Cache County School District

Data Governance Plan

I. Purpose

Data governance is an approach to data and information management that is formalized as a set of policies and procedures which encompass the full life cycle of data; from acquisition, to use, to disposal. The Cache County School District (CCSD) 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 CCSD adopt a Data Governance Plan.

II. Applicability

This plan is applicable to all employees, temporary employees, and third-party contractors of the school district. It will be reviewed and adjusted on an annual basis or more frequently, as needed. This plan is designed to ensure only authorized disclosure of personally identifiable or confidential information.

III. Information Technology Security Plan

The CCSD Data Governance Plan works in conjunction with the Information Technology Security Plan.

IV. Data Governance Team

The CCSD has appointed the following positions to ensure that data is protected at all levels:

A. Chief Information Officer
   1. Authorized to appoint members of the Data Governance Team.
   2. Oversees the work of the Data Governance Team.
   3. Maintains the Information Technology Security Plan.
   4. Investigates complaints of alleged violations of systems breaches.
   5. Provides an annual report to the board on CCSD's systems security needs.

B. Student Data Manager
   1. Maintains the Data Governance Plan, Metadata Dictionary and third party contracts.
   2. Authorizes and manages the sharing, outside of the education entity, of personally identifiable or confidential student data from a cumulative record for the education entity.
   3. Acts as the primary local point of contact for the state Student Data Officer.
   4. Creates and maintains a list of all LEA staff that have access to personally identifiable or confidential student data.
   5. Ensures annual LEA-level training on data privacy to all staff members with access to personally identifiable or confidential information, including volunteers. Documents all staff names, roles, and training dates, times, locations, and agendas.
   6. Manages Research Application requests

C. Information Systems Manager
   1. Collects, manages, maintains and ensures the security of student data and secure transmission of data in and between any of the district's information systems,

including PowerSchool, Upland Document Management, Caredox, curriculum and associated programs, messaging systems and transfer of data to USBE.
2. Works closely with district and school personnel to ensure secure transmission of student data between district and school personnel as well as other LEA personnel.
3. Works closely with the Student Data Manager to fulfill approved data requests.
4. Works closely with the Security Officer to ensure the security of student data.

D. Security Officer
1. Acts as the primary point of contact for implementation of the Information Technology Security Plan.
2. Investigates complaints of alleged violations of systems breaches.

V. Data Classification Levels

A. Class 1 Personally Identifiable or Confidential Information

Class 1 Data is personally identifiable information (PII) or confidential information that is collected or assigned to students or staff members. This information includes:

1. A student or employee ID
2. A place and/or date of birth
3. Personal address and phone numbers
4. Personal email addresses
5. Social Security Number
6. Medical records
7. Bank account information
8. Staff or student evaluations
9. Private education records such as ESL, 504 or Special Education records.
10. System access passwords or file encryption keys

Unauthorized or improper disclosure, modification, or destruction of this information could violate state and federal laws, result in civil and criminal penalties, and cause serious legal implications. Class 1 Data is kept primarily in the following electronic systems: PowerSchool, Munis, and the Active Directory System, and the following third party vendors Caredox, InfinityHR, and the Upland Document Management System. Some student information such as a student's name or student ID is also kept in a variety of curriculum programs. Staff and student data may also be kept in paper files in a student cumulative file or personnel file. If Class 1 Data is in an electronic format outside these systems it should be in an encrypted state, or if it is to be transmitted, it should be transmitted through a secure method. Class 1 electronic data should never be emailedå, stored on a computer hard drive or external storage device, or stored in the cloud (Google, Dropbox, etc.). If in printed format, Class 1 Data should be kept in a locked filing cabinet inside a locked facility. It should never be left unsecured and unattended on a desktop or in a drawer

B. Class 2: Private Information

Class 2 Data is private business or educational data that is part of the day to day operations of the school district. This information includes but is not limited to:

1. Business records such as contracts, bids, purchase requisitions, purchase orders, invoices, account numbers, budgets, job postings, interview documents, internal policies and procedures, etc..
2. Educational records such as attendance rolls, class rosters, student assignments, grades, quizzes, tests, etc.

