



Access 4 Learning
Community

Powered by:  **SIF**

Simple. Secure. Scalable. Standard.



Student Data Privacy Consortium



Unifying Student Data Privacy with Data Interoperability

~ the Unity Blueprint ~



Access 4 Learning
Community

Powered by:  **SIF**

Simple. Secure. Scalable. Standard.



Student Data Privacy Consortium



Agenda

Risks

How do we decrease the risk of data “leakage” when so much data is flying around our digital ecosystem?

Requirements

How do you convey privacy legal requirements to marketplace providers?

Standards

Is there a way I can address/enforce privacy requirements through openly developed technical standards?

Implementation

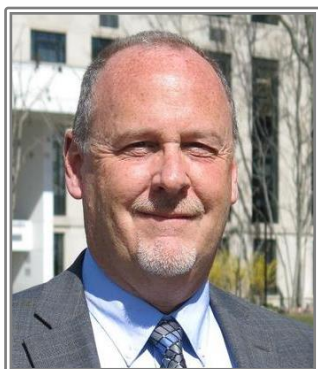
How are your vendors implementing privacy requirements in the real world?

“Next”?

Who are we?



Steve Smith



CIO

Cambridge Public Schools, MA

ssmith@cpsd.us

Ben Silberglitt



CSO

Cedar Labs

Ben.Silberglitt@cedarlabs.com

Jeff Simons



CIO

WSIPC

jsimons@wsipc.org

John Lovell



Technology Director

A4L Community

jlovell@A4L.org

Level Setting.....



Access 4 Learning Community

- Non-Profit started in 1997
- Membership driven with schools, districts, regional and state agencies, other professional organizations and marketplace providers in the Community
- Collaboratively develops technical blueprints (SIF) for data to move safely and securely between school software applications
- Used in every state and Communities in 4 Countries
- <https://www.A4L.org>

Student Data Privacy Consortium

- Special Interest Group of A4L Community started in 2015
- Maintains its own governance, oversight and resource support
- 31 State Alliances representing over 9,000 schools and 75+ vendors
- Addressing privacy “Pain Points”
- Working collaboratively on projects, tools, effective practices and partnerships for “tactical student data privacy”
- <https://sdpc.A4L.org>



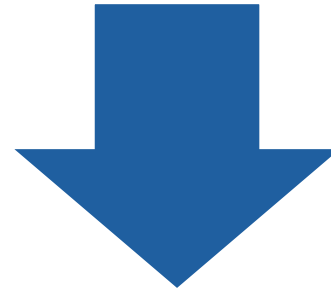
How do we decrease the risk of data “leakage” when so much data is flying around our digital ecosystem?

Don't worry, we are here to help you modernize your environment....

Its Not “One or the Other”!



Student Data Privacy Consortium



No One Gets It!



Everyone Gets It!



A4L & SDPC: Supporting the “New School” Role?



*“Leadership
and learning
are
indispensable
to each other.”*

John F. Kennedy

- Increased interoperability without the inclusion of privacy requirements equals increased **RISK**.
- **BOTH** data sharing and privacy parameters must be identified and communicated.
- Learning institutions often do not have the human and/or fiscal resources to successfully address both parameters
- A4L and SDPC is the **ONLY** community collaboration that is addressing **BOTH** interoperability and privacy

The A4L and SDPC Communities will help schools and marketplace providers establish “connected, secure and effective K12 ecosystems”



How do you convey privacy legal requirements to the marketplace providers?

...Clauses, Obligations, & Benchmarks, Oh My!

Linkages for Privacy.....



Agreement CLAUSES

Main FERPA Exception:
School officials with legitimate educational interest – a data privacy agreement is a must!

National Data Privacy Agreement: Standardize the DPA Format so it looks the same by Identifying common legal clauses across jurisdictions

Example: *"Upon written request from the LEA, Provider shall dispose of or provide mechanism for the LEA to transfer Student Data..." (IV, 6)*

Technical OBLIGATIONS

How product providers will technically implement the agreement **CLAUSES** to adhere to customer requirements

Addressing the “legalese” of the **CLAUSES** to “technical effective practices”.

Example: *“Acknowledge and register adequate signals for for the interpretation, operational execution and notice of deletion request”*

Standards BENCHMARKS

Technical Standards establishing agreed principles or criteria so that their users can make reliable assumptions about technical **OBLIGATIONS**.

A technical standard is an established norm or requirement in regard to technical systems.

Example: *“Execute delete requests and subsequent notice (to controller and/or subject) under reasonable timeframes and in accordance to retention schedules defined by purpose in the Service Agreement.” (NIST)*

National Data Privacy Agreement (NDPA) v1



NDPA Feature	Description
New Format	Designed to provide everything the reader needs to know on page 2
Section	Cover Page and Directive
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 Data - E = General Offer of Terms - F = Data Security Requirements - G = Supplemental State Terms - H = Additional Terms or Modifications





Is there a way I can address and enforce privacy requirements through openly developed technical standards?

Yes!

Linkages for Privacy.....



