Federal Register Notice 87 FR 35250, https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies, June 9, 2022

Request for Information (RFI) on

Advancing Privacy Enhancing Technologies

Access 4 Learning Community

Larry L Fruth II, PhD
Executive Director/CEO
Access 4 Learning Community
Non-Profit Educational Technology Collaborative

Data access today is critical as major decisions on policy development, funding, program impact, and an array of other "data driven, time sensitive decisions". This is all dependent on having access to the right data at the right time. Layer on top of this is the need for control by the appropriate data stewards in the sectors the data is held within – privacy and security layers!

The *Access 4 Learning Community (A4L)* is proud to respond to *Advancing Privacy-Enhancing Technologies* request for Information. We hope that this feedback and details of our successful data management and privacy work over the past 25 years will inform the agency's understanding of how to accelerate the responsible development and adoption of PETs in a manner that promotes trust in data processing and information technologies.

The A4L Community, and its special interest group the Student Data Privacy Consortium (SDPC), is a unique, non-profit collaboration composed of schools, districts, local authorities, states, US and International Ministries of Education, software vendors and consultants. The Community is "Powered by SIF" as its major technical tool to help manage learning data simply, securely and in a scalable, standard way regardless of platform. The SDPC is designed to address the day-to-day, real-world multi- faceted issues faced when protecting learner information by setting common expectations between market providers and end users. The A4L Community has united these education technology end users and providers in an unprecedented effort to '*connect and secure effective learning ecosystems*' to give teachers more time to do what they do best: teach.

The education sector is still struggling today with privacy enforcement in general. There is a great deal of data sharing that occurs in the education environment. This included not only internal data sharing but external data sharing between local education agencies and community partners, higher education agencies, edtech vendors and researchers. A4L & SDPC are on the verge of implementing privacy enforcement technologies through the Global Education Privacy Standard (GEPS) which includes Privacy Obligation Documents (PODs). PODs are the first iteration of what we call "privacy over the wire".

A4L has had great success in assisting both schools and providers to navigate privacy issues while providing effective and secure online tools. One of SDPC's cornerstone work has been the creation of the National Data Privacy Agreement (NDPA) that is in use now in 34 states. This NDPA has successfully bridged the gap between school and provider expectations around protecting student data. The SDPC Registry currently contains over 67,000 Data Privacy Agreements between schools and vendors for close to 8,000 applications impacting 34 million students. Through all of this work, the SDPC's success can be attributed to the focus on bringing all sides together to find common ground and build from there.

The Access 4 Learning Community (A4L), linked to the Student Data Privacy Consortium (SDPC), has "moved the needle" on the marketplace addressing both interoperability and privacy controls of student data – the two must be taken collectively. These activities are global in nature but local in impact which has added to its success. Below are the areas of focus of A4L & SDPC related to data privacy;

Resource Registry

A set of “on the ground and real world” set of privacy tools allowing schools to manage and communicate on the software solutions impacting learning. The ***SDPC Resource Registry*** allows schools, districts, divisions, states, territories, and vendors to find resources, adapt them to their unique context and implement needed protections. This school-based tool allow schools to manage their applications and privacy “rules of the road” and currently is still growing with;

- 4 Countries collaborating
- 7,959 Resources in Registry Database
- 10,794 School Districts represented
- 34 States participating
- 86 Participating Vendors
- 70,000 Signed Data Privacy Agreements
- 34,000,000 Students supported by SDPC tools

National Data Privacy Agreement

The ***National Data Privacy Agreement (NDPA)*** has been developed with extensive review and comments from schools, districts, state organizations, marketplace providers and their legal representatives. It is designed to address common student data privacy concerns and streamline the educational application contracting processes for schools/districts who do not have the legal or fiscal resources and vendors who previously had to sign “one off” contracts with each of the over 13,000 US school districts. While the NDPA allows for any state specific legislative requirements, the majority of the privacy expectations are standardized and can be used by any entity as part of their Terms of Service Agreements.