3. Staff or student email or documents stored in student or staff accounts or on student or staff computers.

Unauthorized disclosure of this information to people without a business or educational need may violate federal or state laws and regulations, or violate the right to privacy of staff, parents, students, or business partners. Decisions about access to this information should always be cleared through the information owner or responsible parties. Class 2 Data should be kept private and care should be taken in storing this data in electronic or printed format. If possible, printed data should be kept in a locked facility. Class 2 Data is always subject to inspection by district or school officials.

C. Class 3 Data: Student Directory Information

Class 3 Data is Student Directory Information. This information includes:

1. Student first and last name
2. Student gender
3. Student home address
4. Student photograph
5. Student dates of attendance (years)
6. Student grade level
7. Student diplomas, honors, awards received
8. Student participation in school activities or school sports
9. Student weight and height for members of school athletic teams
10. Student most recent school attended

Cache County School District may disclose appropriately designated "directory information" without written parental consent, unless the parent has advised the district to the contrary. Notice of this policy is included in the district's summer mailing and published on the district website. The primary purpose of directory information is to allow the district to include this type of information in certain school publications. Examples include: A playbill, showing the student's role in a drama production, the annual yearbook, honor roll or other recognition lists, graduation programs, sports activity sheets, such as for wrestling, showing weight and height of team members. Directory information can also be disclosed to outside organizations without prior written consent. Outside organizations include, but are not limited to, companies that manufacture class rings or publish yearbooks or institutions of higher education. In addition, two federal laws require local educational agencies (LEAs) receiving assistance under the Elementary and Secondary Education Act of 1965 (ESEA) to provide military recruiters, upon request, with the following information – names, addresses and telephone listings.

D. Class 4 Data: Public Data

Class 4 Data is any information that may be shared with the public. Public Information may include, but is not limited to:

1. Calendar information on upcoming events or schedules.
2. Staff (name, business phone or business email).
3. General information about the district, school, or staff, registration information, etc..
4. Articles recognizing staff or student achievement.
5. Aggregated data such as assessment results, financial reports, and enrollment data.
6. Policies and procedures.
7. Blank Documents for student, staff or parent use.

VI. Employee Non-disclosure Assurances

Employee non-disclosure assurances are intended to minimize the risk of human error and misuse of information.

A. All CCSD board members, employees, contractors and volunteers, with access to personally identifiable or confidential information must sign and comply with the **CCSD Employee Non-Disclosure Agreement.** (See Appendix A)

B. All CCSD employees (including contract or temporary) with access to personally identifiable or confidential information will:

1. Complete Data Security and Privacy Training.
2. Consult with CCSD internal data stewards when creating reports containing personally identifiable or confidential information.
3. Keep printed reports with personally identifiable or confidential information in a locked location while unattended, use a paper shredder, or use the secure document destruction service provided at CCSD when disposing of such records. Flash drives, DVD, CD-ROM or other removable media, or personally owned computers or devices are not appropriate for storage of personally identifiable or confidential information.
4. Delete files containing personally identifiable or confidential information after using them on computers, or move them to secured servers or personal folders accessible only by authorized parties.
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. NOT use email to send screenshots, text, or attachments that contain personally identifiable or confidential information. If users receive an email containing such information, they must 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 Manager should be consulted.
8. NOT transmit child/staff-level data externally unless expressly authorized in writing by the data steward, and then only transmit data via approved methods.
9. NOT share personally identifiable or confidential information during public presentations, webinars, etc. If users need to demonstrate child/staff level data, demo records should be used when possible or personally identifiable or confidential information should be redacted in accordance with guidance in Appendix B (Protecting Personally Identifiable Information in Public Reporting).

VII. Data Security and Privacy Training

CCSD will provide training for all CCSD staff, including volunteers, contractors and temporary employees with access to student personally identifiable or confidential information in order to minimize the risk of human error and misuse of information. This training must be completed within 60 days of employment and repeated yearly.