Agreement CLAUSES

Main FERPA Exception:
School officials with legitimate educational interest – a data privacy agreement is a must!

National Data Privacy Agreement: Standardize the DPA Format so it looks the same by Identifying common legal clauses across jurisdictions

Example: *"Upon written request from the LEA, Provider shall dispose of or provide mechanism for the LEA to transfer Student Data..." (IV, 6)*



Technical OBLIGATIONS

How product providers will technically implement the agreement **CLAUSES** to adhere to customer requirements

Addressing the “legalese” of the **CLAUSES** to “technical effective practices”.

Example: *“Acknowledge and register adequate signals for for the interpretation, operational execution and notice of deletion request”*



Standards BENCHMARKS

Technical Standards establishing agreed principles or criteria so that their users can make reliable assumptions about technical **OBLIGATIONS**.

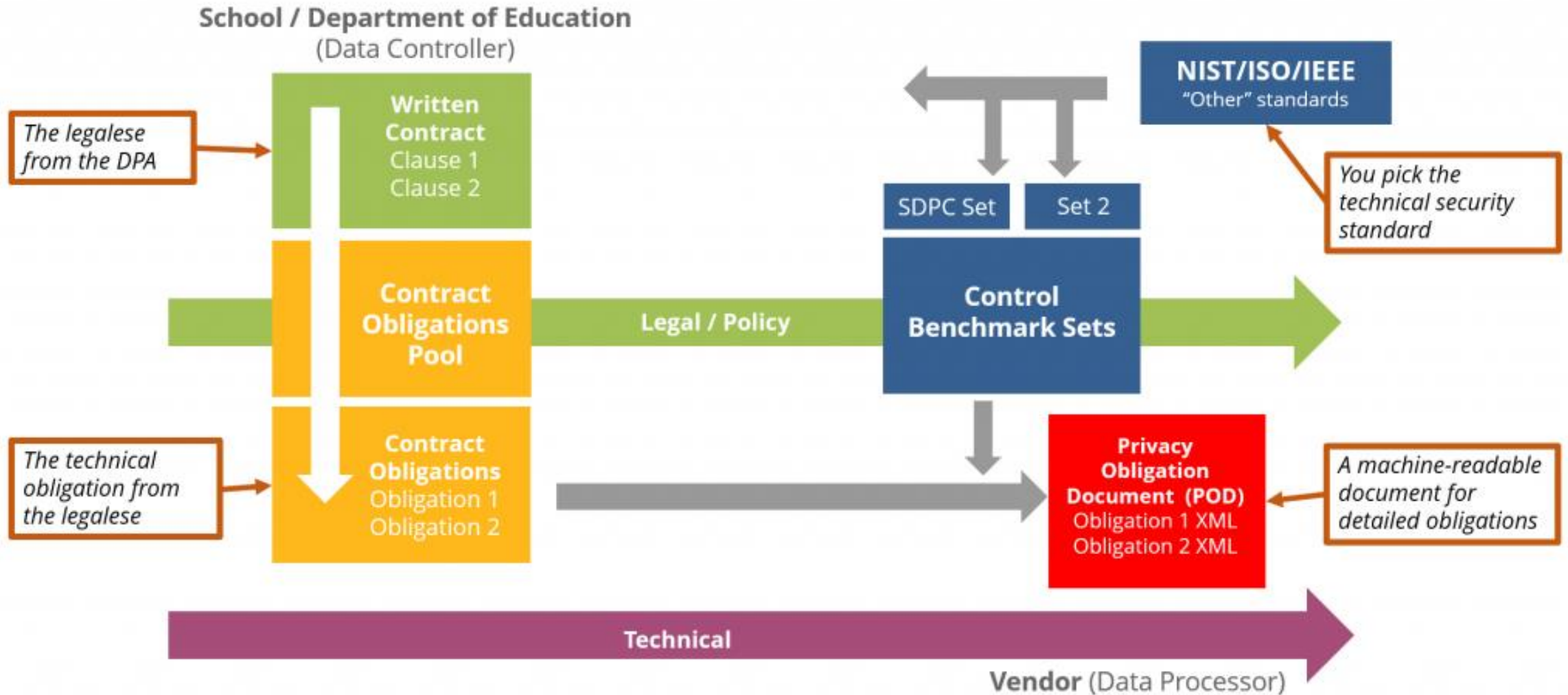
A technical standard is an established norm or requirement in regard to technical systems.

