7:340 Student Records

School student records are confidential. Information from them shall not be released other than as provided by law. A school student record is any writing or other recorded information concerning a student and by which a student may be identified individually that is maintained by a school or at its direction by a school employee, regardless of how or where the information is stored, except as provided in State or federal law as summarized below:

1. Records kept in a staff member's sole possession.
2. Records maintained by law enforcement officers working in the school.
3. Video and other electronic recordings (including without limitation, electronic recordings made on school buses) that are created in part for law enforcement, security, or safety reasons or purposes. The content of these recordings may become part of a school student record to the extent school officials create, use, and maintain this content, or it becomes available to them by law enforcement officials, for disciplinary or special education purposes regarding a particular student.
4. Any information, either written or oral, received from law enforcement officials concerning a student less than the age of 18 years who has been arrested or taken into custody.

State and federal law grants students, parents/guardians, and when applicable, the Ill. Dept. of Children and Family Services' Office of Education and Transition Services, certain rights, including the right to inspect, copy, and/or challenge school student records. The information contained in school student records shall be kept current, accurate, clear, and relevant. All information maintained concerning a student receiving special education services shall be directly related to the provision of services to that child. The District may release directory information as permitted by law, but a parent/guardian shall have the right to opt-out of the release of directory information regarding his or her child. The District will comply with State or federal law with regard to release of a student's school records, including, where applicable, without notice to, or the consent of, the student's parent/guardian or eligible student. Upon request, the District discloses school student records without parent consent to the official records custodian of another school in which a student has enrolled or intends to enroll, as well as to any other person as specifically required or permitted by State or federal law.

The Superintendent shall fully implement this policy and designate an *official records custodian* for each school who shall maintain and protect the confidentiality of school student records, inform staff members of this policy, and inform students and their parents/guardians of their rights regarding school student records.

Student Biometric Information Collection

The Superintendent or designee may recommend a student biometric information collection system solely for the purposes of identification and fraud prevention. Such recommendation shall be consistent with budget requirements and in compliance with State law. Biometric information means any information that is collected through an identification process for individuals based on their unique behavioral or physiological characteristics, including fingerprint, hand geometry, voice, or facial recognition or iris or retinal scans.

Before collecting student biometric information, the District shall obtain written permission from the person having legal custody/parental responsibility or the student (if over the age of 18). Upon a student's 18th birthday, the District shall obtain written permission from the student to collect student biometric information. Failure to provide written consent to collect biometric information shall not be

the basis for refusal of any services otherwise available to a student.

All collected biometric information shall be stored and transmitted in a manner that protects it from disclosure. Sale, lease, or other disclosure of biometric information to another person or entity is strictly prohibited.

The District will discontinue use of a student's biometric information and destroy all collected biometric information within 30 days after: (1) the student graduates or withdraws from the School District, or (2) the District receives a written request to discontinue use of biometric information from the person having legal custody/parental responsibility of the student or the student (if over the age of 18). Requests to discontinue using a student's biometric information shall be forwarded to the Superintendent or designee.

The Superintendent or designee shall develop procedures to implement this policy consistent with State and federal law.

LEGAL REF.:

20 U.S.C. §1232g, Family Educational Rights and Privacy Act; 34 C.F.R. Part 99.

50 ILCS 205/7, Local Records Act.

105 ILCS 5/10-20.12b, 5/10-20.40, and 5/14-1.01 et seq.

105 ILCS 10/, Ill. School Student Records Act.

105 ILCS 85/, Student Online Personal Protection Act.

325 ILCS 17/, Children's Privacy Protection and Parental Empowerment Act.

750 ILCS 5/602.11, Ill. Marriage and Dissolution of Marriage Act.

23 Ill.Admin.Code Parts 226 and 375.

Owasso I.S.D. No. I-011 v. Falvo, 534 U.S. 426 (2002).

Chicago Tribune Co. v. Chicago Bd. of Ed., 332 Ill.App.3d 60 (1st Dist. 2002).

CROSS REF.: 5:100 (Staff Development Program), 5:130 (Responsibilities Concerning Internal Information), 7:15 (Student and Family Privacy Rights), 7:220 (Bus Conduct), 7:345 (Use of Educational Technologies; Student Data Privacy and Security)

Adopted: December 21, 2022

STUDENTS

7:345 Use of Educational Technologies; Student Data Privacy and Security

Educational technologies used in the District shall further the objectives of the District's educational program, as set forth in Board policy 6:10, *Educational Philosophy and Objectives*, align with the curriculum criteria in policy 6:40, *Curriculum Development*, and/or support efficient District operations. The Superintendent shall ensure that the use of educational technologies in the District meets the above criteria.

The District and/or vendors under its control may need to collect and maintain data that personally identifies students in order to use certain educational technologies for the benefit of student learning or District operations.

Federal and State law govern the protection of student data, including school student records and/or *covered information*. The sale, rental, lease, or trading of any school student records or covered information by the District is prohibited. Protecting such information is important for legal compliance, District operations, and maintaining the trust of District stakeholders, including parents, students and staff. The Board designates the Technology Director to serve as Privacy Officer, who shall ensure the District complies with the duties and responsibilities required of it under the Student Online Personal Protection Act, 105 ILCS 85/, amended by P.A. 101-516, eff. 7-1-21.

Definitions

Covered information means personally identifiable information (PII) or information linked to PII in any media or format that is not publicly available and is any of the following: (1) created by or provided to an operator by a student or the student's parent/guardian in the course of the student's or parent/guardian's use of the operator's site, service or application; (2) created by or provided to an operator by an employee or agent of the District; or (3) gathered by an operator through the operation of its site, service, or application.

Operators are entities (such as educational technology vendors) that operate Internet websites, online services, online applications, or mobile applications that are designed, marketed, and primarily used for K-12 school purposes.

Breach means the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of covered information maintained by an operator or the District.

Operator Contracts

The Superintendent or designee designates which District employees are authorized to enter into written agreements with operators for those contracts that do not require separate Board approval. Contracts between the Board and operators shall be entered into in accordance with State law and Board policy 4:60, *Purchases and Contracts,* and shall include any specific provisions required by State law.

Security Standards

The Superintendent or designee shall ensure the District implements and maintains reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure. In the event the District receives notice from an operator of a breach or has determined a breach has occurred, the Superintendent or designee shall also ensure that the District provides any breach

notifications required by State law.

LEGAL REF.:

20 U.S.C. §1232g, Family and Educational Rights and Privacy Act, implemented by 34 C.F.R. Part 99.

105 ILCS 10/, Ill. School Student Records Act.

105 ILCS 85/, Student Online Personal Protection Act.

23 Ill. Admin. Code Part 380.

CROSS REF.: 4:15 (Identity Protection), 4:60 (Purchases and Contracts), 6:235 (Access to Electronic Networks), 7:340 (Student Records)

Adopted: January 19, 2022