VIII. Data Disclosure

This plan establishes the protocols and procedures for sharing data maintained by the CCSD. 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 Data Protection Act (SDPA), U.C.A §53A-1-1401.

A. Student or Student's Parent/Guardian Access

1. CCSD will provide parents with access to their child'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), within 45 days of receiving an official request.
2. CCSD is not required to provide data that it does not maintain, nor is CCSD required to create education records in response to an eligible student's request.

B. Third-Party Vendors
   1. Third-party vendors may have access to students' personally identifiable or confidential 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.
   2. All third-party vendors contracting with CCSD must be compliant with Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401. Vendors determined not to be compliant may not be allowed to enter into future contracts with CCSD without third-party verification that they are compliant with federal and state law, and board rule.

C. Governmental Requests
   1. CCSD may NOT disclose any student's personally identifiable or confidential information 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.

D. External disclosure of Non-personally identifiable or confidential information
   1. Some data that does not directly contain personally identifiable or confidential information may, nonetheless, be used to identify individual students. CCSD has thus determined three levels for appropriately protecting all data. based on risk: low, medium, and high. Following are guidelines for dealing with each level.
      a) Low-Risk Data - 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 the Data Request Form. Data Request is forwarded to the appropriate Data Steward. Data Steward fulfills the request and saves the dataset in a secure folder managed by the Student Data Manager.
      b) Medium-Risk Data Request Process - 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 the Data Request Form. Data Request is forwarded to the appropriate Data Steward, Data Steward fulfills the request, applies appropriate disclosure avoidance techniques, and sends to the Student Data Manager for Quality Assurance (QA) which ensures student data protection. If it passes QA, data are sent to the requester and the dataset is saved in a secure folder which is managed by the Student Data Manager. If it does not pass QA, the data are sent back to the Data Steward for modification.

c) High-Risk Data Request
Examples: De-identified student-level graduation data; de-identified student-level SAGE ELA assessment scores for grades 3-6.
Process: Requester completes a Data Request Form. If the request is approved, an MOA is drafted and sent to legal, placed on the CCSD School Board consent calendar, reviewed by the Chief Information Officer and sent to the Student Data Manager. The appropriate Data Steward fulfills the request and de-identifies the data as appropriate, then sends it to another Data Steward for QA (ensuring student data protection). If it passes QA, data are sent to the requester and the dataset is saved in a secure folder. If it does not pass QA, the data are sent back to the Data Steward for modification.

E. Data Disclosure to an External Researcher or Evaluator
The Student Data Manager will ensure that any data shared with external researchers or evaluators to comply with federal, state, and School Board rules. CCSD may not disclose personally identifiable information (PII) 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 researchers or evaluators for projects unrelated to federal or state requirements if:

1. A CCSD Director, Superintendent, or board member sponsors an external researcher or evaluator request.
2. Student data are not PII and are de-identified through disclosure avoidance techniques and other pertinent techniques as determined by the Student Data Manager.
Process: Data requests must be submitted using the CCSD Research Application Form. Research proposals are sent directly to the Student Data Manager for review. If the request is approved, a memorandum of understanding is drafted and sent to legal, placed on the School Board consent calendar, reviewed by the Chief Information Officer, sent to Student Data Manager, appropriate Data Steward fulfills request, de-identifies data as appropriate, and sends to another Data Steward for Quality Assurance (ensuring student data protection). If it passes QA, data are sent to requester and saves the dataset in a secure folder managed by the Student Data Manager. If it does not pass QA, the data are sent back to the Data Steward for modification.

IX. Data Breach

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. A 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.

A. CCSD shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, CCSD staff shall follow industry best practices as outlined in the district IT Security Plan for responding to the breach. Further, CCSD shall follow best practices for notifying affected parties, including students (in the case of an adult student), or parents/legal guardians (if the student is not an adult student).

