

# SOPPA – LEGAL UPDATE AND Q&A

**Use the Chat Box or  
Q&A Feature to ask  
us questions!**

**We will start at 1:30pm!**

- **Questions and Answers with  
Attorneys at Miller, Tracy, Braun,  
Funk & Miller, Ltd.**
- @dbraun\_mtbfm – David Braun
- @bwright\_mtbfm – Brandon  
Wright

*[www.millertracy.com](http://www.millertracy.com)*

# SOPPA – LEGAL UPDATE AND Q&A

---

UNDERSTANDING SCHOOL DISTRICTS' DATA PRIVACY  
REQUIREMENTS

# OUTLINE

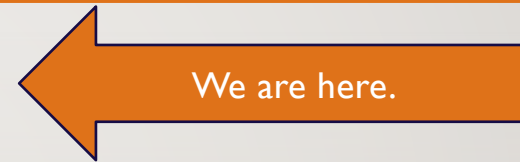
---

1. Data Privacy – Generally
2. Student Data Privacy
  - SOPPA – Generally and Definitions
  - SOPPA -- Amendments
3. Data Privacy – What Can you Do?
4. Top Ten Reminders for Cyber Security in Schools

# OUTLINE

---

## 1. Data Privacy – Generally



## 2. Student Data Privacy

- SOPPA – Generally and Definitions
- SOPPA -- Amendments

## 3. Data Privacy – What Can you Do?

## 4. Top Ten Reminders for Cyber Security in Schools

# DATA PRIVACY

---

All school employees must be concerned about protecting school district student, employee, and financial, information, such as, Social Security numbers, credit card numbers, financial information, drivers license information, and health information.

# DATA PRIVACY

---

The information legally required to be protected must be safeguarded pursuant to both the **Family Educational Rights and Privacy Act (FERPA)** and the **Children's Online Privacy Protection Act (COPPA)**, which both address the privacy and security of student's and children's information. These statutes regulate the purposeful disclosure of their information by regulating the process of acquiring parental notice and consent.

# DATA PRIVACY

---

The Federal Trade Commission published a Frequently Asked Questions publication answering questions about complying with COPPA requirements relevant to schools. It addresses schools consenting to the collection, use, and disclosure of the child's information:

<https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>

# DATA PRIVACY

---

The Department of Education has made multiple resources available at:

[studentprivacy.ed.gov](http://studentprivacy.ed.gov)

[studentprivacypledge.org](http://studentprivacypledge.org)



# OUTLINE

---

1. Data Privacy – Generally
- 2. Student Data Privacy**
  - **SOPPA – Generally and Definitions**
  - **SOPPA -- Amendments**
3. Data Privacy – What Can you Do?
4. Top Ten Reminders for Cyber Security in Schools



# DATA PRIVACY

---

Illinois has additional data protection requirements imposed in 105 ILCS 85, the Student Online Personal Protection Act (2017). These guidelines were recently amended and beginning July 1, 2021 school districts will have additional guarantees for student data protection.

# DATA PRIVACY

---

Recent Illinois legislation (effective July 1, 2021):

105 ILCS 85 – Creates many, many new mandates regarding data privacy, the use of software and applications, and requirements in the case of a data breach or improper disclosure. Requires schools to use security measures which meet or exceed “industry standards”.

# GOALS OF SOPPA

---

- Increase transparency
- Protect student data
- Protect students

# GOALS OF SOPPA

---

- The SOPPA amendment is meant to strengthen the protections of student data, referred to in the act as “covered information”.

# “COVERED INFORMATION”

---

- “Covered information” is nonpublic, personally identifiable information in any media or format that:
  - (1) an **operator gathers** through the operation of its site, service, or app, **and that personally identifies a student**; OR
  - (2) is **created or provided to an operator** by a student, a student’s parent or guardian, or an employee or agent of a school or school district in the course of using an operator’s services.

# WHAT ARE THE NEW REQUIREMENTS FOR SCHOOLS?

---

# NEW REQUIREMENTS

---

- SOPPA amendments PROHIBIT a school from selling, renting, leasing, or trading Covered Information.
- Generally (with limited exceptions) a school MUST have a written agreement to share access to student's Covered Information with anyone who is not: (1) the student's parent; (2) school personnel; (3) certain state and local officials.

105 ILCS § 85/26



# NEW REQUIREMENTS

---

- School Websites **MUST** explain how schools **collect, use, and disclose** student Covered Information. Websites must also explain to whom and why they disclose that information.
- The statute requires that these explanations be understandable to a layperson.

