Data Governance Plan

Scope and Applicability

This Plan is applicable to all employees, temporary employees, and contractors of the District. The 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 fourteen subsections are included in this Plan:

1. Standard Terms
2. Standard Policies and Procedures
3. Data Advisory Team (Decision-making authority)
4. Data Inventories
5. Data Content Management
6. Data Access
7. Non-Disclosure Assurances for Employees
8. Data Security and Privacy Training for Employees
9. Data Disclosure
10. Data Breach
11. Record Retention and Expungement (Data records management)
12. Data Quality
13. Transparency
14. External Research

Standard Terms

Direct identifiers include information that relates specifically to an individual such as the individual's residence, including for example, name, address, Social Security Number or other identifying number or code, telephone number, e-mail address, or biometric record.

Education records are those records that are directly related to a student and are maintained by an educational agency or institution or by a party acting for the agency or institution. For more information, see the Family Educational Rights and Privacy Act (FERPA), 34 CFR §99.3.

Indirect identifiers include information that can be combined with other information to identify specific individuals, including, for example, a combination of gender, birth date, geographic indicator and other descriptors. Other examples of indirect identifiers include place of birth, race, religion, weight, activities, employment information, medical information, education information, and financial information.

Personally identifiable information (PII) includes information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. See FERPA, 34 CFR §99.3, for a complete definition of PII specific to education data and for examples of education data elements that can be considered PII. PII includes, but is not limited to:

- First and last name
- Names of family members

- Address
- Email address and contact info
- Telephone number
- Social Security number
- Biometric data
- Health or disability data
- Student ID
- Username, Password, Alias
- If associated with PII student data,
    - Custom number held in a cookie
    - Processor serial number
    - Combination of students last name or photograph with other information that permits a person to contact them online
    - Information about a student or a student's family that a person collects online and combines with other PII to identify the student and information that alone or in combination would allow a reasonable person to identify the student with reasonable certainty

Sensitive data are data that carry the risk for adverse effects from an unauthorized or inadvertent disclosure. This includes any negative or unwanted effects experienced by an individual whose PII was the subject of a loss of confidentiality that may be socially, physically, or financially damaging, as well as any adverse effects experienced by the organization that maintains the PII. See Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), (NIST Special Publication 800-122, 2010) for more information.

Aggregate Data are data expressed in summary form for purposes of statistical analysis. Aggregate data does not contain PII. Summary counts must have a sample size of at least 10 individuals to be reported. Reports with sample sizes less than 10 can be confidentially shared with district employees but may not be shared externally or in public presentations.

Standard Policies and Procedures

This Plan is governed by the following federal and state laws, state board rule, and Salt Lake City School District board policies and administrative procedures.

1. Family Educational Rights and Privacy Act (FERPA)
2. Children's Online Privacy Protection Rule (COPPA)
3. Protection of Pupil Rights Amendment (PPRA)
4. Utah Student Privacy and Data Protection
5. Utah Admin. Code, Rule R277-487: Public School Data Confidentiality and Disclose
6. Board Policy S-2: Student Records, Privacy Rights, and Release of Information
7. Board Policy I-18: Acceptable Student Use of Internet, Computers, and Network Resources
8. Board Policy P-8: Acceptable Employee Use of Internet, Computers, and Network Resources
9. District IT Security Plan
10. Data Collection/Privacy Notice

Data Advisory Team

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.

District Data Manager (Chief Information Officer)

1. Authorizes and manages 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. Shares or authorizes sharing of 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 Division of Juvenile Justice Services;
   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 share student data, including personally identifiable student data, in response to a request to share student data for the purpose of research or evaluation, if the student data manager:
   1. verifies that the request meets the requirements of 34 C.F.R. §99.31(a)(6);
   2. submits the request to the education entity's research review process; and
   3. fulfills the instructions that result from the review process.
5. Will create and maintain a list of all District staff that have access to personally identifiable student data.
6. Ensure all staff members, including certain volunteers, receive annual District level training on data privacy. Document all staff names, roles, and training dates, times, locations, and agendas.
7. Is responsible for monitoring completion of data privacy training by employees.

IT Systems Security Manager (Chief Information Officer)

1. Acts as the primary point of contact for 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. May provide an annual report to the board on the District's systems security needs.

Supervisor 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.

General Counsel

1. Acts as legal representative to ensure all procedures and policies comply with federal and state law.

Non-Disclosure Assurances for Employees

Employee non-disclosure assurances are intended to minimize the risk of human error and misuse of information. 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 certain volunteers) must complete District Acceptable Use Policy Review, Student Privacy Rights (FERPA), and Protecting Student Data training in the District training system and electronically sign the Employee Non-Disclosure agreement at the end of the trainings. Contractors

and volunteers with access to student data must complete District Acceptable Use Policy Review, Student Privacy Rights (FERPA), and Protecting Student Data training and sign and follow the Salt Lake City School District Employee Non-Disclosure Agreement (See Appendix A), which describes the permissible uses of District technology and information.

