Datamation Imaging Services
7700 Griffin Way
Willowbrook, IL 60527
(630) 321-0601
www.datamationis.com

Datamation Imaging Services Overview
Student Online Personal Protection Act (SOPPA) - 105 ILCS 85

BACKGROUND AND LEGISLATIVE INTENT

The intent of the SOPPA Act is to ensure that student data will be protected when it is collected by educational technology companies. Additionally, the data may be used for beneficial purposes such as providing personalized learning and innovative educational technologies. The Act requires additional safeguards to protect student data when collected by educational technology companies, and that data is used for beneficial purposes only. It is effective as of July 1, 2021.

Schools today increasingly use a wide range of online services and other technologies to help students learn. However, concerns have been raised about whether sufficient safeguards exist to protect the privacy and security of data about students when it is collected by educational technology companies.

The need for SOPPA arose out of various data breaches where personal information in an online student data system was compromised.

Datamation Imaging Services complies with SOPPA by using extensive security and privacy measures in its systems and practices to ensure the use of any content or data in its systems is protected and used specifically for the benefit of the district only.

"ED TECH"

While student tracking appears to be less publicized at the elementary and high school levels, big tech's presence in classrooms looms large. In the 2017-2018 school year, the top five digital products used in K-12 classrooms were from Google; it's a trend some call the "Google-ization of the classroom."

With the popularity of Google's G Suite for Education — a collaborative Google platform with more than 90 million users worldwide as of April 2019, according to estimates provided by the company to Teen Vogue — some worry about how the tech leviathan may be using kids' data.

In their privacy notice for the product, Google does generally lay out how it collects user data but advocates and parents are concerned about specifics.
www.teenvogue.com/story/education-technology-student-attendance-data

WHAT IS COVERED UNDER SOPPA

SOPPA covers Personally Identifiable Information (PII) or material or information that is linked to personally identifiable information or material in any media or format that is not publicly available.

Under SOPPA, a school is defined as any preschool, public kindergarten, elementary or secondary educational institution, vocational or secondary educational agency or institution. This includes private or nonpublic schools.

DISTRICT REQUIREMENTS

Below is a high-level overview of the new requirements. Please refer to the legislation for specific timelines and components of each element. School districts must:

1. Annually post a list of all suppliers/providers of online services or applications utilized by the district.
2. Annually post all data elements that the school collects, maintains, or discloses to any entity. This

information must also explain how the school uses the data, and to whom and why it discloses the data.

3. Post contracts for each operator within 10 days of signing.
4. Annually post subcontractors for suppliers/providers.
5. Post the process for how parents can exercise their rights to inspect, review and correct information maintained by the school, operator, or ISBE.
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. Designate a privacy officer to ensure compliance.
9. Maintain reasonable security procedures and practices. Agreements with vendors in which information is shared must include a provision that the vendor maintains reasonable security procedures and practices.

DATAMATION AND SOPPA COMPLIANCE

SOC Audit & Compliance

As business continues to shift into remote work, companies not only need to have easy access to their documents online but also must consider the security of those sensitive documents while being digitized. Finding a company you can trust to have the highest security standards is vital when seeking a partner to outsource processes such as mailroom, document scanning, cloud document management software, and workflow automation services.

Since 2014, Datamation Imaging Services continues to receive its SOC 2 Type 2 Report. SOC 2 Type 2 is an audit that guarantees a business process outsourcing (BPO) partner has successfully implemented and follows a set of operating procedures that ensure all documents are handled securely while in their facility. A SOC 2 Type 2 accreditation is a guarantee that both internal and external compliance guidelines are being followed accordingly.

The accreditation and audit is completed by a third-party, which audits internal processes for a period and makes sure up to five “trust principles” are being met. Those five standards for the compliance guidelines are: security, confidentiality, availability, processing integrity, and privacy. Passing the accreditation process means that a third party has verified a business is trustworthy and has a clear process in place to protect their clients’ sensitive information.

In summary, passing a SOC 2 Type II audit ensures that all customer data is handled in a secure, private, and confidential manner.

Please contact Datamation if you would like a copy of our SOC 2 report.

Safety & Privacy Protocols

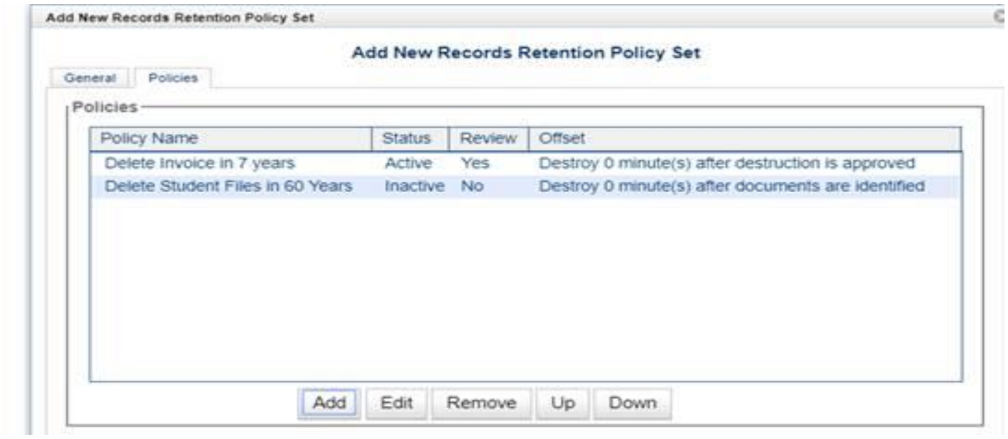
Datamation implements many practices and protocols to ensure compliance with SOPPA. These include:

- *Encryption* – All data is encrypted in transit as well as at rest. All connections to the system are secure via HTTPS. All encryption pass phrases are stored in an encrypted state as well.
- *User Sessions* - System usage is granted using a unique session ID that is passed between the system and the user. The session ID is also encrypted. User sessions are automatically disconnected after a defined period of inactivity.
- *SSL* – All external facing portals, where customers access their data, are secured via SSL.
- *Facility and Network Security* – Physical access to the facility is limited. Logical access to the networks is in place and monitored.
- *Vulnerability Assessment* – A third party performs regular vulnerability assessments using tests and monitoring to identify and resolve critical risk vulnerabilities.