B. Concerns about security breaches must be reported immediately to the IT security manager, who will then collaborate with appropriate members of the CCSD Data Governance Team to determine whether a security breach has occurred. If the Data Governance Team determines

that one or more employees or contracted partners have substantially failed to comply with CCSD Information Technology Security Plan and relevant privacy policies, they will refer the individual(s) to the Human Resource department for action, which may include termination of employment or a contract, and further legal action. Concerns about security breaches that involve the Security Officer must be reported immediately to the Chief Information Officer and Superintendent.

C. CCSD will provide and periodically update, in keeping with industry best practices, resources for Utah LEAs in preparing for and responding to a security breach.

X. Records Retention and Expungement

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

A. The CCSD, staff, Utah LEAs and schools shall retain and dispose of student records in accordance with Section 63G-2-604, 53A-1-1407, and shall comply with active retention schedules for student records per Utah Division of Archive and Record Services.

B. In accordance with 53A-1-1407, the CCSD shall expunge, upon request of the student, student data that is stored, if the student is at least 23 years old. The CCSD may expunge medical records and behavioral test assessments. The CCSD will not expunge student records of grades, transcripts, a record of the student's enrollment or assessment information. CCSD staff will collaborate with Utah State Archives and Records Services in updating data retention schedules.

C. CCSD- maintained student-level discipline data will be expunged after three years.

XI. Data Transparency

Annually, the CCSD will publically post:

A. CCSD data collections

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

Appendix A. CCSD Employee Non-Disclosure Agreement

Please initial your acknowledgement and affirmation of the following items.

As an employee of the CCSD, I hereby affirm that: Trainings

_____ I have completed or will complete CCSD's Data Security and Privacy Fundamentals Training within 60 days from the start of the school year.

Using CCSD Data and Reporting Systems

_____ I will not share or exchange individual passwords, for either personal computer(s) or CCSD system user accounts, with CCSD staff or participating program staff.

_____I will log out of and close the browser after each use of CCSD data and reporting systems.

_____I will only access data for which I have received explicit written permissions from the data's owner.

_____I will not attempt to identify individuals, except as is required to fulfill job or volunteer duties, nor will I publicly release a student's personally identifiable or confidential information.

Handling Sensitive Data

_____ I will keep sensitive data on password-protected, state-authorized computers.

_____ I will keep any printed files containing personally identifiable or confidential 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 (including from trash) containing sensitive data, after working with them, from my desktop, or move them to a secured CCSD server.

Reporting & Data Sharing

_____ I will not disclose or share any confidential data analysis, except to other authorized personnel, without CCSD's expressed written consent.

_____ I will not publically publish any data without getting approval from the Student Data Manager.

_____ I will take steps, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc., to avoid disclosure of personally identifiable or confidential information in state-level reports._____ I will <u>NOT</u> use email to send screenshots, text, or attachments that contain personally identifiable or confidential information 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.

_____ I understand that, when sharing child/staff-identifying data with authorized individuals, the only approved methods are phone calls or *CCSD's* method for securely sending data. Also, sharing within secured server folders is appropriate for a CCSD 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 CCSD Security 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 CCSD 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 any 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 the CCSD, I will not disclose or otherwise disseminate any confidential or personally identifiable or confidential information to anyone outside of the CCSD without the prior written permission of the CCSD Student Data Manager.

Print Name: _____

Signed: _____

Date: _____

Appendix B. Protecting Personally Identifiable or Confidential Information in Public Reporting

Data Gateway Statistical Reporting Method for Protecting Personally Identifiable Information (PII)

Public education reports offer the challenge of meeting transparency requirements while also meeting legal requirements to protect each student's PII. Recognizing this, the reporting requirements state that subgroup disaggregation of the data may not be published if the results would yield PII about an individual student. While the data used by the CCSD are comprehensive, the data made available to the public are masked to avoid unintentional disclosure of PIIat summary school, LEA, or state-level reports.

This is done by applying the following statistical method for protecting PII:

1. Underlying counts for group or subgroup totals are not reported.
2. If a reporting group has one 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 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)