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 Salt Lake City School District (District) takes seriously its responsibility to protect student privacy and ensure data security. Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401, requires that the District adopt a Data Governance Plan (Plan).

2 SCOPE AND APPLICABILITY

This Plan is applicable to all employees, temporary employees, and contractors of the District. The Plan

Official Policies and Procedures **of the** **Salt Lake City School District**	
Effective/Revision Date: 6/26/2017	
Title: Salt Lake City School District Data Governance Plan	

must be used to assess agreements made to disclose data to third-parties. This Plan must also be used to assess the risk of conducting business. In accordance with board policies and district administrative procedures, this Plan will be reviewed and adjusted on an annual basis, or more frequently, if needed. This Plan is designed to ensure only authorized disclosure of confidential information. The following eight subsections indicate the data governance processes addressed in this Plan:

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 Plan works in conjunction with the District IT Security Plan which provides policies and processes 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 TEAM

3.1 STRUCTURE

The District has a data advisory team, which consists of district leadership who have responsibility for providing data to internal and external stakeholders as appointed by the Superintendent.

3.2 INDIVIDUAL AND GROUP RESPONSIBILITIES

The following tables outlines individual District staff and advisory group responsibilities.

Role	Responsibilities
LEA Student Data Manager (Chief Information Officer)	1. May authorize and manage the sharing, outside of the education entity, of personally identifiable student data from a cumulative record for the education entity. 2. Acts as the primary local point of contact for the State's student data officer. 3. May share personally identifiable student data that is: a. about a student with that student and/or that student's parent; b. required by state or federal law; c. in an aggregate form with appropriate data redaction techniques applied; d. for a school official; e. for an authorized caseworker or other representative of the Department of Human Services or the Juvenile Court; f. in response to a subpoena issued by a court g. directory information; or h. in response to submitted data requests from external researchers or evaluators. 4. May not share personally identifiable student data for the purpose of external research or evaluation. 5. Will create and maintain a list of all LEA staff that have access to personally identifiable student data.

	6. Ensure all staff members, including volunteers, receive annual LEA level training on data privacy. Document all staff names, roles, and training dates, times, locations, and agendas.
IT Systems Security Manager (Chief Information Officer)	1. Acts as the primary point of contact for state student data security administration; 2. Ensures compliance with security systems laws throughout the public education system, including: a. providing training and support to applicable District employees; and b. producing resource materials, model plans, and model forms for District systems security; 3. Investigates complaints of alleged violations of systems breaches; and 4. Provides an annual report to the board on the District's systems security needs.
Director of Assessment and Evaluation	1. Acts as the primary point of contact for external research requests. 2. Directs staff who provide reports to internal stakeholders.
Executive Director of Policy and Legal Services	1. Acts as legal representative to ensure all procedures and policies comply with federal and state law.

3.2.1 Table 1. Individual District Staff Responsibilities

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 District board members and employees are expected to comply with board policies and district administrative procedures. Each board member and employee (including contractors and volunteers) must complete student data FERPA and data protection training in the district training system and electronically sign the Employee Non-Disclosure agreement at the end of the trainings. All contractors and volunteers must complete FERPA and student data privacy training and sign and follow the Salt Lake City School District 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 the District network; if this access is required for employment, employees and contractors may be subject to dismissal.

4.3 NON-DISCLOSURE ASSURANCES

All student data utilized by the District is protected in accordance with the Family Educational Rights and Privacy Act (FERPA) and Utah law. This Plan outlines the way District staff are to utilize data and protect personally identifiable and confidential information. A signed agreement form is required from all District staff to verify their agreement to adhere to/abide by these practices, and the agreement will be maintained in the District's Human Resource Services department. All District employees (including contract or temporary) will:

1. Complete a Security and Privacy Fundamentals Training.
2. Complete a Security and Privacy Training for Researchers and Evaluators, if your position is a research analyst, or if requested to do so by the Chief Information Officer.
3. Consult with District internal data owners when creating or disseminating reports containing data.
4. Use password-protected state-authorized computers when accessing any student-level or staff-level records.
5. NOT share individual passwords for personal computers or data systems with anyone.
6. Log out of any data system/portal and close the browser after each use.
7. Store sensitive data on appropriate-secured location. Unsecured access and flash drives, DVD, CD-ROM or other removable media, or personally owned computers or devices are not deemed appropriate for storage of sensitive, confidential or student data.
8. Keep printed reports with personally identifiable information in a locked location while unattended, and use the secure document destruction service provided by the District when disposing of such records.