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.

All student data utilized by the District is protected in accordance with FERPA, Utah law, and District board policies. 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 and Information Technology office. All District employees (including contract or temporary) will:

1. Complete District Acceptable Use Policy Review, Student Privacy Rights (FERPA), and Protecting Student Data training annually.

2. Complete a security and privacy training for researchers and evaluators, if the employee's 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 District-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 PII 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 PII 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 PII in reports, by aggregating, data suppression, rounding, recoding, 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.

Data Security and Privacy Training

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.

These training requirements are applicable to all District board members, employees, contracted partners, and volunteers with access to student data. Any individual that does not comply may not be able to use District networks or technology.

The required student data privacy trainings are:

1. District Acceptable Use Policy Review
2. Student Privacy Rights (FERPA)
3. Protecting Student Data

Employees must complete the training by October 1 of each school year. Volunteers, contractors, and temporary employees must complete the trainings prior to gaining access to any district system. Employees that start after October 1 must complete the training within 60 days.

The District requires a targeted District Acceptable Use Policy Review, Student Privacy Rights (FERPA), and Protecting Student Data training for 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.
The Information Technology office will monitor whether individuals have participated in the training and provided a signed copy of the Employee Non-Disclosure Agreement.

Data Disclosure

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 FERPA, 20 U.S.C. 1232g, 34 CFR §99, and Utah's Student Data Protection Act (SDPA), Utah Code Ann. §53E-9-3 et seq.

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. Information on requesting access to student educational records can be found in the S-2: Student Records, Privacy Rights, and Release of Information.

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) and Utah Code Ann. § 53E-9-301(19). 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.

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

Governmental Agency Requests
Without obtaining prior parental consent, the District may not disclose PII 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:

1. State or federal reporting requirement;
2. State or federal audit; or
3. State or federal evaluation.

The Chief Information Officer will ensure the proper data disclosure avoidance safeguards are included if necessary. An Interagency Agreement must be reviewed by General Counsel and must include "FERPA-Student Level Data Protection Standard Terms and Conditions" or the required attachment.

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

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.

The District has determined three levels of data requests with corresponding procedures for appropriately protecting data based on risk: low, medium, and high. The Supervisor of Assessment and Evaluation and the Chief Information Officer will make final determinations on classification of student data requests risk level.

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 End of Level ELA assessment

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 school district
- Percent of third-graders scoring proficient on the End of Level ELA assessment by school
- Child Nutrition Program Free or Reduced Lunch percentages by school

High-Risk Data Request Process
Definition: Student-level data that are de-identified.

Examples:

- De-identified student-level graduation data
- De-identified student-level End of Level ELA assessment scores for grades 3-6.

Data Disclosure to a Requesting External Researcher or Evaluator

All such requests must be submitted to the Supervisor of Assessment and Evaluation on a completed external research form.

Research Proposals must be submitted using this form: https://apex.slcschools.org/apex/r/slcsd/data-external-research-requests/data-public-records-research-requests for review.

Responsibility: The Supervisor 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 PII of students to external persons or organizations to conduct research or evaluation that is not directly related to a district, 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.

The District student data manager may share student data, including personally identifiable student data, in response to a request to share student data for the purpose of research or evaluation, if the student data manager:

- verifies that the request meets the requirements of **34 C.F.R. §99.31(a)(6);**
- submits the request to the education entity's research review process;
- fulfills the instructions that result from the review process;
- maintains and protects the student data in accordance with board policy and Utah Code Ann. §53E-9-307;
- ensures that the student data is not used for a purpose not allowed by Utah Code Ann. §26-7-4; and
- is subject to audit by the state student data officer described in Utah Code Ann. §53E-9-302.

In accordance with state and federal law, the student data manager shall share student data, including personally identifiable student data, as requested by the Utah Registry of Autism and Developmental Disabilities (URADD) described in Utah Code Ann. §26B-7-115.

Research Proposals must be submitted using this form: https://apex.slcschools.org/apex/r/slcsd/data-external-research-requests/data-public-records-research-requests Research proposals must be sent directly to the Supervisor of Assessment and Evaluation for review.

Data Breach

A data breach is any instance in which there is an unauthorized release or access of PII or other information not suitable for public release. This definition applies regardless of whether an organization stores and manages its data directly or through a contractor, such as a cloud service provider. Data breaches can take many forms including:

- hackers gaining access to data through a malicious attack;
- lost, stolen, or temporarily misplaced equipment (e.g., laptops, mobile phones, portable thumb drives, etc.);
- employee negligence (e.g., leaving a password list in a publicly accessible location, leaving computers unlocked, technical staff mis-configuring a security service or device, etc.); and
- safeguards and/or system failure (e.g., a safeguard that doesn't require multiple overlapping security measures—if backup security measures are absent, failure of a single protective system can leave data vulnerable).

