Officer	Fulfills the role described in USBE Internal Policy 5.2 Information Security.
Records Officer	Fulfills the duties of the Records Officer, as defined in 63G-2-103(24).
Records Steward	1. Departmental/section point of contact for the Records Officer.

	2. Meets bi-annually with the Records Officer (fall and spring); and 3. Updates record schedules
Role	Responsibilities
Data and Statistics Coordinator	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 name(s), date, and all data elements shared; 8. Manages Data Quality Process; and 9. Helps ensure 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; 2. Coordinates with Data and Statistics/IT and program areas; and 3. Documents specific internal rules and processes related to data content, context, and associated business rules.

4. 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 confidential information, will be given an additional training on privacy and confidentiality fundamentals no less than annually under the direction of the Chief Privacy Officer.
d. The USBE Student Data Governance Advisory Group shall monitor completion of required 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.

5. USBE may only disclose student data consistent with the disclosure provision of the federal Family Educational Rights and Privacy Act (FERPA), 20 U.S.C.

§1232g and 34 CFR Part 99; Utah's Student Data Protection Act (SDPA), U.C.A. §53E-9-301 et seq; the National School Lunch (NSLA), 42 U.S.C. 1758 and 7 CFR 245.6; the Individuals with Disabilities Education Act, 20 U.S.C. §1401 et seq; and other pertinent federal and state law. This data disclosure policy:

a. Establishes a framework for compliance to federal and/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.

6. 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 CR99.10(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 Chief Privacy Officer.
    c. USBE will respond to reasonable requests 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.
7. All data disclosures must be approved by USBE.
    a. Board requests are requests made by State Board members.
    b. Internal data requests include:
        i. Contracted third-party vendors who perform services USBE would otherwise perform; or
        ii. Federal or state mandated or state-funded program report, audit, research or evaluation.

c. Data requests that are not Board requested or internal are considered external.

8. Requests for information that currently appear on the USBE website or that has previously appeared publicly on USBE's website but has been archived will not be presented to the Board but will be shared with the requesting party in accordance with the Government Records Access and Management Act (GRAMA), Title 63G, Chapter 2.
9. All other board, internal, and external requests will be processed as follows:
    a. The Chief Privacy Officer shall process all data requests according to Table 3.
    b. Table 3 outlines how data requests are processed.

Table 3 Data Request Processing

	Internal Data Request	External Data Request	USBE Board Request
Student Personally Identifiable Information (PII)	Consent Calendar	Law and Licensing Committee	Approval from USBE Board Leadership
De-identified Individual Level	Approval from Coordinator of Data and Statistics and Chief Privacy Officer	Law and Licensing Committee	Approval from USBE Board Leadership
Aggregate	Approval from Coordinator of Data and Statistics and Chief Privacy Officer	Approval from Coordinator of Data and Statistics and Chief Privacy Officer	Approval from USBE Board Leadership

c. 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.

d. External data requests for the purposes of conducting research that will use PII must be submitted using the Data and Statistics Data Request form:
e. If a data request has been approved, the Coordinator 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. The Coordinator of Data and Statistics is responsible for entering any disclosed student data into USBE's Metadata Dictionary within a month of the disclosure.

10. Educator data will be disclosed in accordance with GRAMA classifications found in 63G-2-301 through 63G-2-305 .
11. 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.
12. In the event of a data breach or inadvertent disclosure of student data, USBE employees shall follow the USBE Incident Response Plan:
    a. USBE shall notify affected parties in accordance with 53E-9-304(2).
    b. 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.
13. 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 or a contract and further legal action.

14. Concerns about security breaches that involve the Chief Information Security Officer must be reported immediately to the Superintendent.
15. A fundamental concept of the Public Records Management Act, U.C.A, §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.
16. USBE shall retain, expunge, and dispose of student records in accordance with Section 63G-2-604, 53E-9-306, R277-487-4 and shall comply with active retention schedules for student records per Utah Division of Archive and Record Services.
    a. Intentional inappropriate destruction of records is a class B misdemeanor. Employees who intentionally and inappropriately destroy records may be subject to disciplinary action including suspension or discharge.
    b. The Superintendent of Public Instruction shall designate a Records Officer.
17. 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. The Departmental Records Steward is responsible for updating record schedules and being familiar with records retention requirements.
18. 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.
    a. The Records Officer shall provide annual training to the Departmental Records Stewards.
    b. The Records Officer shall provide “Onboarding” records management and retention training of new USBE employees as part of the USBE “Onboarding” training.

19. The Records Officer shall create a policy to oversee USBE's deletion/purge process to ensure document destruction (and when applicable, migration of data to State Archives) at the end of the document's, file's, and series' lifespan as instructed by the retention schedule.
20. Annually, USBE will publicly post USBE data collections Metadata Dictionary as described in Utah's Student Data Protection Act, U.C.A. §53E-9-301.