9. NOT share personally identifying data during public presentations, webinars, etc. If users need to demonstrate child/staff level data, fictitious records should be used for such presentations.
10. Redact any personally identifiable information when sharing sample reports with general audiences, in accordance with guidance provided by the student data manager, found in Appendix B (Protecting PII in Public Reporting).
11. Take steps to avoid disclosure of personally identifiable information in reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.
12. Delete files containing sensitive data after using them on computers, or move them to secured servers or personal folders accessible only by authorized parties.
13. NOT use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If users receive an email containing such information, they will delete the screenshots/text when forwarding or replying to these messages. If there is any doubt about the sensitivity of the data the Student Data Privacy Manager should be consulted.
14. Use secure methods when sharing or transmitting sensitive data. The approved method is the District's Secure File Transfer Protocol (SFTP) website. Also, sharing within secured server folders is appropriate for the District internal file transfer.
15. NOT transmit child/staff-level data externally unless expressly authorized in writing by the data owner, and then only transmit data via approved methods such as described in item ten.
16. Limit use of individual data to the purposes that have been authorized within the scope of job responsibilities.

4.4 DATA SECURITY AND PRIVACY TRAINING

4.4.1 Purpose

The District will provide a range of training opportunities for all District 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.

4.4.2 Scope

These training requirements are applicable to all District board members, employees, contracted partners, and volunteers with access to student data.

4.4.3 Compliance

New employees that do not comply may not be able to use District networks or technology.

4.4.4 Requirement

1. Within the first week of employment, all District employees and contracted partners must review and follow the District's Employee Acceptable Use Policy, which describes the permissible uses of state technology and information. All volunteers must sign and follow the District's Employee Acceptable Use Policy prior to volunteering. Within two weeks of the

commencement of their term on the Board of Education, each Board member must review and agree to comply with the District's Employee Acceptable Use Policy.

2. New employees that do not comply may not be able to use District networks or technology. Within the first week of service to the District, all District board members, employees, and contracted partners also must review, electronically sign, and follow the District Employee Non-Disclosure Agreement, which describes appropriate uses and the safeguarding of student and educator data. All volunteers must review, sign, and follow the District Employee Non-Disclosure Agreement prior to volunteering.
3. All current District board members, employees, and contracted partners are required to participate in an annual Security and Privacy Fundamentals Training Curriculum within 60 days of the adoption of this Plan.
4. The District requires a targeted Security and Privacy Training for Data Stewards and IT staff for other specific groups within the District that collect, store, or disclose data. The Chief Information Officer will identify these groups. The Data Advisory Team will determine the annual training topics for these targeted groups based on District training needs.
5. Information Systems will monitor whether individuals have participated in the training and provided a signed copy of the Employee Non-Disclosure Agreement.

5 DATA DISCLOSURE

5.1 PURPOSE

Providing data to persons and entities outside of the District increases transparency, promotes education in Utah, and increases knowledge about Utah public education. This Plan establishes the protocols and procedures for sharing data maintained by the District. It is consistent with the disclosure provisions of the Federal Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, 34 CFR Part 99, and Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401.

5.2 POLICY FOR DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

5.2.1 Student or Student's Parent/Guardian Access

Parent or Guardian access to their student's record can be obtained from the student's school. In accordance with FERPA, 20 U.S.C. § 1232g (a)(1) (A) (B) (C) and (D), schools will provide parents with access to their child's education records, or provide 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. The District is not required to provide data that it does not maintain, nor is it required to create education records in response to an eligible student's request.

