Student Information Privacy and Protection

The Board is committed to protecting the confidentiality of student data obtained, created and/or maintained by the district. The Board directs district staff to manage its student data privacy, protection and security obligations in accordance with this policy and applicable law.

The scope of this Board policy is limited to a "school service", as such term is defined in the Colorado Student Data Transparency and Security Act (Act) and this policy.

Definitions

"Local administrator" means the lead administrator for a specific location, department, or area of responsibility such as a school principal, department executive director, or area assistant superintendent.

"School Service" means an internet website, online service, online application, or mobile application that:

a) Is designed and marketed primarily for use in a preschool, elementary school, or secondary school;

b) Is used at the direction of teachers or other employees of a local education provider; and

c) Collects, maintains, or uses student personally identifiable information.

A school service does not include an internet website, online service, online application, or mobile application that is designed and marketed for use by individuals or entities generally, even if it is also marketed to a United States preschool, elementary school or secondary school.

"School service contract provider" or "contract provider" means an entity, other than a public education entity or an institution of higher education, which enters into a formal, negotiated contract with a public education entity to provide a school service.

"School service on-demand provider" or "on-demand provider" means an entity, other than a public education entity, that provides a school service on occasion to a public education entity, subject to agreement by the public education entity, or an employee of the public education entity, to standard, non-negotiable terms and conditions of service established by the providing entity.

"Student personally identifiable information" or "student PII" means information that, alone or in combination, personally identifies an individual student or the student's parent/ guardian 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.

"Security breach" means the unauthorized disclosure of student personally identifiable information by a third party.

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 personally identifiable information.

District employees shall ensure that confidential student personally identifiable information 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 personally identifiable information is disclosed to school service contract providers and school service on-demand providers only as authorized by applicable law and Board policy.

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 personally identifiable information 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.
- A notice to on-demand services providers that, if the district ceases using or refuses to use an on-demand school service provider because the on-demand service provider does not substantially comply with its own privacy policy or does not meet the requirements specified in sections 22-16-109(2), C.R.S. and 22-16-110(1), C.R.S., the district will post on its website the name of the on-demand service provider, with any written response that the on-demand provider may submit. The district will also notify the Colorado Department of Education, which will post on its website the on-demand provider's name and any written response.

Privacy and security standards

The security of student personally identifiable information 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 district-maintained student personally identifiable information.

Security breach or other unauthorized disclosure

Employees who disclose student personally identifiable information 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 local administrator. If the local administrator is the person alleged to be responsible for the security breach, the staff member shall report the concern to the next person in line of responsibility for that specific local administrator (i.e., principal to area assistant superintendent, executive director to superintendent, etc.).

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 personally identifiable information, 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 personally identifiable information 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 personally identifiable information.

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, school service contract provider, or school service on-demand provider has failed to comply with the Act.

Parent/guardian requests to amend student personally identifiable information

Parent/guardian requests to amend his or her child's personally identifiable information 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 chief technology officer, or his/her 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 chief technology officer, or his/her 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 personally identifiable information.

The chief technology officer, or his/her designee, shall annually review this policy and accompanying regulation to ensure it remains current and adequate to protect the confidentiality of student personally identifiable information in light of advances in data technology and dissemination. The chief technology officer, or his/her 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 personally identifiable information. 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: May 24, 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 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