Illinois Council of School Attorneys
One Imperial Place | 1 East 22nd Street, Suite 20
Lombard, Illinois 60148-6120

Answers to FAQs Regarding the Student Online Personal Protection Act and Public Schools

April 2021

Published by a Committee of the Illinois Council of School Attorneys[1]

ICSA publishes this guidance as part of its continuing effort to provide assistance to public school leaders. The responses to the FAQs represent the combined thinking of committee members. **This guidance is published for informational purposes only and is not a substitute for legal advice. For legal advice or a legal opinion on a specific question, you should consult a lawyer.**

---

1. What is SOPPA?

The Student Online Personal Protection Act (105 ILCS 85/), or SOPPA, is a State law that is intended to protect the privacy and security of students' online data at school. When SOPPA was originally enacted, it regulated how educational technology vendors handle student data. In 2019, the law was significantly amended by Public Act 101-516 to also regulate how schools and the Illinois State Board of Education (ISBE) manage student data, in addition to vendors. The amendment is effective July 1, 2021.

2. What are the key definitions in SOPPA with which school districts must be familiar to understand their obligations under this law?

Key definitions in SOPPA include (105 ILCS 85/5):

a. *Operators* – entities that operate Internet websites, online services, online applications, or mobile applications that are *designed, marketed, and primarily used for K-12 school purposes*. SOPPA does not apply to "general audience" Internet websites, online services, or applications that are not designed for K-12 use.

Note: Whether a particular company qualifies as an "operator" will depend upon the specifics of the particular service or application being offered. For example, companies that offer general cloud storage solutions, survey tools, or other business software, may not be "operators" if those services are not designed, marketed, and primarily used for K-12 purposes.

b. *Covered information* – 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:

i. 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 (e.g., student work uploaded on an application);

ii. created by or provided to an operator by an employee or agent of a district (e.g., student PII entered by district personnel into a student information system); or

iii. gathered by an operator through the operation of its site, service, or application (e.g., a username and password or other demographic data connected to a student).

Examples of covered information include information in the student's educational record or electronic mail, first and last name, home address, telephone number, electronic mail address, or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, a social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information.

c. *K-12 school purposes* – purposes that are directed by, or that customarily take place at the direction of, a teacher, school, or school district; aid in the administration of school activities, including, but not limited to, instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents; or are otherwise for the use and benefit of a school.

d. *Breach* – the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of covered information maintained by an operator or school.

3. How does the amendment to SOPPA impact school districts?

SOPPA requires districts to satisfy a number of requirements related to covered information and their contracts with operators. As a practical matter, these changes will require districts to establish a centralized process to vet and approve websites, online services, and applications to ensure their use within the district complies with SOPPA. In general terms, districts must:

a. Enter into a written agreement that contains certain prescribed terms whenever an *operator seeks to receive covered information* from the district and *before* a district discloses any covered information to an operator (105 ILCS 15(4));

b. Enter into a written agreement whenever the district shares, transfers, discloses, or provides access to a student's covered information to a third party other than the student's parent, school personnel, school board member, or ISBE unless the disclosure is otherwise permitted by SOPPA (105 ILCS 26/2);

c. Post on the district website[2] copies of written agreements with operators and specific information that a layperson can understand about what covered information is collected by operators and for what purpose the information is being used (105 ILCS 85/27(a) & (c));

d. Ensure that covered information is protected using reasonable security procedures and practices that meet or exceed industry standards (105 ILCS 85/27(e));

e. Adopt a policy to designate what school employees are authorized to enter into written agreements with operators (105 ILCS 85/27(b));

f. Determine whether to designate a privacy officer to oversee SOPPA compliance, and if applicable, who will serve in that role (105 ILCS 85/27(f));

g. Allow parents to request: (1) copies of their students' covered information, (2) corrections to inaccuracies to their student's covered information; and (3) deletion of their student's covered information (105 ILCS 85/27(b) and 85/33(c)); and

h. Provide notices about breaches of covered information to parents of affected students and in cases involving more than 10% of students enrolled, more general information about breaches on the district's website. (105 ILCS 85/27(5)).