- *Intrusion Protection Systems* – Administrators constantly monitor system firewalls and IPS logs to ensure system usage.
- *Mirrored/Backup* – Sites are securely backed up synchronously and in a separate location using a separate power grid.
- *Inaccessible Data* – Customer data is never exposed to a public network. It is stored on an internal secure network on a separate server from any other database or data.
- *Secure User Access* – Users must authenticate to the application with unique user IDs and complex passwords that change regularly.
- *New User Authorization* – Requests for new user accounts must come from an authorized client contact. In addition, policies exist for modifying user access and the removal of users who no longer need access.
- *Surveillance Cameras* – The Datamation facility has security cameras that monitor production activity as well as facility access.
- *Data Classification* – Policies and procedures are in place for classifying data based on its criticality and sensitivity. This is used to define protection requirements, access rights and restrictions, and set retention and destruction requirements.

Masking of Personally Identifiable Information (PII) Data
Personally Identifiable Information (PII) Data elements can be masked or hidden from users based on security settings and user rights. In addition, data can be redacted and encrypted for additional security.

Data Retention and Destruction
The system regularly and systematically tracks and destroys confidential information that is no longer required based on retention guidelines. See the following graphic for sample records destruction rules.



Add New Records Retention Policy Set

Add New Records Retention Policy Set

Policy Name	Status	Review	Offset
Delete Invoice in 7 years	Active	Yes	Destroy 0 minute(s) after destruction is approved
Delete Student Files in 60 Years	Inactive	No	Destroy 0 minute(s) after documents are identified

STRATEGY TO COMPLY WITH SOPPA

For organizations to comply with SOPPA, it is critical to designate an individual responsible for compliance, similar to that of a FOIA officer. This person must be knowledgeable of the terms of the SOPPA Act as well as put practices in place to ensure the district meets the terms of SOPPA.

For example, for years financial institutions and pharmaceutical companies have been vetting prospective vendors to ensure their system security and practices were thoroughly secure and provided appropriate levels of privacy. Many of these organizations have incorporated this into their purchasing process while also having a vendor relation and/or compliance person or department that is tasked with screening partners and vendors.

SCHOOL DUTIES*

- School districts must adopt a policy for designating which school employees are authorized to enter into written agreements with operators.
- Each school shall post and maintain on its website or, if the school does not maintain a website, make available for inspection by the general public at its administrative office:
  - An explanation of the data elements of covered information collected by the school
  - A list of operators/vendors/suppliers that the school has an agreement with
  - Procedures a parent must use to access covered information
  - A listing of any breaches realized
- After a determination of a breach of covered information maintained by the school, a school shall notify, no later than 30 calendar days after receipt or the notice or determination that a breach has occurred, the parent of any student whose covered information is involved in the breach.
- Each school 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.
- Each school may designate an appropriate staff person as a privacy officer, who may also be an official records custodian as designated under the Illinois School Student Records Act, to carry out the duties and responsibilities assigned to schools and to ensure compliance with the requirements of SOPPA.
- A school shall make a request to delete covered information on behalf of a student's parent if the parent requests from the school that the student's covered information held be deleted, so long as the deletion of the covered information is not in violation of state or federal records laws.

*Applies to public schools only

SUMMARY

In summary, Datamation Imaging has been studying SOPPA since 2019 to understand and comply with this legislation. The services and systems Datamation provide school districts an increased ability to comply with not only SOPPA but FOIA, NCLB, FERPA, and other compliance guidelines.

Please note that the data in this document are collected information and recommendations. A school district should gather final information from its legal counsel. Datamation uses, and recommends, the Tressler Law Firm as they have a team of experts in SOPPA compliance. The main contact for SOPPA at Tressler is:
Todd M. Rowe
trowe@tresslerllp.com
312.627.4180

In the meantime, it's important for school districts to learn and adopt practices to ensure that the district, and its information vendors, are in compliance with SOPPA.

Typically, districts maintain records much longer than they should. To address this, a district should:

- Review, update and approve their document retention schedule
- Purge paper and electronic files according to schedule
- Don't keep what you don't need to keep
- Archived, but retained, records should be kept in a secure and private content management system to ensure that compliance, retention and privacy guidelines are met

To view our webinar on SOPPA, please visit: https://youtu.be/8l8IRY6J0hc

Datamation Imaging Services
7700 Griffin Way
Willowbrook, IL 60527
(630) 321-0601
www.datamationis.com

Datamation Imaging Services is an award-winning and recognized document scanning and imaging system solutions provider. Datamation provides scanning services, systems and on-premise support as well as cloud-based imaging systems to more than 55 school districts.

This document was created by Jim Collins, principal at Datamation Imaging Systems. Please contact Datamation Imaging Systems if you have questions.

Datamation Imaging Systems
7700 Griffin Way, Suite B
Willowbrook, IL 60527
(630) 321-0601
www.datamationis.com