



## SECTION J: Students

### JRC-G Privacy and Protection of Confidential Student Information

Effective:

2/16/2018

## JRC-G Privacy and Protection of Confidential Student Information

The Colorado Early Colleges Network is committed to protecting the confidentiality of student information obtained, created and/or maintained by the network. Student privacy and the network's use of confidential student information are protected by federal and state law, including the Family Educational Rights and Privacy Act (FERPA) and the Student Data Transparency and Security Act (the Act). CEC will manage its student data privacy, protection and security obligations in accordance with this policy and applicable law.

### Definitions

"Student education records" are those records that relate directly to a student. Student education records may contain, but not necessarily be limited to, the following information: identifying data; academic work completed; level of achievement (grades, standardized achievement test scores); attendance data; scores on standardized intelligence, aptitude and psychological tests; interest inventory results; health and medical information; family background information; teacher or counselor ratings and observations; reports of serious or recurrent behavior patterns; and any Individualized Education Program (IEP).

"*Student personally identifiable information*" or "*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 the CEC Network, either directly or through a school service, or by a school service contract provider or school service on-demand provider.

"*Security breach*" means the unauthorized disclosure of student education records or student PII by a third party.

The following terms used in this policy shall be as defined by the Act: "school service," "school service contract provider" and "school service on-demand provider."

### Directory Information

(The term “directory information” is used for the portion of the education record that, if disclosed, would not generally be considered harmful or an invasion of privacy (34 CFR § 99.3). This may include the student’s name, address, telephone number, date and place of birth, honors and awards, and dates of attendance.)

School systems that disclose directory information must give “public notice” of this policy and explain what is included in such information. The notice must also indicate that parents may refuse to allow the school to designate any, or all, of their child’s record as directory information

### **Access, Collection and Sharing Within the CEC Network.**

CEC shall follow applicable law and CEC Network policy in the access to, collection and sharing of student education records.

CEC Network staff members shall ensure that confidential information in student education records is disclosed within the network only to officials who have a legitimate educational interest, in accordance with applicable law and CEC policy.

Appropriate CEC Network staff members shall be required to sign and comply with the network’s agreement (***JRC-R Privacy and Protection of Confidential Student Information Acknowledgement Form***) concerning the protection of confidential student information, which describes the appropriate uses and safeguarding of student education records.

### **Contract Providers, On-Demand Providers, or other Third Parties**

CEC Network staff members shall ensure that student education records are disclosed to persons and organizations outside the network only as authorized by applicable law and CEC policy. The term “organizations outside the network” includes school service on-demand providers and school service contract providers. Acquisition and use of any third-party apps and services that use student data in any capacity must be pre-approved by CEC. Staff must follow the procedure to secure approval before using the contract provider or on demand provider. CEC will identify specific programs or apps that are approved for school and teacher use and make that list available in the CEC Website. CEC will make copies of this policy upon request to the parent of an enrolled student; and will post the policy on its website.

Any contract between the CEC Network and a school service contract provider shall include the provisions required by the Act, including provisions that require the school service contract provider to safeguard the privacy and security of student PII and impose penalties on the school service contract provider for noncompliance with the contract.

In accordance with the Act, the CEC Network shall post the following on its website:

- a) a list of the school service contract providers that it contracts with and a copy of each contract; and
- b) clear explanation of the student PII CEC collects
- c) to the extent practicable, a list of the school service on-demand providers that the network uses.
- d) Privacy and security standards
- e) CDE data inventory index
- f) The security of student education records maintained by the network is a high priority.
- g) Security breach or other unauthorized disclosure

Staff members who disclose student education records in a manner inconsistent with applicable law and CEC policy may be subject to disciplinary action, up to and including termination from employment. Any discipline imposed shall be in accordance with applicable law and CEC policy.

Employee concerns about a possible security breach shall be reported immediately to the Head of School/CEC Administrator. If the School/CEC Administrator is the person alleged to be responsible for the security breach, the staff member shall report the concern to the Governing Board.

When the network determines that a school service contract provider has committed a material breach of its contract with the network, and that such material breach involves the misuse or unauthorized release of student PII, the network shall follow this policy's accompanying regulation in addressing the material breach. CEC will not enter into or renew a contract with a service contract provider or on-demand provider that refuses to abide by the required contract terms/requirements

Nothing in this policy or its accompanying regulation shall prohibit or restrict the network from terminating its contract with the school service contract provider, as deemed appropriate by the network and in accordance with the contract and the Act.

### **Data Retention and Destruction**

The CEC Network shall retain and destroy student education records in accordance with applicable law and network approved procedures.