Example: *“Execute delete requests and subsequent notice (to controller and/or subject) under reasonable timeframes and in accordance to retention schedules defined by purpose in the Service Agreement.” (NIST)*

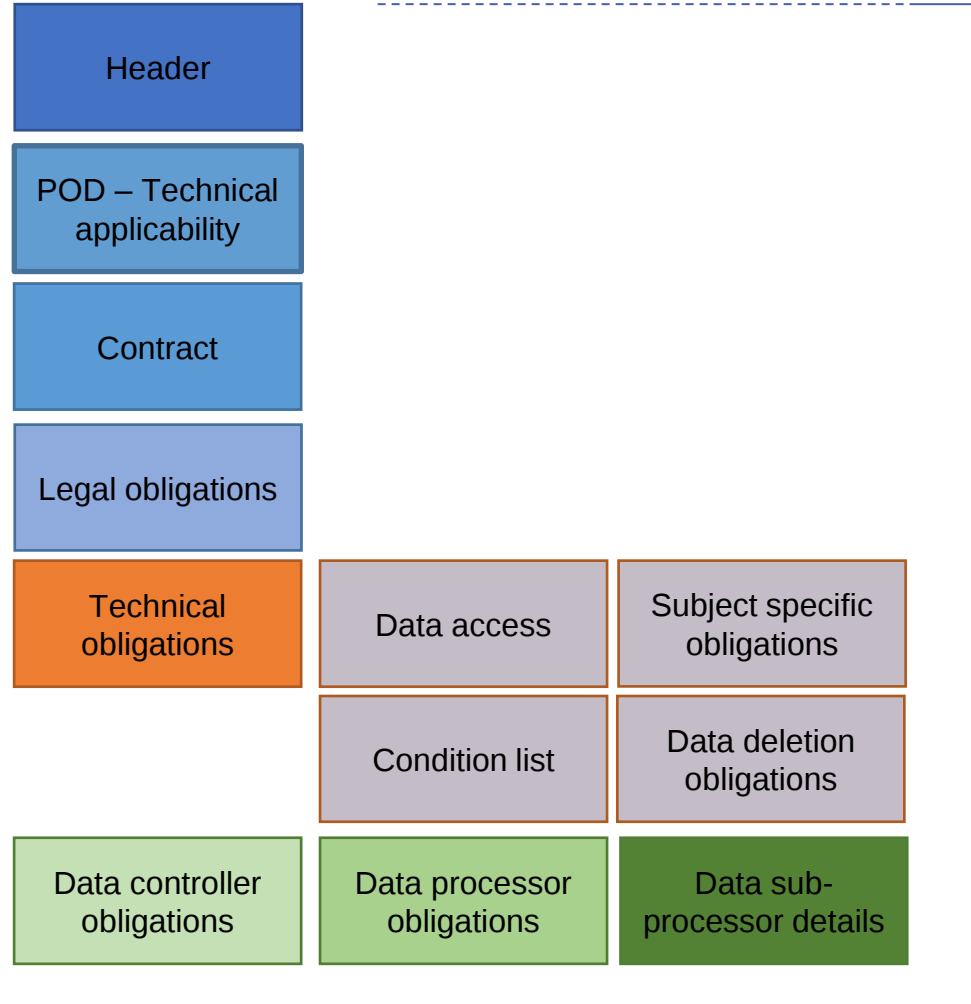
File Edit View Insert Format Data Tools Add-ons Help All changes saved in Drive

	A	B	C	D	E
1			Clause	Obligation/Benchmark	Title
2				Destruction of Data. Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA's designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.	
3	V.1.b			OBLIGATION	Maintain an accessible practice of destruction of data with adequate reference to definitions and policies in presenting general data retention guidelines
4			<i>Benchmark</i>	Present a data retention policy which identifies data classifications, retention schedule, and destruction process in line with data classification level.	Alignment to Known Standards NIST 800- 53 (Rev. 4) System And Information Integrity Control Family SI-12 Information Handling and Retention. National retention standards can be found here https://www.archives.gov/files/records-mgmt/grs/trs29-sch-only.pdf for specific local standards (state, provinces, territory) see the local department responsible for data retention sched
5			<i>Benchmark</i>	Properly address and agree to the definition of delete [link. Talk to making unrecoverable, discuss extent such as backups/etc].	NIST 800-88 R1 are the data delete definition guidelines to be referenced against the legal requirements for retention
6				OBLIGATION	Acknowledge and register adequate signals for the interpretation, operational execution, and notice of deletion requests.
7			<i>Benchmark</i>	Destroy data as a result of a delete request in accordance with Service Agreement... at end of service, at end of purposeful use, when no longer required, when unlawfully collected or requested under legal directive, where guardian has objected, where District is not clear controller of subject data, or where Parental consent has not been obtained for under 14.	NIST 800- 53 (Rev. 4) System And Information Integrity Control Family SI-12 Information Handling and Retention. National retention standards can be found here https://www.archives.gov/files/records-mgmt/grs/trs29-sch-only.pdf for specific local standards (state, provinces, territory) see the local department responsible for data retention sched
8			<i>Benchmark</i>	Execute delete requests and subsequent notice (to controller and/or subject) under reasonable timeframes and in accordance to retention schedules defined by purpose in the Service Agreement.	NIST 800- 53 (Rev. 4) System And Information Integrity Control Family SI-12 Information Handling and Retention. National retention standards can be found here https://www.archives.gov/files/records-mgmt/grs/trs29-sch-only.pdf for specific local standards (state, provinces, territory) see the local department responsible for data retention sched
9			<i>Benchmark</i>	Identify which data or data types are to be returned, destroyed, and anonymized during delete requests .	NIST 800- 53 (Rev. 4) System And Information Integrity Control Family SI-12 Information Handling and Retention. National retention standards can be found here https://www.archives.gov/files/records-mgmt/grs/trs29-sch-only.pdf for specific local standards (state, provinces, territory) see the local department responsible for data retention sched
10			<i>Benchmark</i>	Demonstrate/evidence the execution of a delete request process at a data subject level while maintaining compliance.	NIST 800- 53 (Rev. 4) System And Information Integrity Control Family SI-12 Information Handling and Retention. National retention standards can be found here https://www.archives.gov/files/records-mgmt/grs/trs29-sch-only.pdf for specific local standards (state, provinces, territory) see the local department responsible for data retention sched
11				OBLIGATION	Recognize and plan for limits of data destruction
			<i>Benchmark</i>	Showcase any and all exception practices where information might be retained in accordance with	

