Learning Technology Center

Student Online Personal Protection Act (SOPPA)

4ltc.org/soppa

Last Update: February 11, 2021

What is SOPPA

- Legislation created in 2019.
- Goes into effect on July 1, 2021.
- Places additional requirements on districts (and vendors and ISBE) to protect student data privacy, increase transparency, and hold vendors accountable.

SOPPA Requirements

Reasonable Security Practices

Districts are expected to implement and maintain “reasonable security practices and procedures” as defined by ISBE.

LTC recommends 43 best practices that Illinois districts should implement to comply with SOPPA.

ltcillinois.org/cybersecurity

BEST PRACTICES

Reasonable Security Practices

43 security best practices that all Illinois districts should implement to comply with the Student Online Personal Protection Act.

Beginning July 1, 2021, Illinois public schools must "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 85/15). The Learning Technology Center selected 43 security best practices that all districts should implement to comply with legislation. The practices align with CIS Controls, a globally recognized cybersecurity standard, and are vetted by Illinois school district technology leaders.

HARDWARE ASSETS

Maintain Detailed Asset Inventory

Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not (CIS 1.4).

Address Unauthorized Assets

Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner (CIS 1.6).

SOFTWARE ASSETS

Maintain Inventory of Authorized Software

Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system (CIS 2.1).

Ensure Software is Supported by Vendor

Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system (CIS 2.2).

Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner (CIS 2.6).

VULNERABILITY MANAGEMENT

Deploy Automated Operating System Patch Management Tools

Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor (CIS 3.4).

Deploy Automated Software Patch Management Tools

Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor (CIS 3.5).

ADMIN PRIVILEGES

Change Default Passwords

Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts (CIS 4.2).

Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities (CIS 4.3).

SOPPA Requirements

Data Privacy Agreements

Enter into written agreements with all K-12 service providers who collect student data. Agreements must contain provisions:

A. The categories of covered information to be provided to the operator
B. A statement of the product or service that the operator is providing to the district;
C. A statement that the operator will implement and maintain reasonable security procedures and practices
D. A statement that the operator is acting as a school official under the Family Educational Rights and Privacy Act (“FERPA”);
E. A description of how the district and operator will allocate costs for investigating and remediating a data breach attributable to the operator (including costs for notifying parents and regulatory agencies, credit monitoring, legal fees and audit costs, or any other damages that the district incurs);
F. A statement that the operator must delete or transfer to the district all covered information that is no longer needed for the purposes of the agreement; and
G. A statement that the written agreement will be published on the district’s website.

SOPPA Requirements

Post Data Privacy Agreements

Post and maintain all agreements on the district's websites. Districts websites must contain:

- A list of all operators of online services or applications utilized by the district (annually).
- Contracts for each operator within 10 days of signing.
- Subcontractors for each operator (annually).
- All data elements that the school collects, maintains, or discloses to any entity (annually). This information must also explain how the school uses the data, and to whom and why it discloses the data.
- The process for how parents can exercise their rights to inspect, review and correct information maintained by the school, operator, or ISBE.
- Data breaches within 10 days and notify parents within 30 days.

SOPPA Requirements

Update Policies

- The person(s)/role(s) that can sign agreements.
- The process for how parents can exercise their rights to inspect, review and correct information maintained by the school, operator, or ISBE.
- Annually:
  - Post a list of all operators of online services or applications utilized by the districts
  - All data elements that the school collects, maintains, or discloses to any entity.
  - List of subcontracts.
- 10 Days After Signing: Contracts/Agreements for each operator.
- 10 Days After Breach: Notice of a data breach.
- 30 Days After Breach: Notify Parents

SOPPA Impact

Personally Identifiable Information

SOPPA affects personally identifiable information (PII), material that is linked to PII, and material in any media or format that is not publically available and is any of the following:

- Created by or provided to an operator by a student or the student's parent in the course of the student's, parent's, or legal guardian's use of the operator's site, service, or application for K-12 school purposes.
- Created by or provided to an operator by an employee or agent of a school or school district for K-12 school purposes.
- Gathered by an operator through the operation of its site, service, or application for K-12 school purposes and personally identifies a student.

SOPPA Impact

What does this mean Districts?

All digital resources that collect student data will need to be reviewed, approved, and have a data privacy agreement in place prior to use.

School personnel will need to know what tools they can use and what tools are not allowed.

SOPPA Compliance

Steps to Compliance

1. **Communicate** with Superintendent, Legal Counsel, and Board

2. **Designate.** Assign the role(s) of Data Privacy Officer and contract signer.

3. **Update policies.** Include processes for addressing data breaches and parents rights. For school districts that subscribe to IASB PRESS Policy Services, see *PRESS Policy 7:345, Use of Educational Technologies; Student Data Privacy and Security.*

SOPPA Compliance

Steps to Compliance

4. **Implement and maintain reasonable security measures.** Implement LTC recommendations. Provide appropriate trainings.

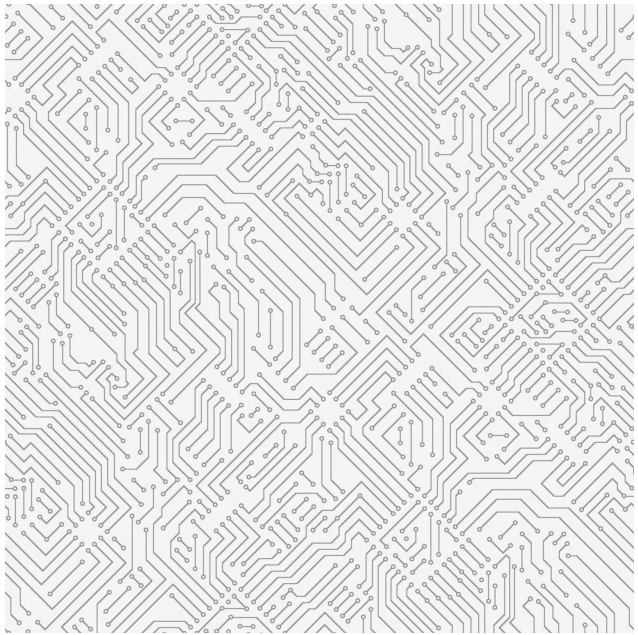
5. **Create an inventory of existing resources.** Gather and review existing vendors and agreements to determine.

6. **Have all operators sign an agreement.** We recommend the National Data Privacy Agreement.

7. **Manage Agreement Processes via ISPA**, alternative 3rd party program, or strict internal processes.

PROGRAM

National Data Privacy Agreement



The National Data Privacy Agreement (NDPA) was developed by 28 state alliances addressing data privacy needs. The LTC encourages districts to adopt the NDPA with the Illinois Exhibit to help streamline the educational application contracting process.

ltcillinois.org/services/ispa

PROGRAM

Illinois Student Privacy Alliance (ISPA) + NDPA

ltcillinois.org/services/ispa

A free tool for managing privacy agreements in compliance with SOPPA. ISPA is a shared database that allows districts to:

- Manage and track agreements.
- “Piggyback” on agreements when another district in Illinois already signed an agreement.
- Post agreements, data elements, and subcontractors on your website.

SOPPA Resources

- Legislative Brief on SOPPA
- SOPPA Introduction Video
- Frequently Asked Questions
- Recommended Reasonable Security Practices

ISPA Resources

- Illinois Student Privacy Alliance (ISPA)
- Using ISPA to Comply with SOPPA (Flowchart)
- Managing Agreements with ISPA (Flowchart)
- Sample ISPA Communications

ltcillinois.org/services/dataprivacy