



## **Cache County School District**

### **Policy Series 6000: Finance and Operations**

**Policy No. 6900 P1**

#### **Data Governance**

##### **Data Governance and Information Technology Security Team Titles and Major Responsibilities**

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

###### **Director of Technology**

- A. Oversees the work of the Data Governance Team.
- B. Authorized to appoint members of the Data Governance Team.
- C. Oversees Implementation of the Data Governance and Information Technology Security Procedures.
- D. Investigates complaints of alleged violations of systems breaches.

###### **Student Data Privacy Manager**

- A. Maintains the Metadata Dictionary and third-party contracts.
- B. 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.
- C. Acts as the primary local point of contact for the state Student Data Manager.
- D. Creates and maintains a list of all LEA staff categories that have access to personally identifiable or confidential student data.
- E. 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.
- F. Works with the grant and research administrator to fulfill approved data requests.
- G. Ensure the following notices are available to parents:
  - a. Annual FERPA notice (see 34 CFR 99.7),
  - b. Directory information policy (see 34 CFR 99.37),
  - c. Survey policy and notice (see 20 USC 1232h and 53E-9-203)
  - d. Data collection notice (see 53E-9-305)

###### **Employee Data Manager**

- A. Collects, manages, maintains and ensures the security of employee data and secure transmission of data in and between any of the district's information systems, including Enterprise ERP(Munis) and Active Directory or with outside entities such as Health Insurance providers, etc.
- B. Works closely with district and school personnel to ensure secure transmission of employee data.
- C. Works closely with the Security Officer to ensure the security of employee data.

###### **Student Data Manager**

- A. 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 SIS, PowerSchool SchoolMessenger and SafeArrival, PowerSchool



## **Cache County School District**

### **Policy Series 6000: Finance and Operations**

PowerHub, FileBound Document Management, various curriculum programs, any other associated programs, and transfer of data to USB.

- B. 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.
- C. Works closely with the Student Data Privacy Manager to fulfill approved data requests.
- D. Works closely with the Security Officer to ensure the security of student data.

#### **Security Officer**

- A. Acts as the primary point of contact for implementation of the Information Technology Security Procedures.
- B. Oversees district-wide IT security.
- C. Works closely with the Director of Technology to develop district policies and procedures concerning cyber security.
- D. Develops and implements internal processes ensuring adherence to the standards outlined in the Data Governance and Information Technology Security Policy and Procedures.
- E. Leads implementation of the district's selected security framework outlined in the associated procedures.
- F. Investigates complaints of alleged violations of systems breaches.

#### **Data Classification Procedures**

##### **Class 1 Personally Identifiable or Confidential Information**

Class 1 data is collected from students when they enroll at a particular school or from an employee during the hiring process.

Class 1 data is kept primarily in three key systems: PowerSchool SIS, Munis, and Active Directory. Other systems used for business and curriculum functions of CCSD use data from the three primary systems to provide the services offered by the district. These include but are not limited to lunch, transportation, secure document storage, and financial systems.

Some student information such as a student's name, student ID, and class schedule 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 an employee 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 shall not be stored on computer hard drives, external storage devices, or unapproved cloud services (e.g., Box, Dropbox), except in rare cases approved by the Security Officer, where additional disk encryption, such as FileVault, BitLocker, or other approved encryption software, is applied. Class 1 electronic data must be immediately deleted upon completion of any task requiring data stored in those methods. Furthermore, Class 1 electronic data should never be transmitted via unsecure email.



## **Cache County School District**

### **Policy Series 6000: Finance and Operations**

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.

#### **Class 2: Private Business or Educational Data**

Class 2 data is created in the course of doing business or in educating students and should be kept private and care should be taken in storing this data in electronic or printed format. When not actively being used, printed data should be stored in a locked room and/or locked cabinet.

#### **Class 3 Data: Student Directory Information**

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. Notice of this policy is included in the district's summer mailing and published on the district website.

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. Parents have the ability to opt out of sharing students' data.

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 and institutions of higher education, upon request, with the following information – names, addresses and telephone listings. Parents may opt out of the ESEA requirements, in writing, to the LEA, as required by law.

#### **Class 4 Data: Public Data**

Public data should be kept as up-to-date as possible.