### **Staff Training**

The CEC Network shall provide periodic in-service trainings to appropriate staff members to inform them of their obligations under applicable law and CEC policy concerning the confidentiality of student education records.

### **Parent/Guardian Complaints**

In accordance with this policy's accompanying regulation, a parent/guardian of a CEC Network student may file a written complaint with the Head of School/CEC Administrator if the parent/guardian believes the network has failed to comply with the Act.

### **Parent/Guardian Requests to View and/or Amend Student Education Records**

Parents have right to inspect/review Student PII; request corrections to Student PII; right to request paper or electronic copy of Student PII, including that which is maintained by any service contract provider.

Parent/guardian requests to amend his or her child's education records shall be in accordance with the CEC Network's procedures governing access to and amendment of student education records under FERPA, applicable state law and CEC policy.

### **Oversight and Review**

The Operations Manager and each Head of School or designee shall be responsible for ensuring compliance with this policy and its required privacy and security standards.

The Operations Manager and each Head of School or designee shall annually review this policy and accompanying regulation to ensure it remains current and adequate to protect the confidentiality of student education records in light of advances in data technology and dissemination. The Operations Manager shall recommend revisions of this policy and/or accompanying regulation as deemed appropriate or necessary to the CEC Governing Board. The CEC Governing Board will review this policy annually and make revisions as necessary to stay current and adequately protect Student PII in light of advancements in technology during the August Board meeting.

### **Compliance with Governing Law and Governing Board Policy**

The CEC Network shall comply with FERPA and its regulations, the Act, and other state and federal laws governing the confidentiality of student education records. The network shall be entitled to take all actions and exercise all options authorized under the law.

In the event this policy or accompanying regulation does not address a provision in applicable state or federal law, or is inconsistent with or in conflict with applicable state or federal law, the provisions of applicable state or federal law shall control.

### **Photographs and Media Release**

Students may occasionally appear in photographs and videos taken by CEC staff members, other students, or other individuals authorized by the Head of School or other CEC staff member. CEC may use these pictures, without identifying the student, in various publications, including but not limited to, the school yearbook, social media, school newspaper, and school website. No consent or notice is needed or will be given before CEC uses pictures of unnamed students taken while they are at school or a school-related activity.

Many times, however, CEC will want to identify a student in a school picture. CEC staff may want to acknowledge those students who participate in a school activity or deserve special recognition. In order for CEC to publish a picture with a student identified by name in any school-sponsored material, including yearbook, one of the student's parents or guardians must sign a consent form. Granting consent allows the CEC School to publish and otherwise use photographs and videos, with the child identified, while he or she is enrolled in a CEC school. This consent is valid for one year and may be revoked at any time by notifying the student's Head of School.

FERPA is not the only statute that limits what providers can do with student information. The Protection of Pupil Rights Amendment (PPRA) provides parents with certain rights with regard to some marketing activities in schools. Specifically, PPRA requires that a school district must, with exceptions, directly notify parents of students who are scheduled to participate in activities involving the collection, disclosure, or use of personal information collected from students for marketing purposes, or to sell or otherwise provide that information to others for marketing purposes, and to give parents the opportunity to opt-out of these activities. While FERPA protects PII from education records maintained by a school or district, PPRA is invoked when personal information is collected from the student.

## **Hearing and Complaint Procedures**

### **Contract Breach by School Service Contract Provider**

Within a reasonable amount of time after the CEC Network determines that a service contract provider or on-demand provider has committed a material breach of its contract/agreement with the network, and that such material breach involves the misuse or unauthorized release of student personally identifiable information (PII), the CEC Governing Board shall make a decision regarding whether to terminate the network's contract with the service contract provider in accordance with the following procedure.

The network shall notify the service contract provider of the basis for its determination that the service contract provider has committed a material breach of the contract and shall inform the service contract provider of the meeting date that the Governing Board plans to discuss the material breach.

Prior to the Board meeting, the service contract provider may submit a written response to the CEC Network regarding the material breach.

The Board shall discuss the nature of the material breach at a regular or special meeting.

At the Board meeting, a network representative shall first be entitled to present testimony or other evidence regarding the network's findings of a material breach. The service contract provider shall then have an opportunity to respond by presenting testimony or other evidence. If the service contract provider is unable to attend the meeting, the CEC Governing Board shall consider any written response that the service contract provider submitted to the network (***Refer to CEC Policy BEA-G Board Meetings***).

If members of the public wish to speak to the Board regarding the material breach, they shall be allowed to do so, in accordance with the Board's policy on public participation at Board meetings.

