COLORADO
Department of Education

Susana Córdova, Commissioner of Education
201 E. Colfax Ave., Denver, CO 80203-1799
June 18, 2025

Data Confidentiality and Security Policy

The Colorado Department of Education (CDE) holds data confidentiality and security practices in the highest regard. The Colorado Universal Policy on Confidentiality and Non-Disclosure concerns the protection of certain confidential information and applies to all classified employees and volunteers of state government. CDE adopts this universal policy for all CDE employees, including non-classified employees. In addition, all CDE employees must adhere to all federal and state data privacy and confidentiality laws, as well as the following practices and procedures, based on the unique work of the department and access to student and educator information.

Student Personally Identifiable Information

Student education records are official and confidential documents protected by the Family Educational Rights and Privacy Act (FERPA), the Colorado Student Data Transparency and Security Act, and other state and federal laws. Employees must not collect, use, or share students' personally identifiable information (PII) beyond the purposes necessary to carry out official job responsibilities.

Per state law, student PII means information that, alone or in combination, personally identifies an individual student or the student's parent or family, and that is collected, maintained, generated, or inferred by a public education entity. (Section 22-16-103(13), C.R.S.) As defined by federal law, student PII 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. (34 CFR §99.3.)

"In combination" refers to when information from different sources can be compared or synthesized to generate new information. For example, a reader might be able to combine a CDE-generated demographics report with certain information suppressed or withheld in order to protect the identity of individuals with a news article celebrating and naming a 10th grade, female, American Indian student, in the one high school in a rural school district who received a prestigious scholastic award. Hence, the reader can identify suppressed information in the CDE-generated report. When analyzing what types of combined information may be considered PII, the department uses the "reasonable person" standard (i.e., what could be determined by a hypothetical, rational, prudent, average individual).

Some examples of student PII collected by CDE include, but are not limited to, the following:

- A student's name*;
- A personal identifier such as a student ID number*;
- Other indirect identifiers such as a student's date of birth;
- Records regarding a student's primary disability;
- A student's socioeconomic information;

- Photos, videos, and voice recordings;
- State-administered assessment demographic, test administration (participation, accommodations used, etc.) and results information, including growth information;
- Information about courses taken and completed, credits earned, course grades, and other transcript information;
- Grade level and anticipated graduation year;
- Degree, diploma credential attainment or other school exit information;
- Attendance and mobility information between and within Colorado school districts;
- Special education data and special education discipline reports; and
- Program participation information required by state or federal law.

*Removal of student's name and masking of personal identifiers does not necessarily make the associated data non-PII.

Educator Personally Identifiable Information

Educator PII includes, but is not limited to: the educator's name, any unique identifier, including social security number, and other information that, alone or in combination, is linked or linkable to a specific educator.

Employees' Internal Use of PII

PII is only available to employees who have a reasonable and appropriate educational purpose to receive that information. The Department's Data Collection Leads and Unit PII Reviewers will review and approve the CDE employees who have a legitimate need for access to PII.

Disclosure of Aggregated Non-PII Data

External requests for aggregated, non-PII data must be submitted through the process outlined on CDE's Data Request page. CDE's Data Sharing and Research Manager will facilitate the process and support efforts to ensure data does not reveal PII.

Disclosure of Student PII for Limited Purposes

CDE may only release student PII to outside entities or individuals that have a legitimate educational purpose for receiving this information. In compliance with state and federal laws, CDE limits access to student PII to the following:

- Authorized staff of the Department that require access to perform assigned duties;
- Department contractors that require access to perform assigned or contractual duties as stated in the contract;
- School district administrators, teachers, and school personnel who require access to perform assigned duties;

- Authorized staff of other state agencies, including public institutions of higher education, as required by law and defined by interagency agreements;
- Entities conducting research on behalf of the Department to develop, validate, or administer tests, administer financial aid programs or improve instruction, as permitted by law and defined by contract or agreements;
- 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; and
- 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.

