NOTE: *Colorado school districts are required by law to adopt a policy on this subject and the law contains some specific direction as to the content or language. This sample contains the content/language that CASB believes best meets the intent of the law. However, the district should consult with its own legal counsel to determine appropriate language that meets local circumstances and needs.*

Privacy and Protection of Confidential Student Information

The Board is committed to protecting the confidentiality of student information obtained, created and/or maintained by the district. Student privacy and the district'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). The Board directs district staff to 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 district, either directly or through a school service, or by a school service contract provider or school service on-demand provider.

NOTE: The Act's definition of "student PII" as defined above is broader than FERPA's definition of "student PII." The use of the terms "student education records" and "student PII" is purposeful in this policy and reflects the legal obligations imposed upon school districts by the Act and FERPA.

"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."

Access, collection and sharing within the district

The district shall follow applicable law and Board policy in the district's access to, collection and sharing of student education records.

District employees shall ensure that confidential information in student education records is disclosed within the district only to officials who have a legitimate educational interest, in accordance with applicable law and Board policy.

Outsourcing and disclosure to third parties

District employees shall ensure that student education records are disclosed to persons and organizations outside the district only as authorized by applicable law and Board policy. The term "organizations outside the district" includes school service on-demand providers and school service contract providers.

Any contract between the district 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 district shall post the following on its website:

- a list of the school service contract providers that it contracts with and a copy of each contract; and
- to the extent practicable, a list of the school service on-demand providers that the district uses.

Privacy and security standards

The security of student education records maintained by the district is a high priority. The district shall maintain an authentication and authorization process to track and periodically audit the security and safeguarding of student education records.

Security breach or other unauthorized disclosure

Employees who disclose student education records in a manner inconsistent with applicable law and Board 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 Board policy.

Employee concerns about a possible security breach shall be reported immediately to the superintendent. If the superintendent is the person alleged to be responsible for the security breach, the staff member shall report the concern to the Board President.

When the district determines that a school service contract provider has committed a material breach of its contract with the district, and that such material breach involves the misuse or unauthorized release of student PII, the district shall follow this policy's accompanying regulation in addressing the material breach.

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

Data retention and destruction

The district shall retain and destroy student education records in accordance with applicable law and Board policy.

Staff training

The district shall provide periodic in-service trainings to appropriate district employees to inform them of their obligations under applicable law and Board policy concerning the confidentiality of student education records.

NOTE: State law provides that the Colorado Department of Education (CDE) shall provide resources that the district may use in training employees regarding student information security and privacy. C.R.S. 22-16-106 (4). In addition, CDE staff shall provide training related to student information security and privacy at the district's request. Id.

Parent/guardian complaints

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

Parent/guardian requests to amend student education records

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

Oversight, audits and review

The superintendent or designee shall be responsible for ensuring compliance with this policy and its required privacy and security standards.

The district's practices with respect to student data privacy and the implementation of this policy shall be periodically audited by the superintendent or designee.

A privacy and security audit shall be performed by the district on an annual basis. Such audit shall include a review of existing user access to and the security of student education records and student PII.

The superintendent 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 superintendent or designee shall recommend revisions to this policy and/or accompanying regulation as deemed appropriate or necessary.

Compliance with governing law and Board policy

The district shall comply with FERPA and its regulations, the Act, and other state and federal laws governing the confidentiality of student education records. The district 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.

Adopted: November 9, 2017

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)*

CROSS REFS.: BEDH, Public Participation at School Board Meetings
EHB, Records Retention
GBEB, Staff Conduct (and Responsibilities)
GBEE*, Staff Use of the Internet and Electronic Communications
JLDAC, Screening/Testing of Students (and Treatment of Mental Disorders)
JRA/JRC, Student Records/Release of Information on Students
JRCA*, Sharing of Student Records/Information between School District and State Agencies
JS*, Student Use of the Internet and Electronic Communications
KLMA, Relations with Military Recruiters, Postsecondary Institutions and Prospective Employers