Global Education Privacy Standard (GEPS)



Unity Enabling Privacy Expectations



Automate Contract Clause Expectations Exchange and Vendor Verification

The “POD”
(Privacy Obligation Document)

Enabled in global SIF Infrastructure



Privacy Support

Built in privacy support, based on GDPR and Student Data Privacy Consortium (SDPC) needs



SIF 3 infrastructure

The REST infrastructure that starts simply and scales easily. Includes JSON conversion and is designed for the cloud. Performance is 'real' (ask Massachusetts!)



Built on SIF 2.x Specification

Leverage existing knowledge and software. Robust, familiar data model.



xPress Roster

Modular API design, most robust roster standard in marketplace. Compliments the Unity Data Model... you can start with xPress Roster and scale up!

Individual Education Plans (IEPs)

1st standardized API for IEPs
Detailed/extensive objects
Ready for 'in District' use and Student transfers



Supporting Documentation

EDFacts Mapping, xPress Roster Mapping & Unity Adoption Guidebook - designed to help from concept to integration plan and API design all the way to development.



Mappings Release

August 2020



CEDS

Added EDFacts & xPress Roster CEDS Mappings in the latest release.
2833 Unity fields mapped to CEDS

EDFacts

Working towards developing a CEDS Integrated Data Store (IDS) Connector for EDFacts Reporting



API Documentation

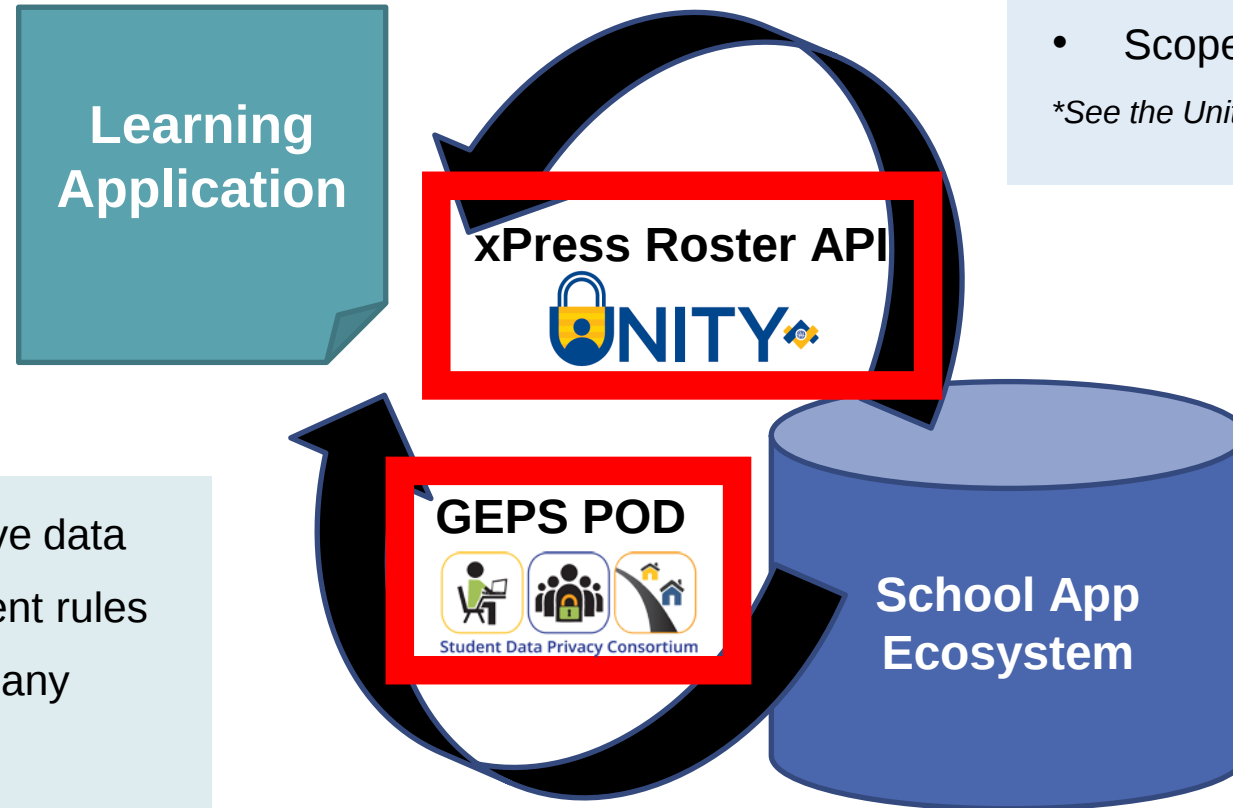
... coming soon!
Follows industry standard API best practices & increases accessibility to all developers



