



USDB Data Governance Plan

Draft 1

Reviewed/Revised: October 2025	Effective Date: To Be Determined
Effective Date:	
Authorized By: Utah State Board of Education	

1. Purpose and Background

- 1.1. Data governance is a formalized organizational approach to data and information management set forth in policies and procedures encompassing the full life cycle of data: from creation or acquisition to disposal. The Utah Schools for the Deaf and Blind (USDB) has a legal responsibility to protect student privacy and ensure data security.
- 1.2. The following Generally Accepted Information Principles (GAIP) guide the USDB approach to data governance:
 - Risk: Data and content carry inherent risks, including liability and costs related to managing such risks.
 - Due Diligence: Known risks must be reported, while potential risks should be investigated and confirmed.
 - Audit: Data and content accuracy are subject to periodic audits conducted by an independent body.
 - Accountability: USDB identifies specific individuals responsible for the management of data and content assets.
 - Liability: Data misuse or mismanagement carries financial and regulatory liability.

2. Data Maintenance and Protection

- 2.1. USDB is committed to implementing industry best practices to mitigate the risks and liabilities associated with maintaining student and educator data.

3. Designated Roles and Responsibilities

- 3.1. The Chief Privacy Officer will oversee the implementation of data privacy and security policies.
- 3.2. USDB will adopt the CIS Controls or comparable frameworks to secure its data systems.

4. Reporting

- 4.1. By October 1 of each year, USDB will report to the Utah State Board of Education (USBE) regarding:
 - 4.1.1. The status of its adoption of the CIS Controls or comparable framework.
 - 4.1.2. Future plans for improving data security and governance.

5. Roles and Responsibilities

- 5.1. Data Manager Responsibilities
 - 5.1.1. Authorize and manage the sharing of personally identifiable student data (PII) outside of USDB.
 - 5.1.2. Provide technical assistance, training, and support related to data privacy.
 - 5.1.3. Act as the local point of contact for the state student data officer.
 - 5.1.4. Ensure the availability of the following notices to parents:
 - 5.1.4.1. Annual FERPA Notice (34 CFR 99.7)
 - 5.1.4.2. Directory Information Policy (34 CFR 99.37)
 - 5.1.4.3. Survey Policy and Notice (20 USC 1232h, 53E-9-203)
 - 5.1.4.4. Data Collection Notice (53E-9-305)

- 5.2. Information Security Officer Responsibilities

- 5.2.1. Oversee the adoption and implementation of the CIS Controls.
 - 5.2.2. Provide technical assistance and training for IT security.

6. Training and Support

- 6.1. All USDB employees, contractors, and volunteers who access student or educator data must complete annual Security and Privacy Fundamentals Training.
- 6.2. Training content will include:
 - 6.2.1. FERPA Compliance
 - 6.2.2. The USDB Data Sharing Policy
 - 6.2.3. Proper handling and protection of sensitive data
- 6.3. USDB will report training completion status to USBE by October 1 annually.

- 6.4. Targeted Training will be provided to Student Data Managers and IT personnel who handle the collection, storage, or disclosure of student data.

7. Audits

- 7.1. USDB will conduct periodic audits to evaluate:
 - 7.1.1. The effectiveness of data governance policies and procedures.
 - 7.1.2. Third-party contractors' compliance with data privacy and security requirements, as outlined in 53E-9-309(2).

8. Data Sharing

- 8.1. USDB recognizes the risk of redisclosure when sharing student data and will implement controls to ensure compliance with federal and state laws. **All data sharing must align with FERPA, Utah Code 53E-9-309, and USBE Data Governance requirements.**
- 8.2. Data Sharing Procedures
 - 8.2.1. The Data Manager must approve all data-sharing requests.
 - 8.2.2. Data sharing will follow strict protocols, including:
 - 8.2.2.1. Low-Risk Data Requests: High-level aggregate data (e.g., graduation rates).
 - 8.2.2.2. Medium-Risk Data Requests: Aggregate data with small group sizes requiring de-identification.
 - 8.2.2.3. High-Risk Data Requests: De-identified student-level data requiring legal agreements (e.g., MOA).
- 8.3. Research Requests
 - 8.3.1. Research requests must comply with FERPA's study exception (34 CFR 99.31(a)(6)).
 - 8.3.2. ~~USDB requires board approval for high-risk research requests.~~
All high-risk research requests require board approval and a signed data-sharing agreement outlining purpose, use, and destruction requirements.
 - 8.3.3. Researchers must submit publications **or findings** to USDB for review 10 business days prior to release.
- 8.4. Sharing Data with Online Services
 - 8.4.1. USDB will only share student data with online service providers that have a current approved Data Privacy Agreement (DPA) on file through the state system.

- 8.4.2. All new online services must go through the vetting process to evaluate data privacy practices, security controls, and compliance with Utah Code 53E-9-309.
- 8.4.3. The Data Manager and IT Department will maintain a metadata dictionary of approved vendors and update it annually.

8.5. **Auditing Third-Party Vendors**

- 8.5.1. USDB will conduct periodic audits of third-party contractors and online service providers to verify compliance with data privacy and security requirements.
- 8.5.2. Audits will review contract terms, data access logs, and vendor responses to data breaches or destruction requests.
- 8.5.3. Findings and non-compliance issues will be reported to USDB leadership, and corrective action plans implemented as needed.

9. **Expungement Requests**

- 9.1. USDB acknowledges the risks of long-term data retention and will review expungement requests per FERPA and Utah statutes.
- 9.2. The following records are ineligible and may not be expunged:
 - 9.2.1. grades
 - 9.2.2. transcripts
 - 9.2.3. a record of the student's enrollment
 - 9.2.4. assessment information
- 9.3. The expungement procedure for eligible records shall match the record amendment procedure found in [34 CFR 99, Subpart C](#) of FERPA.
 - 9.3.1. If a parent believes that a record is misleading, inaccurate, or in violation of the student's privacy, they may request that the record be expunged.
 - 9.3.2. The LEA shall decide whether to expunge the data within a reasonable time after the request.
 - 9.3.3. If the LEA decides not to expunge the record, they will inform the parent of their decision as well as the right to an appeal hearing.
 - 9.3.4. The LEA shall hold the hearing within a reasonable time after receiving the request for a hearing.

- 9.3.5. The LEA shall provide the parent notice of the date, time, and place in advance of the hearing.
- 9.3.6. The hearing shall be conducted by any individual that does not have a direct interest in the outcome of the hearing.
- 9.3.7. The LEA shall give the parent a full and fair opportunity to present relevant evidence. At the parents' expense and choice, they may be represented by an individual of their choice, including an attorney.
- 9.3.8. The LEA shall make its decision in writing within a reasonable time following the hearing.
- 9.3.9. The decision must be based exclusively on evidence presented at the hearing and include a summary of the evidence and reasons for the decision.
- 9.3.10. If the decision is to expunge the record, the LEA will seal it or make it otherwise unavailable to other staff and educators.

10. Data Breach Response

- 10.1. The Information Security Officer will coordinate breach response efforts, including investigation and resolution.
- 10.2. A Cyber Incident Response Team (CIRT) will be activated as needed.
- 10.3. In the event of a significant data breach, affected parties, including students and parents, will be notified following consultation with legal counsel and without unreasonable delay.
- 10.4. In the event of a significant data breach, USDB will report the breach to USBE within 10 business days of the initial discovery.

11. Publication

- 11.1. To ensure transparency, USDB will post its data governance policies, including the following information on its website:
 - 11.1.1. Data governance plan
 - 11.1.2. USDB data collections
 - 11.1.3. Metadata Dictionary