Student Data Privacy

Implementing the
Amendments to Illinois'
Student Online Personal
Protection Act (SOPPA)

Introductions

Tom Kinane (Moderator)
Director of Technology, Elmwood Park CUSD 401

Chris Wherley (Speaker)
Director of Technology Services, LTC of Illinois

Tony Inglese , SFO, CETL (Speaker)
Chief Financial Officer, Batavia USD 101

Outline

I. History and Intent of the Act

II. New Requirements

III. Recommendations to Implement and Comply

IV. Helpful Tools and Resources

Related History and Intent of the Act

- Until SOPPA, Illinois relied mostly on laws from the 1970s designed for paper student records to manage digital data.
- Modernizes and clarifies the responsibilities of operators and school districts to protect student privacy, with emphasis on transparency.

Related Federal Laws

FERPA- Family Educational Rights and Privacy Act

COPPA- Children's Online Privacy Protection Act

CIPA- Children's Internet Protection Act

PPRA- Protection of Pupil Rights Amendment

Related State Laws

ISSRA- Illinois School Student Records Act

MHDDCA - Mental Health and Developmental Disabilities Confidentiality Act

IPA - Identity Protection Act

PIPA - Personal Information Protection Act

Student Online Personal Protection Act (1 c

Effective July 1, 2021, school districts **must** :

1. Annually post a list of all operators of online services or applications utilized by the district.
2. Biannually post all data elements that the school collects, maintains, and discloses; and explain in "lay terms" how the data is used, and to whom and the purpose it is disclosed.
3. Post written agreements with each operator within 10 business days.

SOPPA (2 of 3)

School districts **must** :

5. Post the process for how parents can exercise their rights to inspect, review and correct information covered information.
6. Post data breaches within 10 days and notify parents within 30 days.
7. Create a policy for who can sign contracts with operators.
8. Require that operators maintain “reasonable security procedures and practices.”

SOPPA (3 of 3)

School districts **may** (or should):

1. Designate a privacy officer to ensure compliance.
2. Provide teachers with the list of online operators that are safe and approved for use.
3. Develop a process for keeping data inventory up-to-date.

Data Sharing Agreement in NDPA

NDPA Feature	Description
Section	Cover Page
Section	Page 2 - Options
Section	Page 3 - Signatories
Section	Standard Clauses
Section	- Exhibits - A = Descriptions of Services - B = Schedule of Data - C = Definitions - D = DIrective for Disposition of Da - E = General Offer of Terms - F = Data Security Requirements - G = Supplemental State Terms - F = Additional Terms or Modifications

and is entered into by and between:

[School District Name], located at [Street, City, State] (the "**Local Education Agency**" or "**LEA**") and [Provider Name], located at [Street, City, State] (the "**Provider**").

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions.** ***Check if Required***

   ☐ If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.

   ☐ If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit "H". (Optional)**

   ☐ If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

Reasonable Security Practices

Each District can and will determine

Example Frameworks:

NIST Cybersecurity Framework - https://www.nist.gov/cyberframework

CIS Controls - https://www.cisecurity.org/

CIS Controls V7.1 Implementation Groups

CIS Controls V7.1 Implementation Groups

The CIS Controls Implementation Groups take a "horizontal" look across all of the CIS Controls and identify a set of Sub-Controls to provide a simple and accessible way to help organizations of different classes focus their security resources.

[Learn more about CIS Controls >>]

Implementation Group 1

- 43 Sub-Controls out of the 171 total
- Combination of procedural and technical mitigations
  - Heavily leans procedural
- Represents the essential sub -controls that mitigate the most common attacks
- Many sub -controls may require an IT contractor for smaller organizations
- Defined as cyber hygiene
- Impact on usability should be low

Procedural IG1 Topics

- Maintaining an asset inventory
- Password management
- 1 offsite backup
- Network boundary inventory
- Sensitive information inventory
- Security awareness program
- Incident response planning
- Isolated networks for personal devices

Technical IG1 Topics

- Automated patching
- Secure configuration
- Audit logging
- DNS filtering
- Dedicated admin workstations
- Account management
- Updated antivirus
- Backups
- Smartphone and tablet encryption
- Wireless encryption
- Firewall rules and management

LTC Cybersecurity Resources

https://ltcillinois.org/services/cybersecurity/

	A	B	C	D	E
1		CIS Controls Implementation Group 1 (43 Subcontrols)			Data from https://www.cisecurity.org/controls/cis-controls-implementation-groups/
2		CIS Subcontrols	Asset Type	Title	Description
3		1.4	Devices	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.
4		1.6	Devices	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.
5		2.1	Applications	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.
6		2.2	Applications	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.
7		2.6	Applications	Address unapproved software	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner
8		3.4	Applications	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.
9		3.5	Applications	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.
10		4.2	Users	Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.
11		4.3	Users	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.