Example: Application Rostering



Unity Specification and Privacy Requirements – Limiting Risk



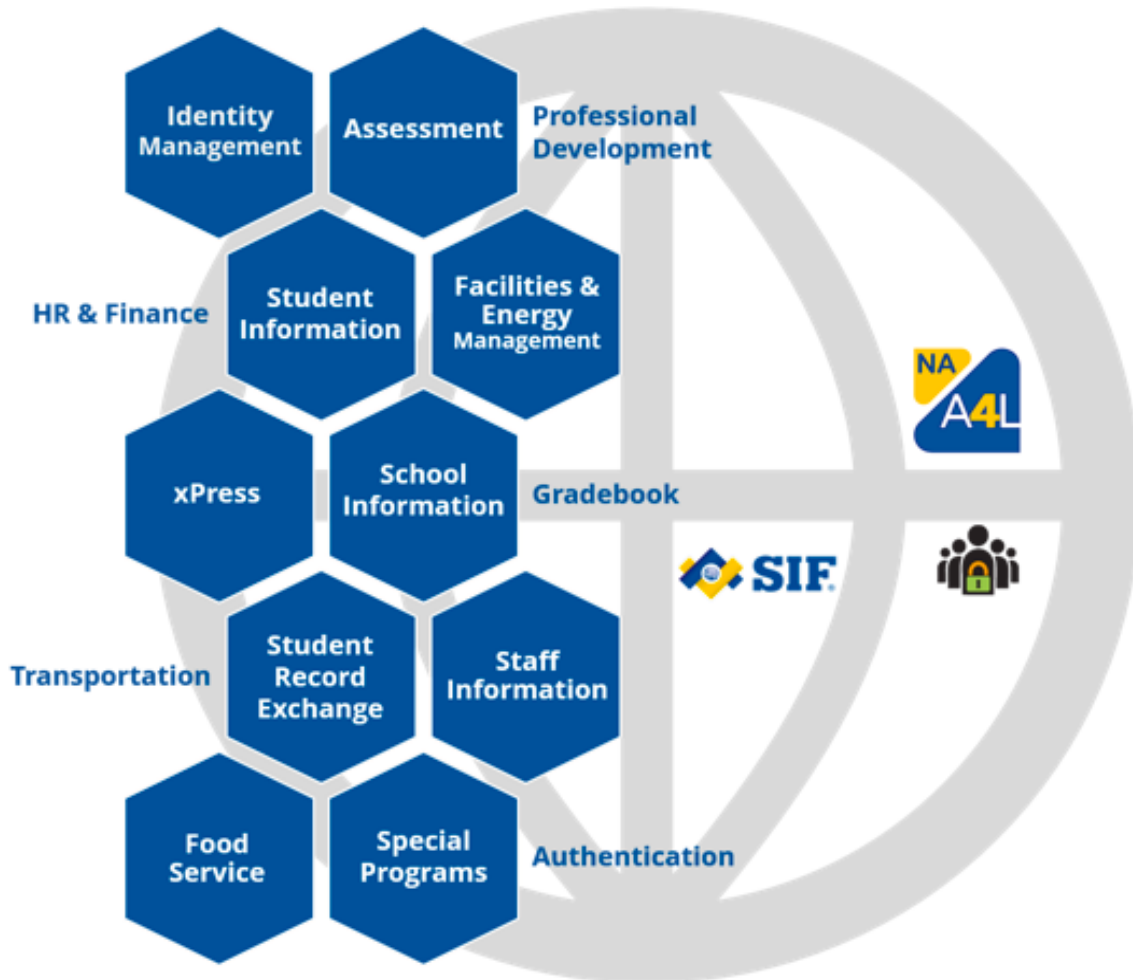
- Pre-Provision Accounts
- Scope based on Course Enrollment*

**See the Unity Adoption Guidebook pages 26 – 29*

- Automatically filter sensitive data
- Automatically set retainment rules
- Know who to contact with any problems

**xPress Roster example:
<https://xpressapi.org/user-examples/xpress-roster/>*

Common Uses for Unity...



