Students

Use of Educational Technologies; Student Data Privacy and Security

Summary: In accordance with state and federal laws governing the use, collection of storage of student data, the Superintendent will be responsible for ensuring the protection and reporting of student data to be used for educational purposes and ensure all data is protected even when using third party services and software systems.

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.

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: September 24, 2020

REVISED: December 15, 2022