4. What terms must be included in agreements with operators?

Written agreements with operators must include (105 ILCS 85/15(4)) and 85/27(g)):

a. A listing of the types or categories of covered information to be provided to the operator;

b. A statement of the product or service being provided to the district by the operator;

c. A statement that, the pursuant to the Family Educational Rights and Privacy Act (FERPA), the operator is acting as a school official with a legitimate educational interest, is performing an institutional service or function for which the school would otherwise use employees, under the direct control of the school with respect to the use and maintenance of covered information, and is using the covered information only for an authorized purpose and may not re-disclose it to third parties or affiliates, unless otherwise permitted under SOPPA, without permission from the district or pursuant to court order;

d. If a breach is attributed to an operator, a description of how any costs or expenses in investigating and remediating the breach will be allocated between the operator and the district;

e. A statement that an operator must delete or transfer to the district all covered information if the information is no longer needed for the purposes of the written agreement and to specify the time period in which the information must be deleted or transferred once the operator is made aware the information is no longer needed; and

f. If the district maintains a website, a statement that the district must publish the written agreement on its website, or if the district has no website, a statement that the agreement is available for public inspection at its administrative office.

g. A provision requiring the operator to implement and maintain 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.

5. Does a district have to renegotiate all of its existing agreements with operators to comply with SOPPA?

Agreements with operators that are entered into, amended, or renewed as of SOPPA's effective date of July 1, 2021, must contain the provisions required by SOPPA (see Question 4). Attorneys have differing opinions about whether this means that existing contracts with operators that are mid-term must contain the prescribed contract terms by July 1, 2021. Districts should seek advice on this issue from the board attorney and discuss the best way to prioritize contract negotiation with vendors in light of the comprehensive nature of SOPPA's new requirements. Districts should also be careful to monitor "evergreen" contracts that are scheduled to automatically renew after July 1, 2021, but which may not yet have the mandatory SOPPA terms. These contracts will need to be revised before renewal to permit compliance with SOPPA. A district may decide to use an addendum or separate privacy agreement to supplement an existing contract.

Finally, districts are still required to post all operator contracts and information about the covered information being shared with the operator, even if the contracts themselves do not yet have all of the required provisions.

6. Is there a Statewide, SOPPA-compliant privacy agreement template that all districts can use?

ISBE does not have a template available, but an Illinois version of a model National Data Privacy Agreement (NDPA) is available through the Illinois Student Privacy Alliance (ISPA) at: https://sdpc.a4l.org/view_alliance.php?state=IL for districts to consider. More information about the ISPA can be found here: https://ltcillinois.org/services/ispa/. The model agreement consists of the National Data Privacy Agreement and other exhibits, including an Illinois addendum, which is labeled Exhibit "G". Exhibit G was drafted and reviewed by members of the Illinois Council of School Attorneys.

The Illinois version of the NDPA acts as an "umbrella" agreement over a district's existing service agreement with a vendor. Districts who join the ISPA (at no cost) have access to the Student Data Privacy Consortium's (SDPC) database tool, which allows districts to upload originating contracts with vendors and display information about those contracts on their websites to assist with SOPPA's website posting requirements for operator contracts. Once a district has uploaded an originating contract to the SDPC database, other districts can subscribe to the terms of the originating agreement by signing a single-page general offer, during a three year offer period. Alternatively, districts may choose to manage their operator contracts through an in-house process or through the use of other third party platforms.

7. Are there other situations in which SOPPA requires a district to have a written agreement with a third party before it can disclose a student's covered information?

As noted in Question 3 above, a district must also enter into a written agreement whenever it shares, transfers, discloses, or provides access to a student's covered information to a third party other than the student's parent, school personnel, school board member, or ISBE. However, a written agreement is not required if the disclosure is: (1) to law enforcement officials to protect the safety of users or other or the security or integrity of the operator's service (to the extent permitted by law), (2) required by court order or State or federal law, or (3) to ensure legal or regulatory compliance. (105 ICLS 85/26(2)). Unfortunately, the scope of this written agreement requirement and what terms such agreements must contain is unclear. It is important for districts to work with their board attorneys to determine when written agreements with third parties should be used and what those agreements ought to contain.