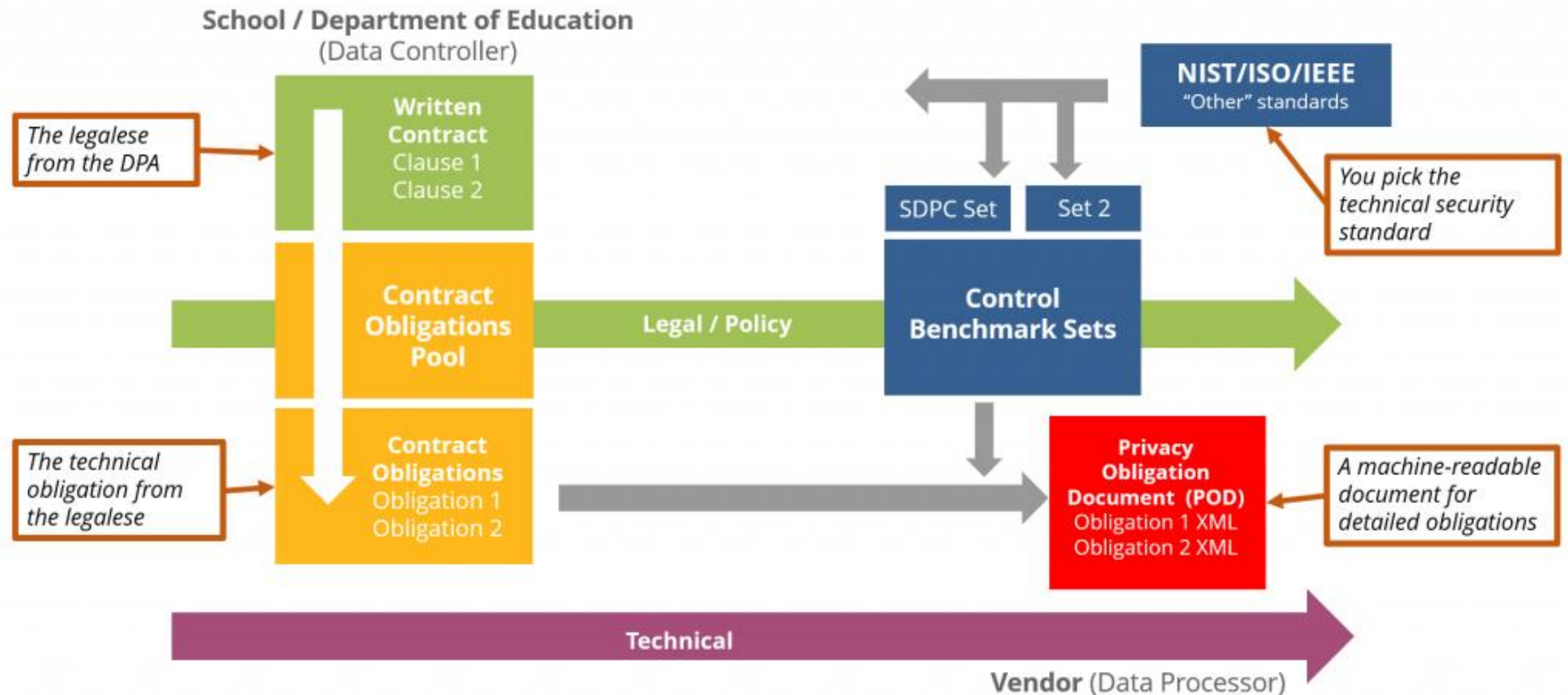
- **Library:** Access and Fines
- **Lunch System:** Access and Account Status
- **Transportation:** The perfect address for every situation
- **Reporting:** Federal and often by State
- **Attendance:** By period or as a summary
- **Assessments:** Administration, recording and between app movement