Disclosure of Educator PII for Limited Purposes

Per state law, CDE may collect information concerning an individual educator's performance evaluation ratings and student assessments results linked to the educator in order to fulfill its duties as required by law, but this information must remain confidential and may not be published in any way that would identify the individual educator. (Section 22-9-109, C.R.S.) The State Board of Education's rules concerning the evaluation of licensed personnel (1 CCR 301-87), in section 6.014(B), further clarify that CDE shall only publicly report data related to performance evaluation ratings in the aggregate at the school-, district-, and state-level, and shall not publicly report this data for cohorts smaller than five educators.

Additionally, as required by section 22-2-111, C.R.S., all papers filed at CDE that contain personal information about holders of educator licenses or authorizations are classified as confidential. The department will not disclose this information unless required by law. Educators may challenge the information in their record by formal letter or other evidence, which must be added to CDE's records.

Disclosure of PII for Research Purposes

CDE has developed a process to consider and review all outside requests for PII or de-identified individual-level data by individuals who seek to conduct research. This process is detailed on CDE's Data Request page. Potential users such as doctoral and master's degree candidates, university faculty, independent researchers, and private and public agencies must submit research requests before receiving PII or de-identified individual level data to conduct and/or publish their research.

The requestor must meet all of CDE's criteria prior to submitting the request for PII. This includes gaining Institutional Review Board (IRB) approval, if required given the scope of the research or data request. CDE will conduct an extensive internal review of the research request. Should CDE program staff and data owners approve the research request, student PII requests will be provided to the State Board of Education for approval.

Once fully approved, CDE and the researcher will enter into a research data sharing agreement for PII that includes the requirements listed below. Approval to use the PII or de-identified individual-level data for one study, audit, or evaluation does not confer approval to use it for another. CDE has the right to review any data/results for approved PII research requests prior to publication to verify that proper disclosure avoidance techniques have been used. CDE also has the right to approve reports prior to publication to ensure they reflect the original intent of the agreement.

Agreements and Contracts for Disclosure of PII

Prior to sharing PII, the Department must enter into a written agreement or contract that meets the following requirements:

- Designates the individual or entity that will serve as the authorized representative or primary individual responsible for protecting and managing PII;
- Specifies the purpose and scope of the contract or agreement;
- Specifies the duration of the contract or agreement;
- Specifies the types of PII that are collected, used, or maintained under the contract or agreement;
- Specifies the uses of PII under the contract or agreement; and
- Specifies the length of time that PII can be held.

In addition to all of the information addressed above, any agreement or contract shall also include the following assurances to protect PII from further disclosure and unauthorized use:

- The third party may use PII only to meet the purpose stated in the written agreement and not for further disclosure, unless authorized;
- The entity or individual must have a training program to teach its employees about how to protect PII;
- CDE shall maintain the right to conduct audits or other monitoring activities of the entity or individual's policies, procedures, and systems; and
- CDE shall verify that the entity or individual has a comprehensive information security program to protect all PII. This includes requirements stating how to respond to any breach in security, including the requirement that any breach in security must be reported immediately to CDE.

Prior to sharing PII for research purposes, the Department must enter into a written agreement or contract that meets the requirements outlined above. In addition, the agreements must include the following:

- The research methodology and the rationale for why disclosure of PII is necessary to accomplish the research;
- The requirement that the researcher conduct the study in a manner that does not permit the personal identification of educators or students by anyone other than authorized persons of the authorized organization with legitimate interests;
- The assurance that the researcher will maintain the confidentiality of PII at all stages of the study, including within the final report, by using appropriate disclosure avoidance techniques; and
- The requirement that the authorized representative destroy the PII at the conclusion of the research according to a specific time period for destruction stated in the agreement.

Failure to Comply with Agreement or Contracts

An individual may file a written complaint with CDE regarding an alleged violation of an agreement or contract. A complaint must contain specific allegations of fact that give reasonable cause to believe that a violation of a data sharing agreement or contract has occurred. CDE will investigate all reasonable and timely complaints. The investigation will be conducted in an impartial manner and by individuals with appropriate training and expertise.