Data Breach Response Team

The District's data breach response team ("District response team") consists of the District's Chief Information Officer, and various senior network services administrators responsible for different areas including the client/server environment, networking, student and financial systems, and databases and development.

Data Breach Response Plan

In the event of a significant data breach or inadvertent disclosure of PII, District staff will complete the following steps:

1. The District response team will be alerted and activated. Chief Information Officer will act as incident manager.
2. The Chief Information Officer will inform the District Superintendent, Business Administrator, and General Counsel of the potential data breach.
3. Response team will notify the Utah Education and Telehealth Network (UETN) security team for response support.
4. District response team will validate the data breach.
5. The District response team and UETN will begin documentation of everything surrounding the potential breach including date and time when the potential breach was discovered, who discovered the potential breach, who reported it, all who know about the potential breach, what type of breach occurred, what was compromised, how it was compromised, what systems are affected, what devices are missing, etc.
6. District response team will stop additional data loss by taking affected machines offline without shutting them down.
7. District response team will interview individuals involved in discovering the breach and anyone else who may know about it. Interviews will be documented.

8. Chief Information Officer will present gathered information to District Superintendent, Business Administrator, General Counsel, and Executive Director of Communications and Community Relations to develop a communication plan based upon the scope of the breach. All communications will abide by the following principles:
    a. Reach out to data owners as soon as possible to notify them of the breach.
    b. Foster a cooperative relationship between District leadership, response team, and data owners.
    c. Work collaboratively with data owners to secure sensitive data, mitigate the damage that may arise, and determine the root cause(s) of the breach to devise mitigating strategies and prevent future occurrences.
    d. Notify law enforcement, if needed, after consultation with General Counsel.
9. District response team will continue to review breach response documentation and analyses reports to complete the following:
    a. Identify root cause of breach.
    b. Address and/or mitigate the cause(s) of the data breach.
    c. Solicit feedback from the responders and affected entities.
    d. Review breach response activities and feedback from involved parties to determine response effectiveness.
    e. Make necessary modifications to breach response strategy to improve response process.
10. In the event of a significant data breach, the District will notify (a) the student, or (b) the student's parent, if the student is not an adult student. (Utah Admin. Code R277-487-3(3))
11. In the event of a significant data breach, the District will report the breach to the Utah State Board of Education within 10 business days of the initial discovery. (Utah Admin. Code R277-487-3(3))

Record Retention and Expungement

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

Information on amending student records can be found in the S-2: Administrative Procedures Student Records, Privacy Rights, and Release of Information.

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

The District recognizes the risk associated with data following a student year after year that could be used to mistreat the student. The District shall review all requests for records expungement from parents and make a determination based on the following procedure.

7.1 Procedure

The following records may not be expunged: grades, transcripts, a record of the student's enrollment, assessment information.

The procedure for expungement shall match FERPA's record amendment procedure found in 34 CFR 99, Subpart C.

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.
2. The District shall decide whether to expunge the data within a reasonable time after the request.
3. If the District decides not to expunge the record, they will inform the parent of their decision as well as the right to an appeal hearing.

4. The District shall hold the hearing within a reasonable time after receiving the request for a hearing.
5. The District shall provide the parent notice of the date, time, and place in advance of the hearing.
6. The hearing shall be conducted by any individual that does not have a direct interest in the outcome of the hearing.
7. The District 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.
8. The District shall make its decision in writing within a reasonable time following the hearing.
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.
10. If the decision is to expunge the record, the District will seal it or make it otherwise unavailable to other staff and educators.

Quality Assurances and Transparency Requirements

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 four areas:

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.
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.
3. Data Auditing. The District's data advisory team and supporting staff perform regular and ad hoc data auditing. They analyze data in the data warehouse for anomalies and investigate the source of the anomalies.
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.

Data Transparency

Annually, the District will publicy post:

- Metadata Dictionary as described in Utah's Student Data Protection Act, Utah Code Ann. §53E-9-3 et seq.

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 board 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 student/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, Supervisor of Assessment and Evaluation, and General Counsel).

_____ I will not publically publish any data without the approval of the District Data Manager.

_____ I will take steps to avoid disclosure of personally identifiable information in state-level reports, such as aggregating, data suppression, rounding, recoding, 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 student/staff-level data externally unless explicitly authorized in writing by the District Data Manager.

_____ I understand that when sharing student/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 District Data Manger (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 student/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: _____

Appendix B. Protecting PII in Public Reporting

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 District is comprehensive, the data made available to the public is masked to avoid unintended disclosure of personally identifiable information at summary school, school district, 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"

Date: _____

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.