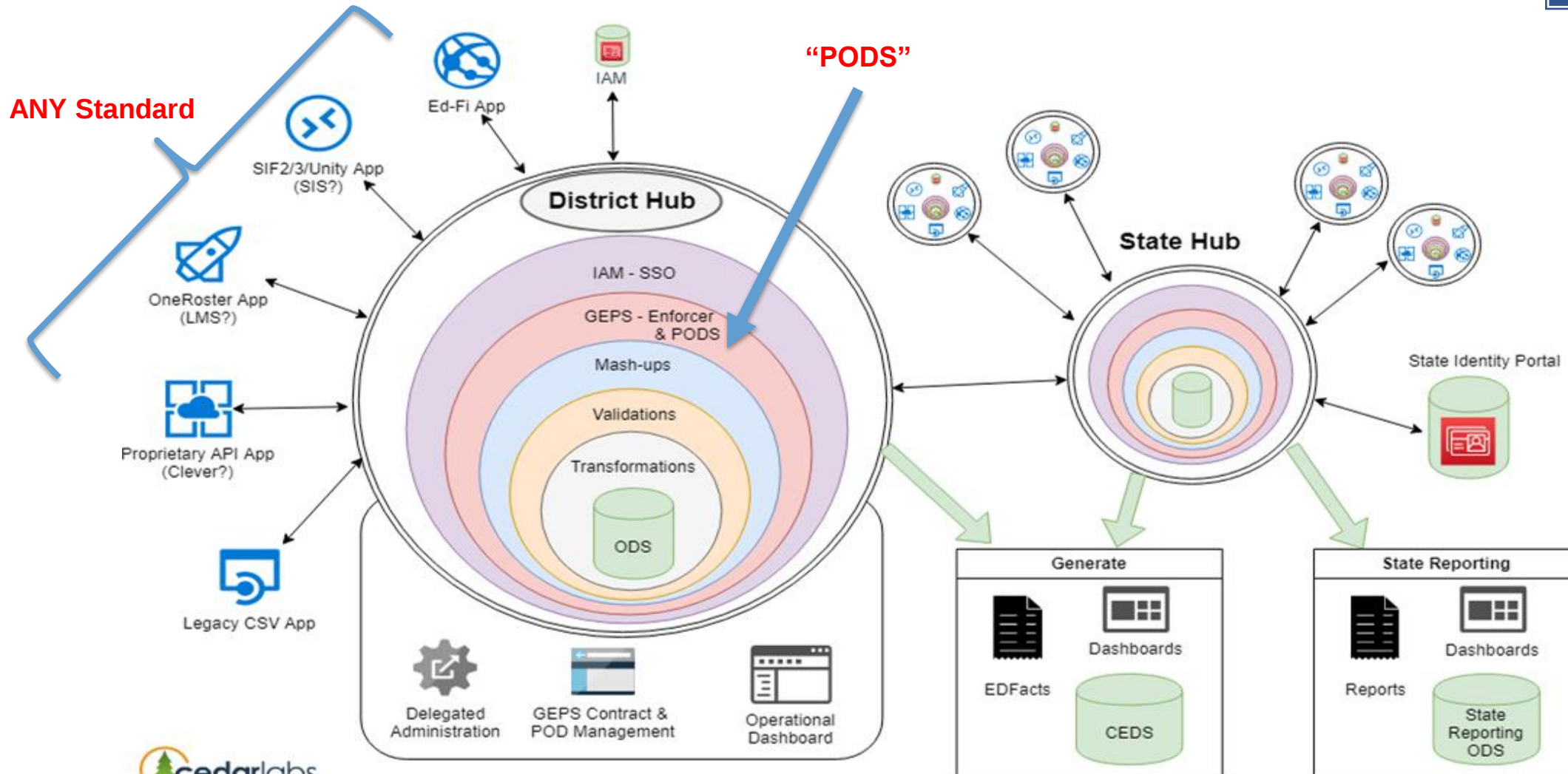
How are your vendors implementing the privacy requirements in the real world?

The Technical Blueprint.

Global Education Privacy Standard (GEPS)



“Learner Centric” MA Data Hub Service



MA Data Hub



- Manage and filter *what* data and *which* students are sent to each vendor
- Transform and anonymize data
 - Connect noncompliant vendors
 - Go beyond “cookie cutter” rostering
- Integrated, one-stop management of data integration and privacy



Keebler, Newell - Grade 03
School(s) Enrolled: Dolorem Academy (02480003)



Software Systems Enrolled:

 = Data Hub Connection  = DPA on file with SDPC

Brain Bits



 Software System Access

What Data?

SCHOOL & DISTRICT

Local Id (School)

STUDENT INFORMATION

English Proficiency Code First Name Gender Gifted Talented
Grade (Student School Enrollment1) Last Name Local Id (Student Personal)
School Name (Student School Enrollment1)
School State Province Id (Student School Enrollment1)

CLASS ROSTER
INFORMATION

Course Code Course Section Code Course Title

STAFF INFORMATION

First Name Job Function Code (Staff Assignment1) Last Name Local Id (Staff Personal)
School Name (Staff Assignment1)

 Privacy and Security Obligations

Privacy Obligations

 All Privacy Obligations

Data Security
Requirements

Assess security controls Audit logs Limit failed logins Password complexity
Protect system media Sanitize equipment Sanitize system media

Privacy Report

Don't miss...



WEBINAR:

FEBRUARY 24, 2021

REGISTER:

<https://bit.ly/3oJmd4P>

Connecting and Securing in the Real World: The MA Data Hub Solution

This pilot project was designed to leverage the MA Department of Elementary and Secondary Education's (DESE) state data collection & Cedar Labs' "hub and spoke" architecture to branch a state reporting data connection and create an easy-to-manage data integration platform for school districts. MA DESE, and Cambridge Public Schools are leveraging the existing state data connection to branch the flow of data not just for state reporting, but to also provide additional value add services such as standards agnostic rostering and privacy enforcement.