CDE may also conduct its own investigation when no complaint has been filed or when a complaint has been withdrawn to determine whether or not a violation has occurred.

Should CDE determine that an outside individual or entity has committed a material breach of the contract that results in the misuse or unauthorized release of PII, CDE will determine whether to terminate the contract in accordance with a policy adopted by the State Board of Education. At a minimum, the policy must require the State Board to hold a public meeting that includes the discussion of the nature of the material breach. The State Board must determine whether to direct CDE to terminate or continue the contract. In addition, CDE may deny the individual or entity further access to personally identifiable data for at least five years or CDE may pursue penalties permitted under state contract law, such as liquidated damages.

Data Retention and Disposition

The data that CDE collects is maintained according to the retention and disposition schedules outlined by the Colorado State Archives in its State Agency Records Management Manual or in the Records Management Manual for School Districts. For information defined as "Student Permanent Record" (i.e., demographics, enrollment and academic performance data), CDE archives this information and protects it with appropriate technical, physical, and administrative safeguards in accordance with state and federal law.

Data Security Practices

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.

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 approved method is CDE's Secure File Transfer Protocol (SFTP) website or Syncplicity or via secured server folders for internal data sharing.
- Employees must only use password-protected state-authorized devices when collecting, viewing, or using 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, Corey Kispert, at dataprivacy@cde.state.co.us.

- Upon separation, employees must relinquish all confidential data and CDE equipment.

Staff Training

In order to minimize the risk of human error and misuse of information, CDE provides a range of training for all staff on data security.

Employees are required to participate in an annual information security and privacy fundamentals training, which is mandatory for continued access to the Department's network.

Additionally, CDE offers targeted information security training for specific groups within the agency. CDE also provides training and guidance to Local Education Agencies (LEAs) concerning compliance with state and federal data privacy laws and best practices.

Breaches in Data Security

If employees are targeted and victimized by a phishing email or other password compromise, those instances must be reported immediately to the help desk for remediation.

Employees and contractors must report any possible data security incidents or breaches immediately to the Department's Information Security Officer, Corey Kispert, at dataprivacy@cde.state.co.us or 720-258-6496. Incidents or breaches include, but are not limited to: (i) successful attempts to gain unauthorized access to a State system or PII regardless of where such information is located; (ii) unwanted disruption or denial of service; (iii) the unauthorized use of a Department system for the processing or storage of data; (iv) changes to Department system hardware, firmware, or software characteristics without the Department's knowledge, instruction, or consent; or (v) a breach in a contract that results in the misuse or unauthorized access to PII.

If the Information Security Officer or Chief Information Officer, in collaboration with the Commissioner and appropriate CDE leadership, determine that one or more employees or contracted partners have substantially failed to comply with the Department's information security and privacy policies, they will, in coordination with Human Resources, identify appropriate consequences, which may include disciplinary action, up to and including termination of employment or termination of a contract as well as further legal action.

Concerns about security breaches brought to CDE's Chief Information Officer or Information Security Officer must be reported immediately to the Commissioner. The Commissioner will collaborate with appropriate CDE leadership and Human Resources to determine what has occurred and will identify appropriate consequences, which may include disciplinary action, up to and including termination of employment or a termination of a contract. The investigation of potential security breaches will be conducted in an impartial manner and by individuals with appropriate training and expertise.

Process for Maintaining this Policy

CDE regularly monitors changes in state and federal law related to data security. This policy is updated, as needed, to incorporate any new requirements and best practices.

Employee Acknowledgment

All CDE employees must sign an acknowledgment form for this Data Confidentiality and Security Policy upon hire and on an annual basis thereafter.

Contact Information

Questions about data confidentiality may be directed to the following individuals:

- Melissa Peterson, Data Privacy Manager, Peterson_M@cde.state.co.us
- Marcia Bohannon, Chief Information Officer, Bohannon_M@cde.state.co.us
- Corey Kispert, Information Security Officer, Kispert_C@cde.state.co.us