Privacy Obligation Documents (PODs): A Deeper Dive

Mike Reynolds, Cedar Labs and Lisa Waters, Cambridge Public Schools
Introductions

Mike Reynolds
A4L Global Infrastructure Co-Lead
Cedar Labs

Lisa Waters
Digital & Creative Services Manager
Cambridge Public Schools &
SDPC Website Developer
**What is a POD?**

**POD** (Privacy Obligations Document) is a standards agnostic machine readable document that contains all data privacy requirements including contract clauses, privacy obligations, technical control benchmarks, and other control metadata.

- Every POD is **unique** to the relationship between:
  - District
  - Vendor
  - Application
  - Place in time

- Every unique POD based upon above query elements will be assigned a unique identifier; **POD-ID**
  - Any change to a POD (added clause, date change, etc.) will create a new POD and new POD-ID

- POD-IDs can be used to convey obligations within PODs without having to exchange the entire POD.
How is a POD generated?

GEPS Manager in the SDPC Registry

Maps DPA to data elements
(Done for every DPA)

Standard NDPA done Nationally

State DPA Exhibit G Clauses

Unique Exhibit H Clauses

- **DPA** = Data Privacy Agreement
- **NDPA** - National Data Privacy Agreement
- **GEPS** = Global Education Privacy Standard
- **SDPC** = Student Data Privacy Agreement
- **Exhibit G** = Supplemental State Terms
- **Exhibit H** = District/Vendor Specific Edits
How is a POD generated? (continued…)

Welcome to the GEPS Custom POD Wizard. To get started creating a custom POD, please complete the following steps.

**SELECT a State**

**Your Custom PODs**

There are no custom PODS.

Get Started! Name this Custom POD

Enter a Name

Continue >>
How is a POD generated? (continued…)

SELECT an agreement type

- National Agreement

Your Custom POD, test includes: National Clause Set

I am finished creating this POD. View Custom POD >>

(+) ADD State Specific Exhibit G Groupings

(+) ADD Exhibit H Groupings

There are no Exhibit Hs available.
How is a POD generated? (continued…)

Your Custom POD, Test Includes: National Clause Set + MA Obligations V1.0 (Exhibit G)

I am finished creating this POD. View Custom POD >>

(+) ADD State Specific Exhibit G Groupings

(-) DELETE additional grouped clauses

There are no Exhibit Hs available.

Name

MA Obligations V1.0 (Exhibit G)
How is a POD generated? (continued…)

1.1 Purpose of POD. The purpose of the POD is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data.

The school will provide the list of data included in the contract to the provider. This will include data shared with the provider and data created by the provider’s service.

1.2 Student Data to be Provided. In order to perform the Services described above, the LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as Exhibit "A".

The definitions of terms are included as Exhibit C.

1.3 CIPA Definitions. The definition of terms used in this CIPA is found in Exhibit "C". In the event of a conflict, definitions used in this CIPA shall prevail over terms used in any other written, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies, etc.

All student data transmitted to the Provider, as well as any modifications made to such data, or any student data created by the service will remain the property of the school. All rights to this data, including any intellectual property rights, shall remain with the school, not the Provider. The Provider is considered a School Official under FERPA.

1.1 Student Data Property of LEA All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this CIPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data, shall remain the exclusive property of the LEA. For purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA, as it pertains to the use of Student Data, not modifying the above.

In the event a parent requests to review or correct erroneous information in the data maintained by the Provider, the Provider shall respond in a reasonable time frame, not more than 45 days. From the date of the request from the school, such request may only come from the school. If a parent contacts the Provider directly, they should be referred back to the school.

1.2 Parent Access. The data requested by the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data, correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner and no later than forty-five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner. The Provider shall report to the LEA or the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent or student contacts the Provider to review any of the Student Data accessed pursuant to the services, the Provider shall refer the parent or student to the LEA, who will follow the necessary and proper procedures regarding the requested information.

When requested by the school, the Provider will transfer, or provide a mechanism for the school to transfer, student generated data to a separate account created by the student.

1.3 Separate Account. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

If the Provider is approached by Law Enforcement to provide access to student data the Provider will notify the school in advance of any disclosure of student data.

1.4 Law Enforcement Requests. Should law enforcement or other government entities ("Requesting Party") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a completed disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

The provider will establish written agreements with all sub-processors addressing all obligations included in the data privacy agreement. The agreements must hold sub-processors in the same level of student data.
Purpose of DPA. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LBA. Provider shall be under the direct control and supervision of the LBA, with respect to its use of Student Data.

Clause 1: Privacy

The provider will provide a list of data included in the contract to the provider. This will include data shared with the provider and data created by the provider’s service.

Clause 2: Data to be Provided

In order to perform the Services described above, LBA shall provide Student Data as identified in the Schedule of Data, attached hereto as Exhibit B.

Clause 3: Definitions

- Data: The definition of terms used in this DPA is found in Exhibit A. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the service agreement, terms of service, privacy policies, etc.
- Provider: The entity performing the services described in this DPA.
- School Official: All student data transmitted to the provider, as well as any modifications made to such data, or any student data created by the service will remain in the property of the school. All rights to this data, including any intellectual property rights, shall remain with the school, and not the provider. The provider is considered a School Official under FERPA.

Clause 4: End User License Agreement

The provider shall protect the confidentiality and security of your Student Data, as well as any modifications made to such data, or any student data created by the service will remain in the property of the school. All rights to this data, including any intellectual property rights, shall remain with the school, and not the provider. The provider is considered a School Official under FERPA.
As part of SIF Infrastructure Specification 3.6 Community Review the following updated resources are available to members.

**POD Spreadsheet:**
http://specification.sifassociation.org/Implementation/Infrastructure/temp/pods.xlsx

**POD Normative:**
http://specification.sifassociation.org/Implementation/Infrastructure/3.6/PrivacyServices.html#obj:Pod
End-to-End Privacy Solution?

Automate Contract Clause Expectations Exchange and Vendor Verification

The "POD" (Privacy Obligation Document)

- Header
- POD – Technical applicability
- Contract
- Legal obligations
- Technical obligations

Data access
Subject specific obligations
Condition list
Data deletion obligations
Data controller obligations
Data processor obligations
Data sub-processor details

May 17-19, 2023
Adaptations for POD support

- The POD is a Standard Agnostic specification
- SIF 3 Infrastructure was extended to support
  - POD Sharing and Administration
  - Basic Gatekeeping
  - (Limited) Enforcement Potential
Infrastructure Support

Vendor Conversations

- RESTful Bridge to Adoption
- Flat File Bridge to Adoption
  - Use Gatekeeping and Handshake facility of SIF Infrastructure
Flat File Adapters

- Can’t touch existing “heavy lifting”
- Add value for both Providers and Consumers
- Flexible (e.g. allow for some future proofing)
- Scalable (must be automated not manual processing)
Infrastructure Support

Flat File Blueprint | Simple Gatekeeper

- Version ###
- Service X
- Service Y
- Effective Date

Traditional ETL Pipeline

CSV → SFTP → Database
Infrastructure Support

Flat File Blueprint | Gate Keeper + Audit Trail

Out of band exchange

- Version ###
- Service X
- Service Y
- Effective Date

Pod

POD

JOb

POD Status
- Delivered
- Picked Up
- Processed
- Expunged

SDPC Registry

Traditional ETL Pipeline

SFTP

CSV