### **Employee Training and Non-disclosure Assurances**

Employee non-disclosure assurances are intended to minimize the risk of human error and misuse of information. All CCSD employees (including contract or temporary) with access to Class 1 data will:

- A. Complete district provided Data Security and Privacy Training, including training covering "student privacy laws" as defined in Utah State Code 53E-9-204(3). Training shall also include training on "confidentiality of student data" per USBE Rule R277-487(3)(8) covering "employees' obligation to not disclose or transmit information to unauthorized parties". This training shall be completed annually.
- B. Consult with CCSD internal data stewards when creating reports containing Class 1 Data.

## Cache County School District

### Policy Series 6000: Finance and Operations

- C. Keep printed reports with Class 1 Data 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. Removable media, such as flash drives, and personally owned computers or devices are never suitable for storing personally identifiable or confidential information.
- D. Delete files containing Class 1 Data after using them on computers, or move them to secured servers or personal folders accessible only by authorized parties.
- E. Encrypt Class 1 Data whenever possible during storage outside of the primary systems that host such data.
- F. NOT share individual passwords for personal computers or data systems with anyone.
- G. Log out of any data system/portal and close the browser after each use.
- H. NOT use email to send screenshots, text, or attachments that contain Class 1 Data. 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 or Employee Data Manager should be consulted.
- I. NOT transmit child/staff-level data externally unless expressly authorized and then only transmit data via approved methods.
- J. NOT share Class 1 Data information during public presentations, webinars, etc. If users need to demonstrate child/staff level data, demo records should be used when possible or Class 1 Data should be redacted in accordance with guidance in Appendix B (Protecting Personally Identifiable Information in Public Reporting).
- K. Utilize two-factor authentication procedures for logging into computer systems, including Google, Enterprise ERP (Munis), district servers, and SIS systems as permitted.

All CCSD board members, employees, contractors, temporary employees, and volunteers, with access to Class 1 data must sign and comply with the **CCSD Employee Non-Disclosure Agreement (Form 1)**. CCSD will provide training for all CCSD staff, including volunteers, contractors and temporary employees with access to Class 1 Data 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.

#### Data Disclosure Procedures

Disclosure procedures are 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 §53E-9-308.

- A. Student or Student's Parent/Guardian Access
  - a. 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.
  - b. 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.

## Cache County School District

### Policy Series 6000: Finance and Operations

#### B. Third-Parties

- a. Third-parties may have access to students' Class 1 data if the third-party 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.
- b. All third-parties contracting with CCSD must be compliant with Utah's Student Data Protection Act (SDPA), U.C.A §53E-9-308. Third-parties determined not to be compliant may not be allowed to enter into future contracts with CCSD without verification that they are compliant with federal and state law, and board rule.

#### C. Governmental Requests

- a. CCSD may NOT disclose any student's Class 1 Data 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

- a. 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:
  - i. Low-Risk Data - High-level aggregate data
    1. Examples: Graduation rate by year for the state; percent of third-graders scoring proficient on the State Summative ELA assessment.
    2. Process: Requester completes the Data Request Form. Data Request is forwarded to the appropriate Data Steward. Data Steward fulfills the request and the Student Data Manager records the collection for inclusion in the publicly available data collection notice.
  - ii. Medium-Risk Data - Aggregate data, but because of potentially low n-sizes, the data must have disclosure avoidance methods applied.
    1. Examples: Graduation rate by year and LEA; percent of third-graders scoring proficient on the State Summative ELA assessment by school; Child Nutrition Program Free or Reduced Lunch percentages by school.
    2. 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 it to the Student Data Privacy Manager for Quality Assurance (QA) which ensures student data

## Cache County School District

### Policy Series 6000: Finance and Operations

protection. If it passes QA, data is sent to the requester and the Student Data Manager records the collection for inclusion in the publicly available data collection notice. If it does not pass QA, the data is sent back to the Data Steward for modification.

#### iii. High-Risk Data

1. Examples: De-identified student-level graduation data; de-identified student-level State Summative ELA assessment scores for grades 3-6.
2. Process: Requester completes a Data Request Form. If the request is approved, an MOU is drafted and sent to Legal, 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 is sent to the requester and the Student Data Manager records the collection for inclusion in the publicly available data collection notice. If it does not pass QA, the data is sent back to the Data Steward for modification.