All Controls

Action | Save | Filter | Download Report

	#	Control Question	Applicable	Assigned	Completed	Validated	Policy Defined	Control Implemented	Control Automated	Control Reported
☐	1.4	Maintain Detailed Asset Inventory	Yes	✓	✗	✗	Informal Policy	Parts of Policy Implemented	Not Automated	Not Reported
☐	1.6	Address Unauthorized Assets	Yes	✓	✗	✗	Informal Policy	Parts of Policy Implemented	Not Automated	Not Reported
☐	2.1	Maintain Inventory of Authorized Software	Yes	✓	✗	✗	Approved Written Policy	Implemented on Most Systems	Automated on Most Systems	Reported on Most Systems
☐	2.2	Ensure Software is Supported by Vendor	Yes	-	-	-	Select an option	Select an option	Select an option	Select an option
☐	2.6	Address Unapproved Software	Yes	-	-	-	Select an option	Select an option	Select an option	Select an option
☐		Deploy Automated Operating System	Yes							

Requirement: Publishing Agreements Onlin

Within 10 business days, school district must publish all written agreements with operators in their website, including:

- Data elements disclosed to the operator
- Operator’s business address and contact information
- Subcontractors of the the operator

Requirement: Designate Authorized Signat

“A school may not ... (2) Share, transfer, disclose [covered information] ... without a written agreement ...” (105 ILCS 85/26)

“Each school must adopt a policy for designating which school employees are authorized to enter into written agreements with operators. ... Any agreement or contract entered into in violation of this Act is void and unenforceable as against public policy.” (105 ILCS 85/27(b))

Rec. 1: Establish an Implementation Team

- Create a multi -disciplinary team to lead the implementation
- At a minimum, include technology, business, and curriculum and instruction
- Review requirements, policies, workflow, and documentation

Rec. 2: Ascertain Software Currently Used

- The Act requires due diligence to catalog all software currently in use, including:
  - Applications, apps, web sites and services, and browser extensions
- Consider using software to automate the discovery process

Rec. 3: Establish Contract Management

- Track each written agreement, including:
  - Status of the agreement; operator and business contact information; purpose of the software; data elements involved and how they are used; start, end and renewal dates; value or amount of the contract; the operator's subcontractors; any data breaches and related details, including number of students involved.
- Contract management system should comport with requirements for annual statement of affairs (ASA) and contracts for budget and annual financial report (AFR)

Rec. 4: Implement a Software Vetting Proce

Include Data Privacy: Evaluate terms of service, privacy policy, and MOU/contract

Existing Process:

- Appropriate for the Curriculum
- Impact on technology environment including storage and bandwidth
- Hardware requirements, including any additional hardware
- License requirements/structure, number of licenses needed, and renewal cost
- Maintenance agreements including cost
- Resource update and maintenance schedule
- Funding for the initial purchase and continued licenses and

Rec. 5: (Re)negotiate Compliant Contracts

Take advantage of IL-NDPA

Exhibit E - General offer of terms from
Vendor and Originating District's Agreement

Rec. 6: Comply with Publishing Requiremen

On their website, school districts must publish:

1. Data elements of covered information that the school collects, maintains, or discloses; must be “clear and understandable to by a layperson” (105 ILCS 85/27(a)(1))
2. Written agreements within 10 business days, including data elements disclosed to the operator, business address, and subcontractors
3. Written description of the procedures that a parent may use to inspect or correct covered information and records.

Rec. 6: Comply w/ Publishing Requirements

4. Notice of breach and related details
    - Date (or range) of breach
    - Number of students involved (unless identifiable in PIPA)
    - Name of operator
5. Update published information within 30 calendar days of start of fiscal year **and** calendar year

Tools and Resources

A. Sample data sharing agreement
B. Shared contract management database
C. Reasonable security practices
D. Example policy for authorized signatories

More Information

Learning Technology Center of Illinois - https://ltcillinois.org

Webinars also available on-demand

Data Privacy Services and Resources including IL -NDPA

Cybersecurity Services and Resources

Center for Internet Security (CIS) https://www.cisecurity.org

CIS Implementation Groups

CIS CSAT

Presenters

Tom Kinane (Moderator)
Director of Technology, Elmwood Park CUSD 401
(708) 583-5707; kinanet@epcusd401.org

Chris Wherley (Speaker)
Director of Technology Services, LTC of Illinois
(217) 372-1130; cwherley@ltcillinois.org

Tony Inglese , SFO, CETL (Speaker)
Chief Financial Officer, Batavia USD 101
(630) 937-8833; inglese@bps101.net