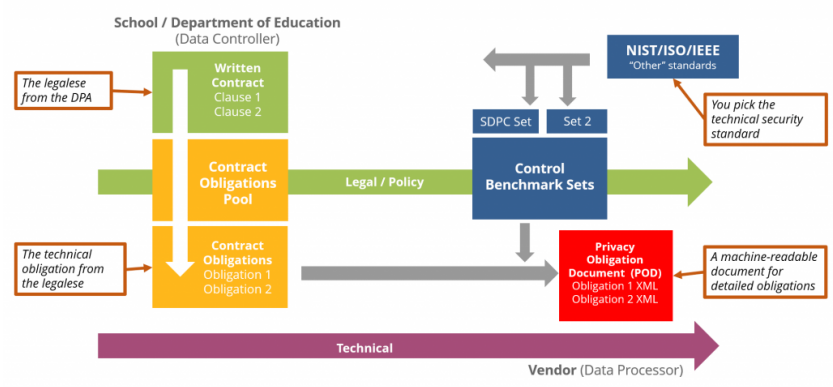
The NDPA is the first step in getting common expectations around safeguarding student privacy – but only the first step.

Global Education Privacy Standard (GEPS)

After the NDPA is established, the next step in getting common expectations around safeguarding student privacy established begs a question: What if you could automatically communicate these expectations between end users and vendors?

- Simply what you can and can't do with data
- Stipulates purpose - why you are being supplied with the data
- Legal obligations and technical benchmarks
- A green list of data elements you can access
- Data conditions (subsets of data e.g. senior years only)
- What you should do with the data if the data is no longer required
- Details of recipient of the data, who to contact if there are issues, who is handling the data, countries impacted

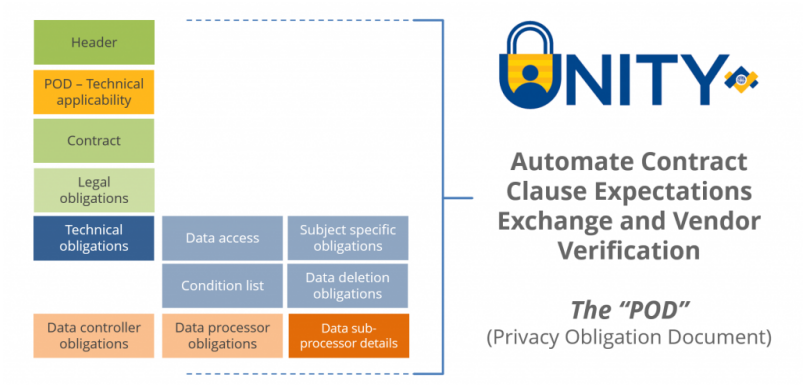
The ***Global Education Privacy Standard (GEPS)*** is designed to simplify, and in some cases automate, the software on-boarding process by aligning contract clauses to technical obligations to security standards It is designed to set common expectations between vendors and their customers.



Privacy Obligation Document (POD)

A “POD” may sound foreign to you but this one addressing student privacy expectations is not a group of killer whales – on second thought that may not be a bad idea! The SDPC ***“Privacy Obligation Document” (POD)*** is a machine readable “meta-data” document that communicates the specifics of the privacy obligations each vendor is contractually bound to and ensures acknowledgement of those obligations by the vendor before they receive data. This split-second exchange and acknowledgement provides school districts, students, and parents with the assurance that their data privacy will be protected.

PODs contain all the required privacy metadata in a standard, industry accepted format. These obligations are driven by national and state laws as well as local requirements. The obligations are driven by Data Privacy Agreements (DPAs), including the National Data Privacy Agreement, executed by and between the LEA and Provider. The DPAs contain references to all applicable state and federal laws, technical obligations and security requirements where applicable. This will ensure that privacy *and* interoperability can be managed at the same time, bringing much-needed support to districts trying to keep up with the demands of exchanging da-ta across their growing software infrastructure, while protecting the privacy of sensitive student, parent, and staff information. The POD is part of the *Global Education Privacy Standard (GEPS)* and can be “carried over the wire” utilizing the newest ‘Unity’ SIF Specification, developed by the A4L Community.

