Document Status: Draft Update - New

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

New/Unpublished Section

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.[PRESSPlus1]

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*.[PRESSPlus2] The sale, rental, lease, or trading of any school student records or covered information by the District is prohibited.[PRESSPlus3] Protecting such information is important for legal compliance, District operations, and maintaining the trust of District stakeholders, including parents, students and staff.[Q1]

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.[PRESSPlus4]

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.[PRESSPlus5]

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.[PRESSPlus6] 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.[PRESSPlus7]

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.[PRESSPlus8] 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.[PRESSPlus9]

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.

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

Questions and Answers:

***Required Question 1. SOPPA permits, but does not require, districts to designate an appropriate staff person as a Privacy

Officer, who may also be an official records custodian under ISSRA, to carry out the duties and responsibilities assigned to schools and to ensure a district's compliance with the requirements of SOPPA. 105 ILCS 85/27(f), added by P.A. 101-516, eff. 7-1-21. Boards may designate an individual other than the Superintendent to serve in the capacity of Privacy Officer, such as a Business Manager, IT Director, or District Records Custodian.

Has the Board designated a Privacy Officer?

- No. (default)
- Yes, the Superintendent is designated to serve as Privacy Officer. (IASB will add the following sentence: "The Board designates the Superintendent 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.")
- Yes, a title other than Superintendent has been designated to serve as Privacy Officer. (IASB will add the following sentence: "The Board designates the [Insert Title] 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.") What is the Privacy Officer's Title?:

PRESSPlus Comments

PRESSPlus 1. The Student Online Personal Protection Act (SOPPA) (105 ILCS 85/), amended by P.A. 101-516, eff. 7-1-21, specifically requires boards to adopt a policy for designating which district employees are authorized to enter into agreements with *operators* (see **Operator Contracts** subhead). SOPPA is the State law that governs how educational technology companies, schools, and the Ill. State Board of Education (ISBE) use and protect *covered information* of students. The amendments to SOPPA were intended to strengthen protections for online student data, in part by centralizing the vetting and contracting process within schools, and to give parents ready access to information about how their children's data is being used at school. SOPPA does not, however, require a district to obtain parent opt-in or separate consent for the use of online services or applications, nor is such consent required if the operator is acting as a *school official* pursuant to the delineated exception in the Family Educational Rights and Privacy Act's (FERPA)(20 U.S.C. §1232g) implementing regulations. See 34 C.F.R. §99.3(a). **Issue 104, June 2020**

PRESSPlus 2. See policy 7:340, *Student Records*, and its implementing administrative procedure, 7:340-AP1, *School Student Records*, available at PRESS Online by logging in at www.iasb.com, for requirements addressing school student records under federal and State law. SOPPA does not override or otherwise supersede the requirements of FERPA or the Ill. School Student Records Act (ISSRA) (105 ILCS 10/). 105 ILCS 85/30(9), amended by P.A. 101-516, eff. 7-1-21.

Covered information is a broader concept than student records, and may include information that does not qualify as a student record. However, even if the covered information is not maintained as a student record, it may still qualify as a *public record* under the Local Records Act (50 ILCS 205/), such that a district would have an obligation to maintain it. Consult the board attorney for guidance on these issues. **Issue 104, June 2020**

PRESSPlus 3. 105 ILCS 85/26(1), added by P.A. 101-516, eff. 7-1-21. SOPPA includes a clarification that schools and operators are not prohibited from producing and distributing, free or for consideration, student class photos and yearbooks to the school, students, parents, or others authorized by parents, as long as there is a written agreement between the operator and district. 105 ILCS 85/30(10), amended by P.A. 101-516, eff. 7-1-21. **Issue 104, June 2020**

PRESSPlus 4. SOPPA specifically provides that it does not apply to general audience websites, online services, online applications, or mobile applications, even if login credentials are required to access the general audience sites, services, or applications. 105 ILCS 85/30(3), amended by P.A. 101-516, eff. 7-1-21. Consult the board attorney for guidance regarding whether certain applications that may be widely used by schools, but which may not have been originally marketed to K-12 (e.g., certain video conference applications), come within the scope of SOPPA. **Issue 104, June 2020**

PRESSPlus 5. Operators must notify districts of a breach of covered information within the most expedient time possible and without reasonable delay, but no later than 30 calendar days after the determination that a breach has occurred. 105 ILCS 85/15(5), added by P.A. 101-516, eff. 7-1-21. **Issue 104, June 2020**

PRESSPlus 6. This statement is required by 105 ILCS 85/27(b), added by P.A. 101-516, eff. 7-1-21. SOPPA provides that any agreement entered into in violation of SOPPA "is void and unenforceable as against public policy." Id. SOPPA does not provide for a private right of action against school districts; the Ill. Attorney General has enforcement authority under SOPPA through the Consumer Fraud Deceptive Trade Practices Act. 105 ILCS 85/35. **Issue 104, June 2020**

PRESSPlus 7. SOPPA requires specific provisions be included in a contract with any operator that seeks to receive covered information from a school district. 105 ILCS 85/15(4), added by P.A. 101-516, eff. 7-1-21. See 7:345-AP, *Use of Educational Technologies; Student Data Privacy and Security*, available at PRESS Online by logging in at www.iasb.com, for details. **Issue 104, June 2020**

PRESSPlus 8. 105 ILCS 85/27(e), added by P.A. 101-516, eff. 7-1-21. SOPPA does not provide specifics regarding security procedures or practices, nor is there a formal, nationalized standard specific to K-12. However, SOPPA requires ISBE to make available on its website guidance for schools pertaining to reasonable security procedures and practices. 105 ILCS 85/28, added by P.A. 101-516, eff. 7-1-21. ISBE, the U.S. Dept. of Education (DOE) and other experts in the field agree that training of all staff with access to a school's network is important to protecting schools against cyber threats, although such training is not currently mandated in Illinois. ISBE's grant-funded program, the Learning Technology Center of Illinois, offers cybersecurity training to administrators and educators throughout the State. See www.ltc.org. The U.S. Dept. of Education has also issued multiple guidance documents on security best practices for schools, available at www.studentprivacy.ed.gov/topic/security-best-practices. **Issue 104, June 2020**

PRESSPlus 9. In the event of a breach of covered information of students, SOPPA requires school districts to provide two types of notices: (1) individual notices to the parents of students whose covered information was involved in the breach and (2) a more general notice about the breach on the district's website (or at the district administrative office, if it does not maintain a website) if the breach involved 10% or more of the district's student enrollment. 105 ILCS 85/27(a)(5) & (d), added by P.A. 101-516, eff. 7-1-21. See 7:345-AP, *Use of Educational Technologies; Student Data Privacy and Security*, available at PRESS Online by logging in at www.iasb.com, for details about the required notices. **Issue 104, June 2020**