AURORA PUBLIC SCHOOLS **APS Code: JRCB**
Adopted October 2017

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.

"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 Chief Information Officer. If the Chief Information Officer is the person alleged to be responsible for the security breach, the staff member shall report the concern to the Chief of Staff.

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.

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

PRIVACY AND PROTECTION OF CONFIDENTIAL STUDENT INFORMATION

FERPA, applicable state law and Board policy.

Oversight, audits and review

The Director of Accountability and Data Reporting shall be responsible for ensuring compliance with this policy and its required privacy and security standards.

The Director of Accountability and Data Reporting 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 Director of Accountability and Data Reporting 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.

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)*

PRIVACY AND PROTECTION OF CONFIDENTIAL STUDENT INFORMATION

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 Board Meetings
EHB, Aurora Public Schools Records Retention and Destruction
JLDAC, Screening/Testing of Students
JRA/JRC, Student Records/Release of Information on Students
JS, Student Use of the Internet and Electronic Communications

PRIVACY AND PROTECTION OF CONFIDENTIAL STUDENT INFORMATION

Contract breach by school service contract provider

Within a reasonable amount of time after 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 Board shall make a decision regarding whether to terminate the district's contract with the school service contract provider in accordance with the following procedure.

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

2. Prior to the Board meeting, the school service contract provider may submit a written response to the district regarding the material breach.

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

4. At the Board meeting, a district representative shall first be entitled to present testimony or other evidence regarding the district's findings of a material breach. The school service contract provider shall then have an opportunity to respond by presenting testimony or other evidence. The Board shall retain the authority to set the amount of time established to present testimony or evidence. If the school service contract provider is unable to attend the meeting, the Board shall consider any written response that the school service contract provider submitted to the district.

5. 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.

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

PRIVACY AND PROTECTION OF CONFIDENTIAL STUDENT INFORMATION

Parent/guardian complaints

In accordance with the accompanying policy, the parent/guardian of a district student may file a written complaint with the Chief of Staff or designee if the parent/guardian believes the district has failed to comply with the Student Data Transparency and Security Act (the Act).

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

2. The Chief of Staff or designee shall respond to the parent/guardian's written complaint within 30 calendar days of receiving the complaint.

3. Within 10 calendar days of receipt of the district's response, the parent/guardian may appeal to the Board. Such appeal must be in writing and submitted to the Chief of Staff or designee.

4. The Board shall review the parent's complaint and the district's response at a regular or special meeting. A district 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.

5. The Board shall make a determination regarding the parent/guardian's complaint that the district failed to comply with the Act within 60 days of the Board meeting. The decision of the Board shall be final.

6. 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 district shall follow its procedures governing access to and review of student education records, in accordance with FERPA, applicable state law and Board policy.

Governing law and Board policy

Nothing contained herein shall be interpreted to confer upon any person the right to a hearing independent of a Board policy, administrative procedure, statute, rule, regulation or agreement expressly conferring such right. The complaint and hearing procedures described in this regulation

PRIVACY AND PROTECTION OF CONFIDENTIAL STUDENT INFORMATION

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.