5.2.2 Third Party Vendor

Third party vendors may have access to students' personally identifiable information if the vendor is designated as a "school official" as defined in FERPA, 34 CFR §§ 99.31(a)(1) and 99.7(a)(3)(iii). A school official may include parties such as: professors, instructors, administrators, health staff, counselors, attorneys, clerical staff, trustees, members of committees and disciplinary boards, and a contractor,

consultant, volunteer or other party to whom the school has outsourced institutional services or functions.

All third-party vendors contracting with the District must be compliant with Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401. Vendors determined not to be compliant may be prohibited from entering into future contracts with the District, without third-party verification that they are compliant with federal and state law, and board policy.

5.2.3 Internal Partner Requests

Internal District partners include LEA and school officials that are determined to have a legitimate educational interest in the information. All requests shall be documented in the District's data request ticketing system.

5.2.4 Governmental Agency Requests

Without obtaining prior parental consent, the District may not disclose personally identifiable information of students to a governmental agency for research or evaluation purposes if the research or evaluation is not directly related to a state or federal program reporting requirement, audit, or evaluation. In order to disclose this information without parental consent, the requesting governmental agency must provide the District with evidence of one of the following in order to satisfy FERPA disclosure exceptions:

a) State or federal reporting requirement;
b) State or federal audit; or
c) State or federal evaluation.

The Director of Assessment and Evaluation and Chief Information Officer will ensure the proper data disclosure avoidance are included if necessary. An Interagency Agreement must be reviewed by legal staff and must include "FERPA-Student Level Data Protection Standard Terms and Conditions or Required Attachment Language."

5.3 Procedures for External disclosure of Non-Personally Identifiable Information (PII)

5.3.1 Scope

Governs external data requests from individuals or organizations that are not intending on conducting external research or are not fulfilling a state or federal reporting requirement, audit, or evaluation.

5.3.2 Student Data Disclosure Risk Levels

The District has determined three levels of data requests with corresponding procedures for appropriately protecting data based on risk: Low, Medium, and High. The Director of Assessment and Evaluation and Chief Information Officer will make final determinations on classification of student data requests risk level.

5.3.2.1 Low-Risk Data Request Process

Definition: High-level aggregate data
Examples:

- Graduation rate by year for the state
- Percent of third-graders scoring proficient on the SAGE ELA assessment

Process: Requester completes external research form and submits it to the Director of Assessment and Evaluation.

5.3.2.2 Medium-Risk Data Request Process

Definition: Aggregate data, but because of potentially low "n-sizes", the data must have disclosure avoidance methods applied.

Examples:

- Graduation rate by year and LEA
- Percent of third-graders scoring proficient on the SAGE ELA assessment by school
- Child Nutrition Program Free or Reduced Lunch percentages by school

Process: Requester completes external research form and submits it to the Director of Assessment and Evaluation.

5.3.2.3 High-Risk Data Request Process

Definition: Student-level data that are de-identified.

Examples:

- De-identified student-level graduation data
- De-identified student-level SAGE ELA assessment scores for grades 3-6.

Process: Requester completes external research form and submits it to the Director of Assessment and Evaluation.

5.4 Data Disclosure to a Requesting External Researcher or Evaluator

Responsibility: The Director of Assessment and Evaluation will ensure proper data is shared with external researcher or evaluator to comply with federal and state law, and board policies and district administrative procedures.

The District may not disclose personally identifiable information of students to external persons or organizations to conduct research or evaluation that is not directly related to a state or federal program audit or evaluation. Data that do not disclose PII may be shared with external researcher or evaluators for projects unrelated to federal or state requirements if:

1. A Salt Lake City School District Director, Superintendent, or board member sponsors an external researcher or evaluator request.
2. Student data is not PII and is de-identified through disclosure avoidance techniques and other pertinent techniques as determined by the Data Advisory Team.
3. Researchers and evaluators supply the District with a copy of any publication or presentation that uses District data at least 10 business days prior to any publication or presentation.