105 ILCS § 85/27

# NEW REQUIREMENTS

---

- School websites must also have:
  - Procedures for parents to exercise their new rights (Section 33 Rights);
  - A list of operators with whom the school has contracts, copies of the contracts, and a business address for each contractor.
  - A list of subcontractors to whom the operator discloses student Covered Information. Schools could also provide a link to this information on the operator's website.
  - A list of Covered Information violations by the school.

105 ILCS § 85/27(a)

# NEW REQUIREMENTS

---

- Covered Information breaches do not need to be included on the school's website if to the best of the school's knowledge, the number of student's involved is less than 10% of the school's overall enrollment.
- The breach occurred prior to July 1, 2021

105 ILCS § 85/27(a)(5)

# NEW REQUIREMENTS

---

- The school's website must be updated with the items previously listed no later than 30 calendar days following the start of a fiscal year and no later than 30 days after the beginning of a calendar year.
- 105 ILCS § 85/27(a)(5)

# NEW REQUIREMENTS

---

- School districts **MUST** adopt a policy for designating which school employees are allowed to enter into written agreements with operators.
- These written agreements **MUST** be posted to the school's website no later than 10 business days after entering into the agreement.

105 ILCS § 85/27(b); 105 ILCS § 85/27(c)

# NEW REQUIREMENTS

---

- School districts must make a request to an operator to delete Covered Information on behalf of a student's parent if the parent requests from the school that the Covered Information be deleted AND deletion of the Covered Information is not in violation of state and federal laws.

105 ILCS § 85/27(g)

# NEW REQUIREMENTS

---

- Schools must also implement and maintain reasonable security procedures and practices to protect student Covered Information from unauthorized access, modification, destruction, use, or disclosure.
  - These procedures and practices must be at industry standards or exceed industry standards.
- Schools must also require this same level of security from any third parties to whom the school district discloses student Covered Information.

105 ILCS § 85/27(e)

# NEW REQUIREMENTS

---

- If there is a data breach, schools **MUST** notify parents, or guardians of the affected student(s) of the following within 30 calendar days:
  - The date, estimated date, or estimated date range of the breach.
  - A description of the Covered Information that was compromised or reasonably believed to have been compromised in the breach
  - Information the parent may use to contact the operator and school to inquire about the breach.
  - The toll-free numbers, addresses and websites for the consumer reporting agencies and the Federal Trade Commission.
  - A statement that the parent may obtain information from the Federal Trade Commission and consumer reporting agencies about fraud alerts and security freezes.

105 ILCS § 85/27(d)



# NEW REQUIREMENTS

---

- A school district MAY designate an appropriate staff person as a privacy officer.
  - This Privacy Officer may also be an official records custodian under the Illinois School Student Records Act.

105 ILCS § 85/27(f)

# NEW REQUIREMENTS

---

- It is not just school districts who have new requirements under this Amendment so do:
  - Operators -- 105 ILCS 85/10; 105 ILCS 85/15; 105 ILCS 85/20
  - The State Board of Education -- 105 ILCS 85/28
- Students and Parents also have new, specifically enumerated rights. 105 ILCS § 85/33.

# OUTLINE

---

1. Data Privacy – Generally
2. Student Data Privacy
- 3. Data Privacy – What Can you Do?**
  - **Complying with SOPPA amendments**
  - **Practical tips**
4. Top Ten Reminders for Cyber Security in Schools



We are here.

# WHAT SHOULD DISTRICTS DO NOW TO COMPLY WITH **SOPPA**?

---

# (I) IMPLEMENT AND MAINTAIN REASONABLE SECURITY MEASURES.

- Illinois has some of the most stringent data protection/ data breach laws in the United States.
- Make sure the programs and operators you use are at, or exceed the Illinois industry standard for data protection.

# (I) IMPLEMENT AND MAINTAIN REASONABLE SECURITY MEASURES.

- The Illinois Learning Technology Center (LTC) has generated a list of 43 reasonable security practices school districts should implement to comply with SOPAA:
- <https://docs.google.com/document/d/1vIO6REvpqmu39xwISJTYLRrm6xOKdLeaimFYm3eYeXo/edit>

## (2) CONTACT OPERATORS TO ENSURE COMPLIANCE.

---

- Contact your vendors now to ensure they are aware of the new regulations and are ready to comply with them.

## (3) GATHER ALL INFORMATION NEEDED TO BE POSTED ON SCHOOL WEBSITES

- Prepare:
  - List of Operators used by the school district
  - List of subcontractors used by Operators (or links to this information on Operator's websites)
  - Procedures for Parents/Guardians to exercise their rights under Section 33 (these need to be posted to the website).