8. Does SOPPA require a district to have certain policies or procedures in place?

SOPPA requires districts to:

a. Adopt a policy for designating which school employees are authorized to enter into written agreements with operators. (105 ILCS 85/27(b)).

b. Implement and maintain 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. (105 ILCS 85/27(e)).

c. Post on their websites a description of the procedures that parents may use to carry out their rights to: (1) inspect and review their student's covered information, (2) request a paper or electronic copy of their student's covered information, and (3) request corrections for factual inaccuracies contained in their student's covered information. (105 ILCS 85/27(a)(4)).

SOPPA also requires ISBE to adopt model policies and procedures, as well as guidance for reasonable security procedures and practices, to assist schools with implementation of the law. In March of 2021, ISBE adopted the **PRESS** 7:345 suite of sample materials as its "model" policy and procedures (See www.isbe.net/Pages/Educational-Technology.aspx). In addition to this FAQ, the PRESS materials are a helpful resource to understand a district's SOPPA compliance obligations. ISBE's security guidance is also available at www.isbe.net/Pages/Educational-Technology.aspx.

9. Are districts required to have contracts with social media companies, such as Twitter or Facebook, if they post student photos or other personally identifiable information about students on their social media feeds?

Probably not, because sites like Facebook, Instagram and Twitter likely fall under the category of a general audience website or application that is not designed, marketed, and primarily used for K-12 purposes. Those companies would therefore not likely meet the definition of an "operator" in SOPPA. Districts, however, should consult the board attorney for guidance if they have questions about SOPPA's applicability to specific sites and applications.

10. What information does SOPPA require a district to post on its website? And how often must a district update that information?

Districts are required to post the following information on their websites, which must be updated (as needed) by January 31st and July 31st each year:

a. A list of operators with whom the district has written agreements and the following for each operator: 1) copy of the agreement, 2) business address, and 3) list of any subcontractors to whom covered information may be disclosed or a link to a page on the operator's website that clearly lists the subcontractors. Within

10 days after entering into a new agreement with an operator, the district must post on its website a copy of the agreement, along with operator's business address, list of subcontractors, and explanation of data elements (see #2 below).

b. Explanation of the data elements of covered information that the district collects, maintains, or discloses to any person, entity, third party, or governmental agency.

c. A list of breaches of covered information maintained by the school or an operator involving 10% or more of the district's student enrollment. (105 ILCS 85/27(a)(5)). The list must include:

   i. Number of students whose covered information was involved in the breach, unless the breach involved "personal information" as defined in the Personal Information Protection Act, 815 ILCS 530/5[3], in which case the number of students involved may not be disclosed.

   ii. Date, estimated date, or estimated date range of the breach

   iii. Name of the operator, if applicable

d. A description of the procedures that parents may use to carry out their rights to: (1) inspect and review their student's covered information, (2) request a paper or electronic copy of their student's covered information, and (3) request corrections for factual inaccuracies contained in their student's covered information. (See Question 8).

11. Apart from the required website postings, are there any other notice requirements under SOPPA with which districts must comply?

Yes. Individual parent notification is required in the event of a breach of covered information. (See Question 12). Districts are also required to provide parents and students with ISBE's model annual notice about operators at the beginning of each school year. ISBE has adopted **PRESS** sample exhibit 7:345, AP-E2, *Student Data Privacy; Notice to Parents About Educational Technology Vendors*, as its model notice. (Districts that are not **PRESS** subscribers can access the notice by following the instructions at: www.isbe.net/Pages/Educational-Technology.aspx). The annual notice must be provided by the same means a school generally uses to send notices parents, such as in a student handbook. (105 ILCS 85/28(e)).

12. What does SOPPA require a district to do in the case of a breach of covered information?

Unless a law enforcement agency has requested in writing that notification be delayed for purposes of a criminal investigation, after receipt of notice from an operator that a breach has occurred, or after determination of a breach of covered information maintained by a school, a district must notify the parent of any student whose covered information is involved in the breach. The notice must be given within 30 calendar days of receipt of the notice or the determination that a breach has occurred, and must contain: 1) the date, estimated date or estimated date range of the breach, 2) a description of the covered information that was compromised or reasonably believed to have been compromised, 3) operator and school contact information that a parent can use to inquire about the breach, 4) contact information and websites for consumer reporting agencies and the Federal Trade Commission (FTC), and 5) a statement that the parent may obtain information from the FTC and consumer reporting agencies about fraud alerts and security freezes. (105 ILCS 85/27(d)).

