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 Canyons School District ("Agency") takes seriously its moral and legal responsibility to protect student privacy and ensure data security. Utah's Student Privacy and Data Protection Act (SPDPA), U.C.A §53E-9-301, et seq. requires that Canyons School District adopt a Data Governance Plan.

2 SCOPE AND APPLICABILITY

Official Procedures **of the** **Canyons School District**	
Effective/Revision Date: 5/10/2019	
Policy Title: Canyons School District Data Governance Plan	

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

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 Canyons School District Data Governance Plan works in conjunction with additional Canyons District security processes and procedures for:

- System 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

Canyons School District has a Data Advisory Team, which consists of District leadership who have responsibility for providing data to internal and external data governance structure to ensure that data is protected at all levels of Canyons School District's educational system.

3.2 INDIVIDUAL AND GROUP RESPONSIBILITIES

The following tables outlines individual Canyons School District staff and advisory group responsibilities:

Role	Responsibilities
LEA Student Data Manager	1. Authorize and manage the sharing, outside of the education entity, of personally identifiable student data from a cumulative record for the education entity. 2. Act as the primary local point of contact for the state student data officer. 3. May share personally identifiable student data that is: a. referring to a student with the student and the 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. 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. Acts as the primary point of contact for State student data security administration.

IT Systems Security Manager	1. Ensures compliance with security systems laws throughout the public education system, including producing resource materials, model plans, and model forms for LEA systems security. 2. Investigates complaints of alleged violations of systems breaches.
Director of Research and Assessment	1. Acts as the primary point of contact for external research requests. 2. Directs staff who provide reports to internal stakeholders.
Director of 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 Canyons School 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

1. All Canyons School District board members and employees are expected to comply with board policies and District administrative procedures. Within the first two-weeks of employment, all Canyons School employees, and contracted partners must participate in CSD's Critical Policies training and follow the Canyons School District's Responsible Access and Use Conduct Guideline, which describes the permissible uses of technology and information.

4.2 NON-DISCLOSURE ASSURANCES

All student data utilized by Canyons School District is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and Utah statute. These procedures outline the way Canyons School District staff is to utilize data and protect personally identifiable and confidential information. All employees are trained and agree to adhere and abide by these practices during the annual Critical Policies training. Each employee shall sign the Critical Policies Read and Sign document annually to agree to adhere to/abide by these practices. All Canyons School District employees (including contract or temporary) will:

1. Complete CSD's Critical Policies training and sign the Critical Policies Read and Sign document.
2. Consult with Canyons School District internal data owners when creating or disseminating reports containing data.
3. Use password-protected LEA-authorized computers when accessing any student-level or staff-level records.
4. NOT share individual passwords for personal computers or data systems with anyone.

5. Log out of any data system/portal and close the browser after each use.
6. 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.
7. Keep printed reports with personally identifiable information in a locked location while unattended and use the secure document destruction service provided at Canyons School District when disposing of such records.
8. NOT share personally identifying data during public presentations, webinars, etc. If users need to demonstrate student/staff level data, demo records should be used for such presentations.
9. 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 A (Protecting PII in Public Reporting).
10. Take steps to avoid disclosure of personally identifiable information in reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.
11. Delete files containing sensitive data after using them on computers or move them to secured servers or personal folders accessible only by authorized parties.
12. 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.
13. Use secure methods when sharing or transmitting sensitive data. The approved method is sharing within the District's secured server folders, using the Districts FTP site, or the District's email encryption tools.
14. NOT transmit student/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.
15. Limit use of individual data to the purposes which have been authorized within the scope of job responsibilities.

4.3 DATA SECURITY AND PRIVACY TRAINING

4.3.1 Purpose

Canyons School District will provide training opportunities for all Canyons School 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.

4.3.2 Scope

All Canyons School District employees, and contracted partners.

4.3.3 Compliance

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

4.3.4 Policy

2. Within the first two-weeks of employmentall Canyons School District employees, and contracted partners must participate in CSD's Critical Policies training and follow the Canyons School District's Responsible Access and Use Conduct Guideline, which describes the permissible uses of technology and information.
3. New employees that do not comply may not be able to use Canyons School District networks or technology. Within the first two-weeks of employment, all Canyons School District employees, and contracted partners also must sign and obey the Canyons School District Employee Confidentiality Agreement, which describes appropriate uses and the safeguarding of student and educator data.
4. All Canyons School Districtemployees, and contracted partners are required to participate in an annual Critical Policies Training and sign the Critical Policies Read and Sign document.
5. Supervisors will annually monitor participation in the training as well as signed copies of the employee documents.

