21st Century Community Learning Centers Grant Data Confidentiality & Security Fact Sheet

CDE's Data Confidentiality and Security Policy

Educational data is essential to CDE's mission to ensure that all students are prepared for success in society, work, and life. The CDE 21st CCLC program is responsible for activities that require the collection of Colorado student data, which helps CDE to report on 21st CCLC program participation and evaluation and to fulfill federal reporting requirements. The Colorado Department of Education's (CDE) 21st Century Community Learning Centers (21st CCLC) team is required by Title IV, Part B of the ESEA, as amended by the Every Student Succeeds Act (ESSA) (20 U.S.C. 7171-7176) to collect and store student information.

CDE holds data confidentiality and security practices in the highest regard and CDE's 21st CCLC program team takes its obligation to protect the privacy of students' Personally Identifiable Information (PII) seriously. Therefore, CDE provides a secure, online system known as EZReports to collect and report PII for this grant program. PII will be collected, used, shared, and stored in compliance with applicable laws and CDE's privacy and security policies and procedures. Aggregated information reported to CDE in relation to grant activities is not confidential and is subject to public request.

CDE has adopted the following policy to protect student data that is collected, used, and stored by CDE.

Student Personally Identifiable Information (PII)

Student Personally Identifiable Information (PII) includes, but is not limited to, information that is collected, maintained, generated, or inferred and that, alone or in combination, personally identifies an individual student or the student's parent(s) or family. PII, as defined by federal law, also includes other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

State and federal regulations require 21st CCLC subgrantees to partner with schools and districts to submit the following demographic data for all students who participate in 21st CCLC programming within a program year for four hours or more:

- State Assigned Student ID (SASID)
- First and last name
- Date of birth
- Race/ethnicity
- Sex
- Economically Disadvantaged
- English Language Learner
- Special Education (IEP or 504 plan)
- Homeless
- Foster Care
- Migrant

In addition, CDE's 21st CCLC subgrantees are required to report the following outcome data for specific subgroups of students who participate in programming within a program year for four hours or more:

CDE uses SASIDs to access this data internally:	**Subgrantees report this data directly to CDE:**
• Colorado Measures of Academic Success English Language Arts and Math results (prior and current year) for participating students in grades 4-8. • Attendance is measured by comparing current and previous year attendance rates for participating students in grades 1-12 who had a school day attendance rate at or below 90% in the prior school year. • In-school suspension rates (prior and current year) for participating students in Grades 1-12 who had at least one in-school suspension in the previous school year.	• Grade Point Averages (prior and current year) for participating students in grades 7-8 and 10-12 with a prior year GPA of less than 3.0 in the previous school year.

CDE recognizes that student education records are official and confidential documents are protected by the Family Educational Rights and Privacy Act (FERPA), the Colorado Student Data Transparency and Security Act, and other state and federal laws. With the increasing use of technology in education, CDE believes it is imperative that information that identifies individual students and their families is protected from misappropriation and misuse.

CDE Employees' Internal Use of PII

PII is only available to CDE employees who have a reasonable and appropriate educational purpose to receive that information. For 21st CCLC, there are several CDE employees that serve as 21st CCLC state administrators who have access to student PII in CDE's 21st CCLC secure data management system called EZReports. The 21st CCLC staff who have access to student PII within the EZReports system adhere to all data security and privacy requirements.

CDE's 21st CCLC program staff hold EZReports administrator roles and can securely view and access student PII for the sake of assisting subgrantees and reporting aggregate data to the USDE. 21st CCLC program staff hold EZReports administrator roles and can securely view and access student PII for the sake of assisting subgrantees and reporting aggregate data to the USDE.

CDE's Data Management Committee includes data owners and coordinators at CDE who help ensure that PII is properly handled from collection to reporting. This committee assists in reviewing and approving the CDE employees who have a legitimate need for access to PII. For more information, see CDE's Data Governance webpage.

Disclosure of Student PII for Limited Purposes

CDE may release student PII only to outside entities or individuals that have a legitimate educational purpose for receiving this information. For example, CDE only shares student-level data with a contracted external evaluator, who completes an attestation for data privacy and security. In compliance with state and federal laws, CDE's 21st CCLC team limits access to student PII to the following:

- Authorized CDE staff that require access to perform assigned duties: CDE's 21st CCLC program shares student PII data with CDE's Information Management Services team to access K-12th grade students' school day attendance data, in-school suspension data, and the Accountability Analytics Office to access 4th-8th grade students' Colorado Measures of Academic Success (CMAS) English Language Arts (ELA) and Math scores for federal reporting purposes.
- CDE contractors that require access to perform assigned or contractual duties as stated in the contract. As mentioned above, CDE's 21st CCLC team only shares student-level data with a contracted external evaluator, who completes an attestation for data privacy and security.
- Vendors, third parties, and other service providers that provide or service databases, assessments, or instructional supports as permitted by law and defined by contractual agreements. CDE's 21st CCLC program currently contracts with EZReports, a web-based data management software, to collect and report outcome data to the U.S. Department of Education.
- Authorized representatives of CDE in connection with an audit or evaluation of federal- or state-supported education programs, or for the enforcement of or compliance with federal legal requirements that relate to those programs.

Additionally, students and/or their parents or legal guardians are allowed access to the student's PII in accordance with state and federal law.

CDE's Data Security Policies and Practices

CDE requires that devices storing sensitive information, even for a limited duration, must be encrypted in compliance with all applicable Colorado Information Security Policies and Office of Information Technology (OIT) Technical Standards as posted on OIT's public website at oit.colorado.gov. CDE monitors all access and access attempts to all of its data systems and maintains a centralized authentication and authorization process to further track access and safeguard data.

CDE employees must abide by the following security protocols.

- Employees must not disable or circumvent any aspects of CDE's security controls.
- Employees must use secure methods when sharing or transmitting PII externally or internally. The 21st CCLC program uses EZReports to collect, validate and report data and Syncplicity for internal and external data sharing.
- Employees must only use password-protected state-authorized devices when collecting, viewing, or using personally identifiable information (PII).

- Employees must not share employee passwords with anyone.
- Employees must log out of any data system/portal and close the browser after each use.
- Employees must store PII on appropriate secured locations. 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 PII.
- Employees must keep printed reports with PII in a locked location while unattended and shall use the secure document destruction service provided at CDE when disposing of such records.
- Employees must store files containing PII only on secured servers or personal folders accessible only by parties who have specifically been authorized by the data owner.
- Employees must not use email to send screenshots, text, or attachments that contain PII. If employees receive an email containing PII, they must delete the screenshots/text when forwarding or replying to these messages and report this to the CDE's Information Security Officer.
- Upon separation, employees must relinquish all confidential data and CDE equipment.

All language in this document is adapted from official CDE data confidentiality and security policy and highlights information that aligns to the 21st CCLC policy. Please see CDE's department-wide policy language and CDE's Data Confidentiality and Security Policy for further reference.