Additionally, a district must list the following information on its website for breaches affecting 10% or more of the district's student enrollment: 1) The number of students whose covered information was involved in breach, unless the breach involved a student's "personal information" as defined by the Illinois Personal Information Protection Act, 2) the date, estimated date or estimated date range of the breach, and 3) the name of the operator. (See Question 10). This public breach list must be updated by January 31st and July 31st each year and stay posted for five years. Breaches that occurred prior to the July 1, 2021, do not have to be included in the list.

Finally, in the event a breach occurs, a district should immediately notify its insurance carrier and review its written agreement with the operator involved to determine whether the district is entitled to reimbursement for costs and expenses that it incurred in investigating and remediating the breach.

13. Is *covered information* equivalent to *school student records* under the Illinois School Student Records Act (ISSRA)?

The definition of covered information (See Question 2) is different and generally broader than the definition of school student records under ISSRA, which, in relevant part, is defined as "recorded information concerning a student and by which a student may be individually identified, maintained by a school...regardless of how or where the information is stored." (105 ILCS 10/2). For example, covered information may include student-generated work and login information that is stored in an application, but not ultimately maintained by a school as a student temporary or permanent record under ISSRA. In contrast, information contained in a district's student information system (SIS) is likely to contain permanent and temporary student record information that has to be preserved in accordance with ISSRA retention requirements.

Interestingly, in at least one aspect, the definition of covered information is narrower than school student records because it is limited to personally identifiable information that is not "publicly available." Under ISSRA, student "directory information," is publicly available and can include basic identifying information which districts must also maintain as part of a student's school student record. Therefore, such information may not technically meet the definition of covered information in SOPPA. However, because parents can "opt out" of release of directory information, the categories a district defines as directory information may not be publicly available for all students. Further, as a practical matter, operators handling any kind of personally identifiable student information, whether publicly available or not, should be protecting that data under a written agreement that specifies the operator's data privacy obligations.

It is important for districts to consult with the board attorney for guidance on the interplay of covered information and student records and related record preservation and release issues. SOPPA does not supersede the provisions of ISSRA, therefore, compliance with both laws needs to be managed. (105 ILCS 85/30(9)). Districts that fail to properly preserve school student records can face increased legal exposure.

14. Does a district need to have a written agreement to transfer covered information when a student is transferring to another school district or private school?

No, provided that the covered information being transferred are school student records under ISSRA. A district does not have to have a written agreement to transfer those records because SOPPA authorizes transfer of covered information when required by law. (105 ILCS 85/26(2)(B)). ISSRA regulations require a school district to transfer a certified copy of a student's permanent and temporary records upon the request of the district or private school to which the student is transferring, with prior written notice to the parent/guardian. (23 Ill.Admin.Code §§375.60; 375.75).

15. How long may an operator keep covered information?

An operator may only retain covered information as long as it is needed to service its agreement with a district, at which point the operator must either transfer to the district or delete the covered information within the time period specified in the agreement. The agreement should also address how the operator will notify the district once the covered information is no longer needed so that the district can review the information and determine what data needs to be maintained (for example, to comply with student records laws) and what can be deleted.

As practical matter, once an operator no longer needs access to the covered information, it loses its "school official" status under FERPA that allowed it to access student data without having to obtain separate parental consent. Most often, the point at which covered information will no longer be needed for an agreement will coincide with the expiration or termination of the services. However, there may be a need to delete or transfer data during the term of a services agreement, such as when a student leaves the district and that former student's data is no longer relevant to the services being provided.

16. How will SOPPA be enforced?

The Attorney General has the authority to enforce SOPPA violations as unlawful practices under the Consumer Fraud and Deceptive Business Practices Act (Act). (105 ILCS 85/35). It is unclear whether the Attorney General can or will bring formal enforcement actions against public schools; the Act is limited to enforcement against "persons," who are not defined to include public entities such as school districts. (815 ILCS 505/1(c)). SOPPA does not provide parents with the right to individually sue districts for violations. However, it is important to note that in the situation of a data breach, a district could still face potential liability exposure under ISSRA or tort law if it failed to adequately protect student data. Failure to comply with SOPPA may also impact a district's ability to maintain cyber liability insurance coverage.