The Board shall decide whether to terminate the contract with the service contract provider within 30 days of the Board meeting and shall notify the service contract provider of its decision. The Board's decision shall be final.

### **Parent/Guardian Complaints**

In accordance with this policy, the parent/guardian of a CEC Network student may file a written complaint with the Head of School/CEC Administrator or designee if the parent/guardian believes the network has failed to comply with the Student Data Transparency and Security Act (the Act).

The parent/guardian's complaint shall state with specificity each of the Act's requirements that the parent/guardian believes the network has violated and its impact on his or her child.

The Head of School/CEC Administrator or designee shall respond to the parent/guardian's written complaint within 30 calendar days of receiving the complaint.

Within 10 calendar days of receipt of the network's response, the parent/guardian may appeal to the CEC Governing Board. Such appeal must be in writing and submitted to the Head of School/CEC Administrator or designee.

The CEC Governing Board shall review the parent's complaint and the CEC Network's response at a regular or special meeting. A Network representative and the parent/guardian may make brief statements to the Board, but no new evidence or claims may be presented. The Board may choose to conduct the appeal in executive session, to the extent permitted by law.

The Board shall make a determination regarding the parent/guardian's complaint that the network failed to comply with the Act within 60 days of the Board meeting. The decision of the Board shall be final. This procedure shall not apply to parent/guardian concerns with his or her child's education records. If the parent/guardian files a complaint regarding his or her child's education records, the network shall follow its procedures governing access to and review of student education records, in accordance with FERPA, applicable state law and CEC policy.

### **Governing Board Policy**

Nothing contained herein shall be interpreted to confer upon any person the right to a hearing independent of a CEC Board Policy, administrative procedure, statute, rule, regulation or agreement expressly conferring such right. The complaint and hearing procedures described in this regulation shall apply, unless the context otherwise requires and/or unless the requirements of another policy, procedure, statute, rule, regulation or agreement expressly contradicts any of these procedures, in which event the terms of the contrary policy, procedure, law, rule, regulation or agreement shall govern.

#### **Policy Ref:**

*ADD-G Safe Schools*

*BEA-G Board Meetings*

*EBCB-G School Safety Plan*

*GBEE-O Employee Computer, Network & Internet Usage Policy*

*GBK-O CEC Network Grievance Policy*

*JII-O Student Grievance Policy*

*JLC-O Health Record Retention*

*JLF-O Employee Mandatory Reporting*

*JRC-R Privacy and Protection of Confidential Student Information Acknowledgement Form*

*JS-O Student Use of the Internet*

*KDE-G Crisis Management/Communication*

*CEC Student Handbook*

*CEC Employee Handbook*

*CEC Transportation SOP*

#### **Legal Refs.:**

*15 U.S.C. 6501 et seq. (Children's Online Privacy Protection Act)*

*20 U.S.C. 1232g (Family Educational Rights and Privacy Act)*

*20 U.S.C. 1232h (Protection of Pupil Rights Amendment)*

*20 U.S.C. 1415 (IDEIA procedural safeguards, including parent right to access student records)*

*20 U.S.C. 8025 (access to student information by military recruiters)*

*34 C.F.R. 99.1 et seq. (FERPA regulations)*

*34 C.F.R. 300.610 et seq. (IDEIA regulations concerning confidentiality of student education records)*

*C.R.S. 19-1-303 and 304 (records and information sharing under Colorado Children's Code)*

*C.R.S. 22-1-123 (district shall comply with FERPA and federal law on protection of pupil rights)*

*C.R.S. 22-16-101 et seq. (Student Data Transparency and Security Act)*

*C.R.S. 22-16-107 (2)(a) (policy required regarding public hearing to discuss a material breach of contract by school service contract provider)*

*C.R.S. 22-16-107 (4) (policy required regarding student information privacy and protection)*

*C.R.S. 22-16-112 (2)(a) (policy required concerning parent complaints and opportunity for hearing)*

*C.R.S. 24-72-204 (3)(a)(VI) (schools cannot disclose student address and phone number without consent)*

*C.R.S. 24-72-204 (3)(d) (information to military recruiters)*

*C.R.S. 24-72-204 (3)(e)(I) (certain FERPA provisions enacted into Colorado Law)*

*C.R.S. 24-72-204 (3)(e)(II) (disclosure by staff of information gained through personal knowledge or observation)*

*C.R.S. 24-80-101 et seq. (State Archives and Public Records Act)*

*C.R.S. 25.5-1-116 (confidentiality of HCPF records)*