5 DATA DISCLOSURE

5.1 PURPOSE

Providing data to persons and entities outside of the Canyons School District increases transparency, promotes education in Canyons School District, and increases knowledge about Utah public education. These procedures establish the protocols and procedures for sharing data maintained by Canyons School District. It is intended to be 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 Privacy and Data Protection Act (SPDPA), U.C.A §53E-9-301, et seq.

5.2 POLICY FOR DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

5.2.1 Student or Student's Parent/Guardian Access

In accordance with FERPA regulations 20 U.S.C. § 1232g (a)(1) (A) (B) (C) and (D), Canyons School District will provide parents with access to their student'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. Canyons School District is not required to provide data that it does not maintain, nor is Canyons School District 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. Vendors that will have access to, or maintain Personally Identifiable Information, must agree to and annually sign Canyons School District Vendor Non-Disclosure Agreement.

All third-party vendors contracting with Canyons School District must be compliant with Utah's Student Privacy and Data Protection Act (SPDPA), U.C.A §53E-9-301, et seq. Vendors determined not to be compliant may not be allowed to enter into future contracts with Canyons School District without third-party verification that they are compliant with federal and state law and board rule.

5.2.3 Internal Partner Requests

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

5.2.4 Governmental Agency Requests

Canyons School 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 reporting requirement, audit, or evaluation. The requesting governmental agency must provide evidence the federal or state requirements to share data in order to satisfy FERPA disclosure exceptions to data without consent in the case of a federal or state

a) reporting requirement
b) audit
c) evaluation

The Student Data Manager 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 Policy for External disclosure of Non-Personally Identifiable Information (PII)

5.3.1 Scope

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

Canyons School District has determined three levels of data requests with corresponding policies and procedures for appropriately protecting data based on risk: Low, Medium, and High. The Student Data Manager 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 Research and Assessment.

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 Research and Assessment.

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 Research and Assessment.

5.4 Data Disclosure to a Requesting External Researcher or Evaluator

Responsibility: The Student Data Manager will ensure the proper data are shared with external researcher or evaluator to comply with federal, state, and board rules.

Canyons School 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. Student data are not PII and are de-identified through disclosure avoidance techniques and other pertinent techniques as determined by the Student Data Management.
2. Researchers and evaluators supply the Canyons School District a copy of any publication or presentation that uses Canyons School District data 10 business days prior to any publication or presentation.

Process: Requester follows the steps outlined on the Conducting Research in Canyons web site. The site can be found at *http://www.canyonsdistrict.org/external-research.*

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

Canyons School 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, Canyons School District staff shall follow industry best practices for responding to the breach. Further, Canyons School 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 Director of Information Technology, who will collaborate with appropriate members of the District technology team to determine whether a security breach has occurred. If it is determined that one or more employees or contracted partners have substantially failed to comply with Canyons School District's 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 Director of Information Technology must be reported to the IT Director's supervisor immediately.

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

Records retention applies to records of all Canyons School District staff and the Board of Education

7.3 POLICY

The Canyons School District, staff, and schools shall retain and dispose of student records in accordance with Section 63G-2-604, 53E-9-306, and shall comply with active retention schedules for student records per Utah Division of Archive and Record Services.

In accordance with 53E-9-306, the Canyons School District shall expunge student data that is stored upon request of the student if the student is at least 23 years old. The Canyons School District may expunge medical records and behavioral test assessments. Canyons School District will not expunge

student records of grades, transcripts, and a record of the student's enrollment or assessment information. Canyons School District staff will collaborate Utah State Archives and Records Services in updating data retention schedules.

Canyons School District 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 Canyons School District data governance policy is structured to encourage the effective and appropriate use of educational data. The Canyons School District data governance structure centers on the idea that data is the responsibility of all Canyons School 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

Canyons School District's technology team perform regular and ad hoc data auditing. They analyze data in the warehouse for anomalies, investigate the source of the anomalies, and work with departments and/or LEAs in explaining and/or correcting the anomalies.

9 Data Transparency

Annually, Canyons School District will publicly post:

- Metadata Dictionary as described in Utah's Student Privacy and Data Protection Act (SPDPA), U.C.A §53E-9-301, et seq.

10 APPENDIX

Appendix A. 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 Canyons School District is comprehensive, the data made available to the public is masked to avoid unintended disclosure of personally identifiable information at summary school or LEA -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)