



## **Data Privacy**

### **Overview**

Data privacy is a critical component of Colorado Early Colleges' (CEC) operations. The protection and management of the various types of student and staff Personally Identifiable Information (PII) is critical to CEC operations. CEC computer systems and related devices collect and record data as required for educational delivery, management, and reporting purposes. This key information should never be disclosed to unauthorized individuals.

### **General Statement of Student Data Privacy**

CEC policy surrounding data privacy falls into three broad classifications protecting information gathered to manage and deliver services to employees, students, and districts. This policy is broken into three separate sections – general network data, PII, and employee information.

Using data effectively and responsibly is foundational to making the best decisions in today's schools about improving student performance. The Family Educational Rights Privacy Act (FERPA), Colorado's Student Data Transparency and Security Act, and other state or federal laws establish baseline parameters for what is permissible when sharing student PII.

Capturing accurate information is necessary for public, state, and federal reporting. Data is also needed to create accurate school and district performance reports. Per state and federal laws, the Colorado Department of Education (CDE) is required and/or permitted to gather data from Local Education Providers. This policy does not restrict the transfers of data to CDE, provided that laws do not prohibit such transfers.

CEC uses additional guidelines and strict processes to protect the privacy of every student and ensure the confidentiality and security of all PII collected and managed.

### **General Network Data**

In the course of normal network operations, computer systems, voice systems, access control systems, and network devices generate and track logging data, source and destination internet protocol (IP) addresses, session times, port numbers, file sizes, etc. (referenced as Network Data).

- Network Data Policy - CEC treats all network data as confidential information. This information may be obtained, stored, and reported for legitimate business, compliance and audit purposes but shall not be exposed to unauthorized individuals except as specifically discussed in this policy. Network data may be disclosed under the following conditions. Requests shall be authorized by the Executive Director of Operations, or their designee:
- Network Operational Viability - Network data may be released under the following situations:

- Network performance monitoring or troubleshooting.
  - Security incident analysis and remediation.
  - Audit, group policy, and security log management and analysis.
  - Litigation holds and requests.
  - Copying, archiving, or otherwise preserving portions of any messages transmitted over the network in the course of business or maintenance.
- Legal or CEC Policy Analysis – Network data may be released to appropriate authorities to indicate the presence of activities that violate internal policies, federal or state law. These requests shall be in response to legal discovery or court requests.
  - Network Security Threats – All relevant data, protocol, logs, and user information may be released as part of incident and breach analysis and remediation. CEC shall investigate and remediate possible network security threats by means of capturing, logging and examination of files, communications, and other traffic and transmissions over or on the network.
  - Network Data Requests - All requests to retrieve and share network data must be submitted to the Executive Office Administrator, or their designee. Any litigation and legal requests require confirmation by both CEC's Chief Executive Administrator (CEA) and CEC attorney. Such requests shall include:
    - Name and role of the requestor.
    - Reason for the request, in accordance with the principles set forth in this policy.
    - Intended use of the requested data.
    - Any network data intentionally shared with third parties must be sanitized and redacted to preserve the anonymity of network users unless that data is used directly in legal discovery or authorized by CEC counsel and the Executive Director of Operations. Requests shall be documented and stored as part of the implementation of this policy.

## Employee Data

All employee data is treated as confidential and private. No employee related information shall be released or disclosed without the express approval of CEC's CEA, or designee.

Employee Data Policy – CEC treats all employee data as private and confidential information. This information may be obtained, stored, and reviewed for legitimate business purposes related to personnel employment, compliance, and audit purposes but shall not be exposed to unauthorized individuals, agencies, or external sources except as specifically discussed in this policy.