17. Does SOPPA give parents the right to opt out of their student's data being shared with operators?

No, SOPPA does not provide parents with such opt-out rights. In fact, language requiring parent consent that was included in the original version of the SOPPA bill (HB 3606) was removed through later amendment in the legislative process.

18. Can districts put any limits on parents' rights to their students' covered information?

Under SOPPA, parents have the right to inspect, review, and copy their student's covered information. If a parent requests paper copies, a district can charge a reasonable cost for the copies but cannot deny the request if the parent does not have the ability to pay. As of the date of the publication of this FAQ, ISBE has proposed rules pending that would place a limit on how often parents can request copies, specify the manner in which such requests must be made, and establish the maximum amount a district can charge per page of copying.

Parents also have the right under SOPPA to request a school to delete their student's covered information, as long as that request would not require a district to delete student records it is required by law to maintain. If a district receives a blanket request from a parent to delete all of his or her student's covered information such that the student would not be able to effectively participate in the curriculum, the district should first consult the board attorney for advice before responding.

19. What does a district do if a parent wants to challenge the accuracy of his or her student's covered information?

Under SOPPA, a parent may request correction of factual inaccuracies in his or her student's covered information. Districts have the authority to determine if such a factual inaccuracy exists and if one does, the district or operator must take action to make the correction within 90 calendar days. The district must then confirm with the parent that the correction was made within 10 days of the operator's confirmation of the correction, if applicable. SOPPA does not provide a way for parents to challenge a district's determination about the need for a correction. However, if the alleged inaccuracy involves student record information, then ISSRA has specific challenge procedures with prescribed timelines. Ideally, any ISSRA record challenge would be resolved within 90 days to also meet the SOPPA timeframe, but that may not always be possible. Districts should consult the board attorney for further guidance on this issue.

20. Does SOPPA require districts to ensure that non-public special education day or residential facilities where students are placed by a school district are complying with SOPPA?

Non-public schools are generally exempted from SOPPA's contracting, posting, breach notification, and parent access requirements. When a district places a student at an ISBE-approved non-public special education day or residential facility, the facility is required by ISBE rules and ISBE's facility placement contract to comply with ISSRA and the student record policy and procedures of a student's public school district of residence, even though ISSRA itself does not apply to non-public schools. (23 Ill.Admin.Code §401.270). As of the date of publication of this FAQ, ISBE has not amended its regulations or its non-public facility placement contract to specifically require these facilities to comply with SOPPA. However, due to a lack of guidance in this area, districts should consult the board attorneys for advice on this issue.

21. What if a district wants to use an online or mobile application to help meet the needs of a special education student, but that application does not meet all SOPPA requirements?

This is a difficult situation because a district may feel it is necessary to use a particular application to support successful implementation of a student's IEP. However, there is no exemption in SOPPA for special education students. Districts may need to explore alternative programs in those situations to avoid SOPPA compliance issues. Districts should consult the board attorney for further guidance when these circumstances arise.

---

[1] The following attorneys are members of this committee: Debra H. Jacobson, Illinois Association of School Boards; Nicki B. Bazer, Franczek P.C.; Heather K. Brickman, Jennifer M. Deutch, and Jennifer Mueller, Rosenberg, Hodges, Loizzi, Eisenhammer, Rodick & Kohn LLP; Joseph P. Clary, Waukegan CUSD 60; Ryan Morton, Ottosen, Dinolfo, Hasenbalg & Castaldo, Ltd.; James A. Petrungaro, Himes, Petrarca and Fester, Chtd.; M. Curt Richardson, McLean Co Unit District 5; and Courtney N. Stillman, Hauser, Izzo, Petrarca, Gleason & Stillman, LLC. The 2021 ICSA Executive Committee provided peer review.

[2] If a district does not maintain a website, it must still make all of the information that SOPPA otherwise requires to be web-posted available for public inspection at its administrative office.

[3] Under the Personal Information Protection Act, 815 ILCS 530/5, "personal information" means either of the following:

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security:

(A) Social Security number.

(B) Driver's license number or State identification card number.

(C) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(F) Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

(2) User name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records.