#### E. Data Disclosure to an External Researcher or Evaluator

- a. The Student Data Manager will ensure that any data shared with external researchers or evaluators 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 does not disclose PII may be shared with external researchers or evaluators for projects unrelated to federal or state requirements if:
  - i. Student data is not PII and is de-identified through disclosure avoidance techniques and other pertinent techniques as determined by the Student Data Manager.
    1. Process: Data requests must be submitted using the CCSD Data Request Form. Research proposals are sent directly to the Student Data Privacy Manager for review. If the request is approved, a memorandum of understanding is drafted, if deemed necessary, and sent to legal, reviewed by the Instructional Council, sent to the Student Data Manager to fulfill the request, de-identifying data as appropriate, and sent to Student Data Privacy Manager (ensuring student data protection). If it passes QA, data is sent to the requester and the Student Data Manager records the collection for inclusion in the publicly available data collection notice.

#### Employee Privacy

- A. In accordance with Utah Code 53G-10-207 except as provided in Sections 53G-7-224 and 64G-2-204, CCSD may not sell or otherwise transfer an employee's work-related

## Cache County School District

### Policy Series 6000: Finance and Operations

contact information to a third party if the sale or transfer is an isolated or standalone transaction.

- B. CCSD does not require an employee to download, install, access, or otherwise use required technology on a personally owned electronic device if use of required technology contains terms, conditions, or data sharing provisions that would allow for access to data or information outside of the required technology.
  - a. If CCSD requires an employee to use required technology that the employee reasonably finds to contain objectionable terms and conditions, CCSD shall provide reasonable accommodations to the impacted employee to avoid mandatory use on the employee's personal device. Accommodations may include:
    - i. using a district owned computer, tablet, etc.; or
    - ii. through similar means that do not obligate personal device use.
  - b. The district will not take adverse action against an employee for exercising rights outlined in 53G-10-207.
  - c. Employees may file a written complaint with USBE alleging violations of 53G-10-207.

#### **Responding to a Data Incident or 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 this document for responding to the breach.
- B. CCSD shall follow USBE administrative rule R277-487-3 (3) for breaches defined in R277-487-2 (14) as "significant data breach". Further, CCSD shall follow State of Utah Code 63A-19-405 and 63A-19-406 for the reporting of a confirmed data breach and notifications of affected parties, including students (in the case of an adult student), or parents/legal guardians (if the student is not an adult student), or current/former employee.
- C. Concerns about security breaches must be reported immediately to the Security Officer, 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 Director of Technology and Superintendent.



## **Cache County School District**

### **Policy Series 6000: Finance and Operations**

#### **Records Retention**

Records retention and expungement procedures 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, 53E-9-306, and shall comply with active retention schedules for student records per Utah Division of Archive and Record Services.
- B. In accordance with 53E-9-306, the CCSD shall expunge, upon request of the student, student data that is stored. CCSD may expunge medical records and behavioral test assessments. 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 of separation.
- D. Personnel records shall comply with the active retention schedules on file with the Utah Division of Archive and Record Services for Cache County School District.

#### **Expungement Request**

CCSD shall review requests for records expungement from parents and make a determination based on the following procedure:

- A. The following records may not be expunged: grades, transcripts, a record of the student's enrollment, assessment information.
- B. The procedure for expungement shall match the record amendment procedure found in 34 CFR 99, Subpart C of FERPA.
  - a. 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.
  - b. The LEA shall decide whether to expunge the data within a reasonable time after the request.
  - c. If the LEA decides not to expunge the record, they will inform the parent of their decision as well as the right to an appeal hearing.
  - d. The LEA shall hold the hearing within a reasonable time after receiving the request for a hearing.
  - e. The LEA shall provide the parent notice of the date, time, and place in advance of the hearing.
  - f. The hearing shall be conducted by any individual who does not have a direct interest in the outcome of the hearing.
  - g. The LEA shall give the parent a full and fair opportunity to present relevant evidence. At the parents' expense and choice, they may be represented by an individual of their choice, including an attorney.
  - h. The LEA shall make its decision in writing within a reasonable time following the hearing.



## **Cache County School District**

### **Policy Series 6000: Finance and Operations**

- i. The decision must be based exclusively on evidence presented at the hearing and include a summary of the evidence and reasons for the decision.
- j. If the decision is to expunge the record, the LEA will seal it or make it otherwise unavailable to other staff and educators.

#### **Data Transparency**

Annually, the CCSD will publicly post:

- A. CCSD data collections
- B. Metadata Dictionary as described in Utah's Student Data Protection Act (SDPA), U.C.A §53E-9-301

Approved by District Administration: May 15, 2025