Requests shall be authorized by the CEA or designee. Data shall be disclosed only under the following conditions and employees shall be informed of such activity prior to release:

- Employee Performance or Transitions – Employee work data may be released under the following situations:
  - Security incident analysis and remediation.
  - Litigation holds and requests.
  - Personnel transitions involving email and work products.
  - Restoration or otherwise preserving portions of messages transmitted over the network in the course of business.
- Legal or Agency Disciplinary Analysis – Employee data may be released to appropriate authorities to indicate the presence of activities that violate internal policies, federal or state law. These requests shall be in response to internal policy incidents, personnel management, legal discovery, or court requests.
- Network or Agency Security Threats – All relevant data, protocol, logs, and user information may be released as part of incident and breach analysis and remediation. CEC shall investigate and remediate possible network security threats by means of capture, logging and

examination of files, communications, and other traffic and transmissions over or on the network, including all employee communications and component activities relevant to the incident or breach.

- Employee Data Requests - All requests to retrieve and share employee data must be submitted according to Policy. Any litigation and legal requests shall include:
  - Name and role of the requestor.
  - Reason for the request, in accordance with the principles set forth in this policy.
  - Intended use of the requested data and whether this information will be used as part of a personnel action.
  - Employee notification of the event unless barred due to legal or disciplinary investigation. In all circumstances, employees shall be notified if information is placed in their permanent files related to an incident or discovery request.

Any employee network data intentionally shared with third parties shall be sanitized and redacted to preserve the anonymity of the employee unless that data is used directly in legal discovery or authorized by CEC Counsel. Requests shall be documented and stored as part of the implementation of this policy.

## **Student Personally Identifiable Information (PII)**

All student PII and is confidential and private. CEC student data privacy procedures adhere to the guidelines set forth in applicable federal and state law, and includes additional safeguards as follows:

- Formal information security policy.
- Security and privacy policies.
- Policy review and revision by national experts and advisors.
- Institutional Review Board (IRB) or a formal process to review and approve research requests to ensure appropriateness and confidentiality of the research.
- Specific liability language and support in vendor contracts/agreements around student data privacy, data breaches, appropriate uses and disclosure of student data, and termination/penalties for non-compliance.
- Annual independent security audits.
- All PII releases shall fall under the Student Data Policy.

Student Data- CEC treats all student PII as private and confidential information. This information may be obtained, stored, and reviewed for legitimate educational purposes related to student achievement, accounting, pupil services, operations, compliance and audit purposes but shall not be exposed to unauthorized individuals, agencies or external sources except as specifically discussed in this policy.

Student data may only be collected and utilized when meeting the express educational needs of the student and as mandated by state and federal law. It shall not be disclosed to any party unless they are designated as the data owner (parent or student beyond the age of majority), an identified "School Official" or an "Authorized Representative" pursuant to federal FERPA guidelines acting in the best interests of the student's education. All record release requests shall be authorized by the CEA, or designee. PII shall be disclosed only under the following conditions and employees shall be informed of such activity prior to release:

- Disaggregated Individual Student Data, including, but not limited to:
  - Allocation of state education funding
  - Administering state assessments
  - Calculating individual student growth
  - Colorado post-secondary enrollment and remediation feedback
- Aggregated (Summary and De-Identified) Student Data, including, but not limited to:
  - School and District Performance Reports
  - Program evaluation and measurement
  - School and District Improvement Plans

- Federal reporting/funding
- Public reporting

Legal or CEC Disciplinary Analysis – Student PII may be released to appropriate authorities to indicate the presence of activities that violate LEP policies or federal/state law. These requests shall be in response to documented policy incidents, legal discovery, or judiciary requests.

Network Security Threats – All relevant data, protocol, logs, and student information may be released as part of incident and breach analysis and remediation. CEC shall investigate and remediate possible network security threats by means of capture, logging and examination of files, communications, and other traffic and transmissions over or on the network, including all student communications and component network activities relevant to the incident or breach.

Student Data Requests - All requests to retrieve and share student data must be submitted under the Rights Concerning Student Records policy.

## **Audit Controls and Management**

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of CEC operations. Examples of audit control and evidence include:

- Process, authorizations, and documentation for PII requests.
- Historical evidence or organizational compliance.
- Functioning IRB and research authorization process and regular evidence of board activity.
- Procedures for executing legal holds, chain of command, and discovery requests.

## **Enforcement**

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.