

# **PRIVACY AND PROTECTION OF CONFIDENTIAL STUDENT INFORMATION**

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

The scope of this Governing Council 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.

## **I. Definitions**

(a) "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).

(b) "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 school, either directly or through a school service, or by a school service contract provider or school service on-demand provider.

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

(d) 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."

## **II. Access, Collection, and Sharing Within the School.**

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

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

### **III. Outsourcing and Disclosure to Third Parties**

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

Any contract between the School 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 School 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 school uses.
- A notice to services providers that, if the School ceases using or refuses to use a school service provider because the provider does not substantially comply with its own privacy policy or does not meet the requirements specified in sections Colo. Rev. Stats. §§ 22-16-109(2) and 22-16110(1), the School will post on its website the name of the provider, with any written response that the provider may submit. The School will also notify the Colorado Department of Education.

The School supports certain research studies of benefit to the School and/or education in general. Research proposals are vetted by the School under established criteria, taking into consideration this policy and applicable law.

### **IV. Privacy and security standards**

The School shall maintain an authentication and authorization process to track and periodically audit the security and safeguarding of student education records.

### **V. Security breach or other unauthorized disclosure**

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



Employee concerns about a possible security breach shall be reported immediately to the Principal or his/her designee. If the Principal is the person alleged to be responsible for the security breach, the staff member shall report the concern to the Chairman of the Governing Council.

When the School determines that a school service contract provider has committed a material breach of its contract with the School, and that such material breach involves the misuse or unauthorized release of student PII, the school 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 school from terminating its contract with the school service contract provider, as deemed appropriate by the school and in accordance with the contract and the Act.

#### **VI. Data Retention and Destruction**

The School shall retain and destroy student education records in accordance with applicable law and Council policy.

#### **VII. Staff Training**

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

#### **VIII. Parent/Guardian Complaints**

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

#### **IX. Oversight, Audits and Review**

Building administrators, with the assistance of the School Technology Officer, shall be responsible for ensuring compliance with this policy and its required privacy and security standards.

The School's practices with respect to student data privacy and the implementation of this policy shall be periodically audited by the Principal, General Counsel, or designee.

A privacy and security analysis shall be performed by the School on an annual basis. Such

analysis shall include a review of existing user access to and the security of student education records and student PII.

The Principal 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 education records in light of advances in data technology and dissemination. The Principal shall recommend revisions to this policy and/or accompanying regulation as deemed appropriate or necessary.

## **X. 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.

### **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*)

