JRCB - PRIVACY AND PROTECTION OF CONFIDENTIAL STUDENT RECORD INFORMATION

The privacy and protection of confidential student education records and the personally identifiable information contained therein shall be governed by the federal Family Educational Rights and Privacy Act ("FERPA"), the Colorado Student Data Transparency and Security Act (the "Colorado Act"), and by this and other applicable District policies. As used in this policy, personally identifiable information from confidential student education records is referred to as "Confidential PII."

- As used in this policy, "confidential student education records" are records, files, documents and other materials in hard-copy or electronic form that: (1) contain information directly related to a student; (2) are maintained by the District or by a party acting for the District as a "District official" as defined in District Policy JRA/JRC; and (3) do not constitute "directory information" as to the student under District Policy JRA/JRC.

- As used in this policy, "personally identifiable information" is information that, alone or in combination, is linked or linkable to a specific student so as to allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty. Personally identifiable information includes but is not limited to: (1) the student's name; (2) the name of the student's parent or other family members; (3) the address or phone number of the student or student's family; (4) personal identifiers such as the student's social security number, student number or biometric record; or (5) indirect identifiers such as the student's date of birth, place of birth or mother's maiden name.

- As used in this policy, a "third party" is an entity other than the District, or a person who is not employed by the District.

AUTHORIZED ACCESS TO, AND COLLECTION AND SHARING OF, STUDENT PERSONALLY IDENTIFIABLE INFORMATION

Access to Confidential PII, and the collection and sharing of Confidential PII, is only authorized in accordance with governing law and District Policies CL and JRA/JRC.

ELECTRONIC DATA SECURITY STANDARDS

Access to District computers and personal communication devices, to District e-mail and document accounts, and to electronically stored Confidential PII shall be password protected. The executive director of information technology shall prescribe

requirements for password complexity and for the period of time a password may remain in effect before needing to be changed.

E-mail between District accounts shall be encrypted in transmission and at rest. Procedures shall be available to encrypt e-mail in transmission and at rest between District accounts and third-party accounts.

The executive director of operations shall implement practices and procedures to help ensure the security of electronically stored Confidential PII, including but not limited to: (1) controlled building and data center access; and (2) video surveillance monitoring.

The executive director of information technology shall implement practices and procedures to maintain the security of electronically stored Confidential PII, including but not limited to: (1) access logging and monitoring by device and location; (2) intrusion penetration and vulnerability testing; (3) use of automated tools and monitoring procedures to detect, report and remediate system vulnerabilities and breaches; (4) responding to threats and occurrences of unauthorized access, loss, disclosure, modification, disruption or destruction of electronically stored Confidential PII; and (5) notifying affected persons and other appropriate parties of such threats and occurrences.

The executive director of information technology shall administer District Policy EHA, shall take steps to ensure that the use of District information technology by District employees and volunteers is in compliance with District Policy GBEE, and shall take steps to ensure that the use of District information technology by District students is in compliance with District Policy JS.

District employees, volunteers and students shall report to the Information Technology Department all threats and known or suspected occurrences of unauthorized access, loss, disclosure, modification, disruption or destruction of electronically stored Confidential PII.

ELECTRONIC DATA SECURITY AUDITS

The executive director of information technology shall ensure that an audit is conducted at least annually regarding the District's electronic data equipment, software, programs and procedures as they relate to the security of Confidential PII. The executive director of information technology shall prepare a confidential written report of each such audit with findings and recommendations, shall provide a copy of the report to the superintendent, and shall provide additional copies of the report to the Board of Education and/or to other District employees as directed by the superintendent.

DATA RETENTION AND DESTRUCTION

All student education records, including but not limited to confidential student education records, shall be retained for the periods required by governing law and District Policy

EHB. Thereafter, such records are subject to destruction in accordance with governing law and District administrative guidelines and procedures.

DISTRICT STAFF TRAINING

The District shall take measures to periodically educate and train staff members regarding their obligation under governing law and District policies to maintain the privacy and protection of Confidential PII, including but not limited to maintaining the privacy and protection of Confidential PII when using District information technology, online services and mobile applications.

SCHOOL SERVICE CONTRACT PROVIDER MISUSE AND/OR UNAUTHORIZED DISCLOSURE OF CONFIDENTIAL PII

If a "school service contract provider" (as defined by the Colorado Act) commits a material breach of a contract with the District that involves the misuse or unauthorized disclosure of Confidential PII, that contract shall be subject to termination and the school service contract provider may be disqualified from future contracts with the District.

In the event a school service contract provider's contract with the District is terminated and/or the provider is disqualified from future contracts with the District as provided in the immediately preceding paragraph, the provider may file a complaint with the Board of Education and request a hearing pursuant to the procedures in section 6 of Board of Education Policy GP 3.12.

PARENT/GUARDIAN COMPLAINTS REGARDING COMPLIANCE WITH THE COLORADO STUDENT DATA TRANSPARENCY AND SECURITY ACT

The parent/guardian of a current District student may file a written complaint with the superintendent if the parent/guardian believes he/she or the student has been harmed as a result of the District's failure to comply with the requirements of the Colorado Act. The written complaint must be filed within thirty (30) calendar days of the date the parent/guardian first learned of the facts causing him/her to believe that the District failed to comply with the requirements of the Colorado Act.

The written complaint filed by the parent/guardian shall include: (1) the name, home address and telephone number of the parent/guardian and the student; (2) a detailed description of the alleged events supporting the parent's/guardian's belief that the District failed to comply with the requirements of the Colorado Act, including to the extent possible the dates and times the alleged events occurred and the names of the individuals involved, including any witnesses; (3) identification of any District employees involved in the alleged failure of compliance with the requirements of the Colorado Act; (4) a description of how the parent/guardian and/or the student was harmed as a result of the District's alleged failure to comply with the requirements of the Colorado Act; and

(5) copies of all hard-copy and/or electronic documents that support the allegations in the complaint.

The superintendent or superintendent's designee shall consider the complaint and all supporting documents filed with the complaint, and shall if he/she deems necessary investigate the allegations and/or conduct a hearing on the complaint. Thereafter, within thirty (30) days after receipt of the complaint or as soon thereafter as reasonably practicable the superintendent or superintendent's designee shall render a written determination on whether the District failed to comply with the requirements of the Colorado Act and, if so, what action (if any) shall be taken by the District to address the matter.

If the parent/guardian is not satisfied with the written determination rendered by the superintendent or superintendent's designee, the parent/guardian may file a complaint with the Board of Education and request a hearing pursuant to the procedures in section 6 of Board of Education Policy GP 3.12.

Adopted by Superintendent: October 2, 2017
Revised by Superintendent: October 16, 2017

LEGAL REFS:
20 U.S.C. 1232g
34 C.F.R. 99.1 et seq.
C.R.S. 22-16-101 et seq.

CROSS REFS:
CL, Research Involving District Students, Employees or Resources
EHA, District Information Technology
EHB, Records Retention
GBEE, Employee Use of District Information Technology
JRA/JRC, Student Records / Release of Information on Students
JS, Student Use of District Information Technology