Process: Research Proposal must be submitted using this form:
http://www.slcschools.org/departments/assessment-and-evaluation/documents/External-Research-

Application.pdf. Research proposals must be sent directly to the Director of Assessment and Evaluation for review.

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 PROCEDURES

The District shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, District staff shall follow industry best practices outlined in the IT Security Plan for responding to the breach. Further, the District 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 Chief Information Officer who will collaborate with appropriate members of the District IT security response team to determine whether a security breach has occurred. If the District data breach response team determines that one or more employees or contracted partners have substantially failed to comply with District's IT Security Plan and relevant privacy policies and procedures, 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 Chief Information Officer must be reported immediately to the Business Administrator or Superintendent.

7 RECORD RETENTION AND EXPUNGEMENT

7.1 PURPOSE

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

7.2 SCOPE

Applies to all Salt Lake City School District board members and staff.

7.3 POLICY

The District, staff, and schools shall retain and dispose of student records in accordance with Utah Code Sections 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 Utah Code Section 53A-1-1407, the District shall expunge student data that is stored upon request of the student if the student is at least 23 years old. The District may expunge medical records and behavioral test assessments. The will not expunge student records of grades, transcripts, and a record of the student's enrollment or assessment information. District staff will collaborate with Utah State Archives and Records Services in updating data retention schedules. Any data that is kept for evaluation purposes will be de-identified prior to permanent storage.

District maintained student-level discipline data will be expunged three years after the data is no longer needed.

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 is addressed in five areas:

8.1.1 Data Governance Structure

The District data governance plan is structured to encourage the effective and appropriate use of educational data. The District data governance structure centers on the idea that data is the responsibility of all District schools and departments 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 District receives training from and regularly communicates with the Utah State Board of Education regarding data requirements and definitions.

8.1.3 Data Auditing

The Data Advisory Team and supporting staff perform regular and ad hoc data auditing. They analyze data in the warehouse for anomalies, and investigate the source of the anomalies.

8.1.4 Quality Control Checklist

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

9 DATA TRANSPARENCY

Annually, Salt Lake City School District will publically post:

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

10 APPENDIX

Appendix A. Salt Lake City School District Employee Non-Disclosure Agreement

As an employee of the Salt Lake City School District, I hereby affirm that: (Initial)

_____ I have read the Employee Non-Disclosure Assurances attached to this agreement form and read and reviewed Data Governance Plan, and all applicable Salt Lake City School District policies and procedures. These assurances address general procedures, data use/sharing, and data security.

_____ I will abide by the terms of the Salt Lake City School District's board policies and corresponding district plans, processes, 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.

Using Salt Lake City School District 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 Salt Lake City School District system user accounts, with Salt Lake City School District staff or participating program staff.

_____I will log out of and close the browser after each use of Salt Lake City School District 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 Salt Lake City School District server.

Reporting & Data Sharing

_____ I will not disclose or share any confidential data analysis except to other authorized personnel without the expressed written consent of the data advisory team (Chief Information Officer, Director of Assessment and Evaluation, and the Executive Director of Policy and Legal Services)

_____ I will not publically 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 by the Chief Information Officer.

_____ I understand that when sharing child/staff-identifying data with authorized individuals, the only approved methods are phone calls, Salt Lake City School District's Secure File Transfer Protocol (SFTP), or other secure methods as approved by the Chief Information Officer. Also, sharing within secured server folders is appropriate for Salt Lake City School District 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 Salt Lake City School District Chief Information 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 Salt Lake City School District 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 Salt Lake City School District, I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone outside of Salt Lake City School District without the prior written permission of the Chief Information Officer of Salt Lake City School District.

Print Name: _____

Signed: _____

Date: _____

Appendix B. Protecting PII in Public Reporting

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 Salt Lake City School District 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