## (4) DESIGNATE WHO WILL BE PERMITTED TO ENTER INTO WRITTEN AGREEMENTS WITH VENDORS.

---

- The statute requires schools to determine who will be permitted to enter into agreements with vendors. Decide this now and write it down.
- Also consider whether you want to have a Privacy Officer as permitted by the statute.
  - This person could be the same as your Official Records Custodian.

## (5) DEVELOP A FORM TO SEND TO PARENTS/GUARDIANS IN THE EVENT OF A DATA BREACH

---

- While not required, it is a good idea to start thinking now about how you will interact with parents and guardians in the event of a data breach. Creating a form now will save you time in the event a breach occurs.

## (6) DATA REDACTION

---

- Mask data displayed by placing an asterisk \* in place of student information to protect student privacy. Applications may use different techniques to do this.
- On student report cards to ensure student privacy, data for groups of fewer than 10 students should have an asterisks on public report cards.

## (7) DEVELOP NEW AGREEMENTS WITH OPERATORS TO ENSURE COMPLIANCE.

- Consider developing new Operator agreements and revising existing agreements to help ensure your vendors know about and comply with SOPPA amendments.

# OUTLINE

---

1. Data Privacy – Generally
2. Student Data Privacy
3. Data Privacy – What Can you Do?
- 4. Top Ten Reminders for Cyber Security in Schools**



# **SCHOOL DISTRICT CYBER SECURITY**

## *TOP TEN LEGAL ISSUES AND REMINDERS*

---

**#1 – Using platforms that are FERPA, ISSRA, and SOPPA compliant.**

# **SCHOOL DISTRICT CYBER SECURITY**

## *TOP TEN LEGAL ISSUES AND REMINDERS*

---

**#2 – Ensuring employees understand (and that the school district enforces) the Acceptable Use Policy/Procedure.**

# **SCHOOL DISTRICT CYBER SECURITY**

## *TOP TEN LEGAL ISSUES AND REMINDERS*

---

#3 – Having a clear (and clearly understand) process (and written policy) for what apps/software are appropriate and secure.

*Who can download what, and when?*



# **SCHOOL DISTRICT CYBER SECURITY**

## *TOP TEN LEGAL ISSUES AND REMINDERS*

---

**#4 – Maintaining security when using personal devices to run school programs (email, student information system, etc.), as well as when using personal or other non-school networks.**

# **SCHOOL DISTRICT CYBER SECURITY**

## *TOP TEN LEGAL ISSUES AND REMINDERS*

---

**#5 – Instituting SOPPA-compliant operator agreements.**

# **SCHOOL DISTRICT CYBER SECURITY**

## *TOP TEN LEGAL ISSUES AND REMINDERS*

---

**#6 – Being prepared for a data breach, including clear procedures for both prevention and response.**

# **SCHOOL DISTRICT CYBER SECURITY**

## *TOP TEN LEGAL ISSUES AND REMINDERS*

---

**#7 – Protecting passwords as the valuable assets they are.**

# SCHOOL DISTRICT CYBER SECURITY

## TOP TEN LEGAL ISSUES AND REMINDERS

---

#8 – Remembering that nothing is free.

# **SCHOOL DISTRICT CYBER SECURITY**

## *TOP TEN LEGAL ISSUES AND REMINDERS*

---

#9 – Preventing the “low tech” security issues (i.e., sharing devices with spouses, children; theft of devices; etc.)

# **SCHOOL DISTRICT CYBER SECURITY**

## *TOP TEN LEGAL ISSUES AND REMINDERS*

---

**#10 – Avoiding the “one-person show”.**

## SOPPA – LEGAL UPDATE AND Q&A

---

**Use the Chat Box  
or Q&A Feature  
to ask us  
questions!**

- Questions and Answers with Attorneys at Miller, Tracy, Braun, Funk & Miller, Ltd.
- @dbraun\_mtbfm – David Braun
- @bwright\_mtbfm – Brandon Wright

*[www.millertracy.com](http://www.millertracy.com)*



Miller, Tracy, Braun, Funk & Miller, Ltd.  
316 S. Charter Street  
Monticello, Illinois 61856  
(217)-762-9416

[www.millertracy.com](http://www.millertracy.com)

[bwright@millertracy.com](mailto:bwright@millertracy.com)

[twitter@bwright\\_mtb\\_fm](https://twitter.com/bwright_mtb_fm)

[dbraun@millertracy.com](mailto:dbraun@millertracy.com)

[twitter@dbraun\\_mtb\\_fm](https://twitter.com/dbraun_mtb_fm)