Boulder Valley School District
File: JRCB
Adopted: December 12, 2017
Revised: May 26, 2020

PRIVACY AND PROTECTION OF STUDENT DATA

The Board values accountability and transparency at all levels including ensuring that student data privacy and security are a top priority. The use of data helps guide parents, teachers, schools, districts and state leaders as we work together to improve student achievement so all children graduate ready for college and career. Student data privacy is addressed by federal and state law, including the Family Educational Rights and Privacy Act (FERPA)**.** This Policy addresses the School District's obligations under 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

"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.

"School service contract provider" or "contract provider" means an entity, other than a public education entity or an institution of higher education, that 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.

"Security breach" means the unauthorized disclosure of student PII by a third party.

"Student personally identifiable information" or "student PII" for purposes of this policy only 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.

Outsourcing and disclosure to third parties

District employees shall ensure that student PII is disclosed to persons and organizations outside the district only as authorized by applicable law and Board policy and only to the extent necessary. 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 district shall maintain an authentication and authorization process to track and periodically audit the security and safeguarding of student education records.

Oversight, audits and review

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

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.

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 data 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.

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.

Compliance with governing law and Board policy

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. The district shall be entitled to take all actions and exercise all options authorized under the law.

LEGAL REFS.:

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

CROSS REFS.:

GBEB, Staff Conduct (and Responsibilities)
GBEE, Staff Use of the Internet and Electronic Communications
JO, Student Records
JS, Student Use of the Internet and Electronic Communications

End of File: JRCB