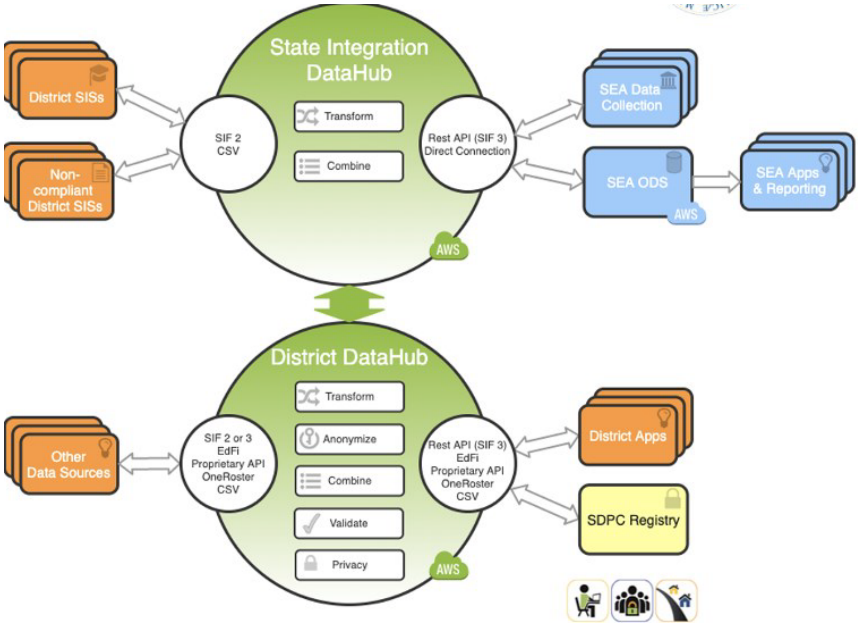


Data Hub Project

The Data Hub is a project to create a connected and secure ecosystem, balancing the needs of privacy and interoperability in one place. The main goals of the project are to:

- Align to open data standards
- Provide an easy-to-manage toolset for districts to handle connecting their many software systems
- Leverage existing state data connections
- Meet vendors “where they are” _to avoid external dependencies for project success
- Handle privacy and interoperability at the same time, in one system

The Data Hub project is also the first proof of concept for the use of PODs to enforce privacy obligations. No data is exchanged until there is an acknowledgement of the POD obligations by the receiver of the data. THis ensures that the data is only being shared with entities that have acknowledged/certified their data privacy obligations.



Standardized Infrastructure

Almost all organizations that develop data models for their particular members/marketplace vertical do not provide an infrastructure for “data over the wire”. They allow for developer/user choice for moving the data between applications or in some cases provide suggested guidance. This does not allow for the full usage of PETs.

In 2014, the Access 4 Learning Community released an open standard infrastructure, SIF 3.0, leveraging a REST based approach to data exchange. The key contribution of this release was to define, coordinate and standardize the ways in which a RESTful educational service can be accessed securely, robustly, and in real time by multiple RESTful clients. This openly developed and freely accessible infrastructure blueprint is separate from any data model defining the payloads it carries, which means it can be used to support many different data models in many different locales such as being down currently with data models from Australia, New Zealand and North America and soon between other Standards Developing Organizations (SDOs) across various verticals. Designed to be separate, but support these data models, the standardized infrastructure can carry any data model and is unique in that it:

- Addresses privacy controls
- Is scalable for use
- Contains security controls
- Has been load tested
- Has an associated certification program

The benefits for a standardized infrastructure used between all data sectors in that it would:

- Pave the way for plug-and-play interoperability between sectors
- Empower meaningful validation and quality control
- Accelerates development.
- Allow for greater marketplace choice.
- Provides functionality clarity.
- Lowers barriers between sectors and geography

Summary

Access 4 learning and the Student Data Privacy Consortium have done more in the education sector to address operational privacy issues than any other organization. A4L has laid the foundation for secure data exchanges with over 20 years experience producing, publishing and implementing data interoperability standards. SDPC has laid the groundwork for addressing the legalities of data shAring across the entire educational ecosystem.

Now that A4L and SDPC have combined their expertise to address the issue of enforcing data privacy obligations from a technical perspective, we are well positioned to have an even larger impact on the education sector. The Global Education Privacy Standard and Privacy Obligation Documents are examples of Privacy Enforcing Technologies that will eventually become common practice in education. These PETs can be replicated across many sectors.