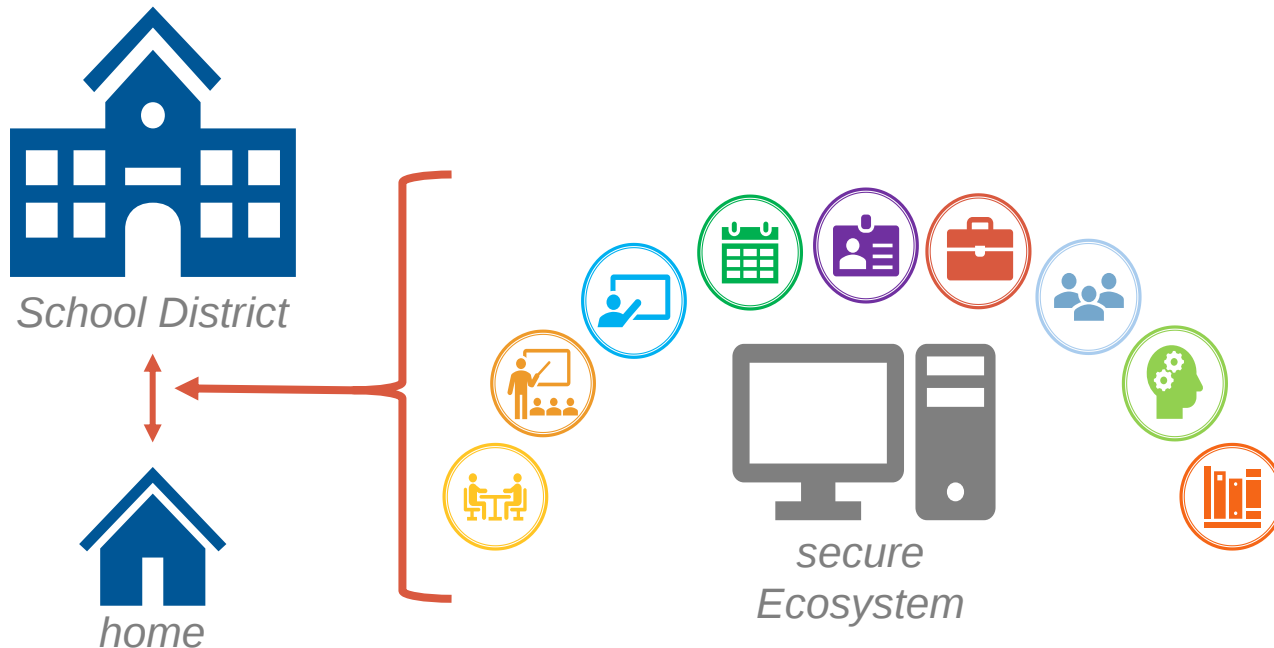
*****use promo code **Unity-Feb2021** during checkout to get 'free' registration*****

Connecting and Securing Effective Learning Ecosystems™



CIOs MUST Address

- ✓ Application Vetting
- ✓ Contracting Process
- ✓ App Management
- ✓ Integration
- ✓ Secure Data Exchange
- ✓ Quality Control
- ✓ Professional Learning

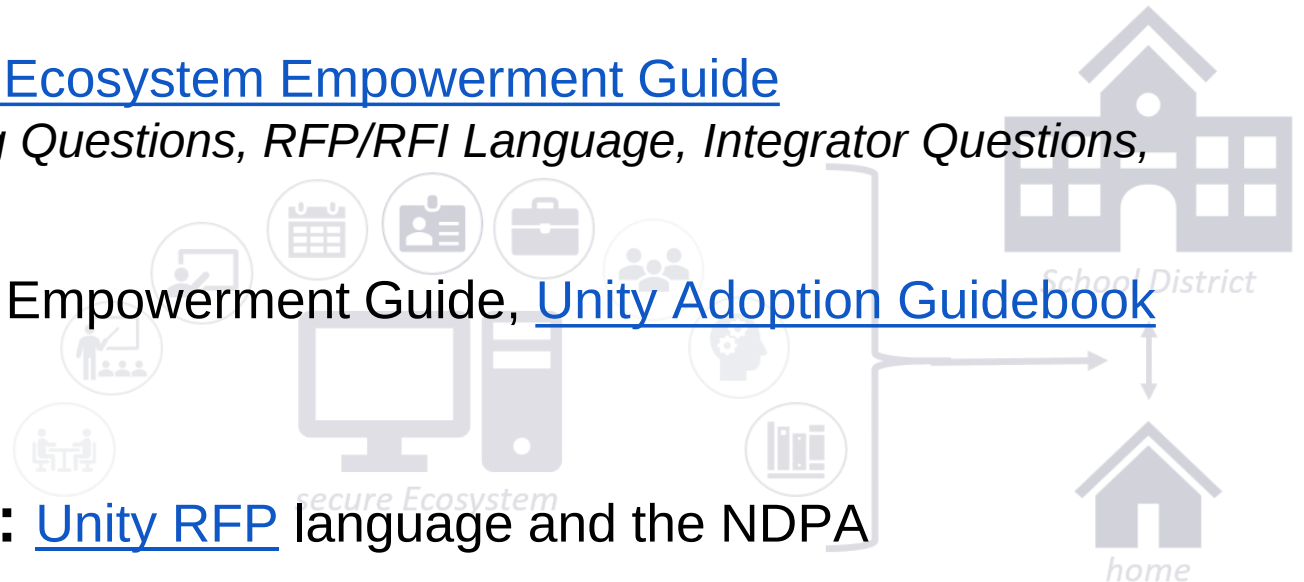


“Connecting and Securing Effective Learning Ecosystems™”

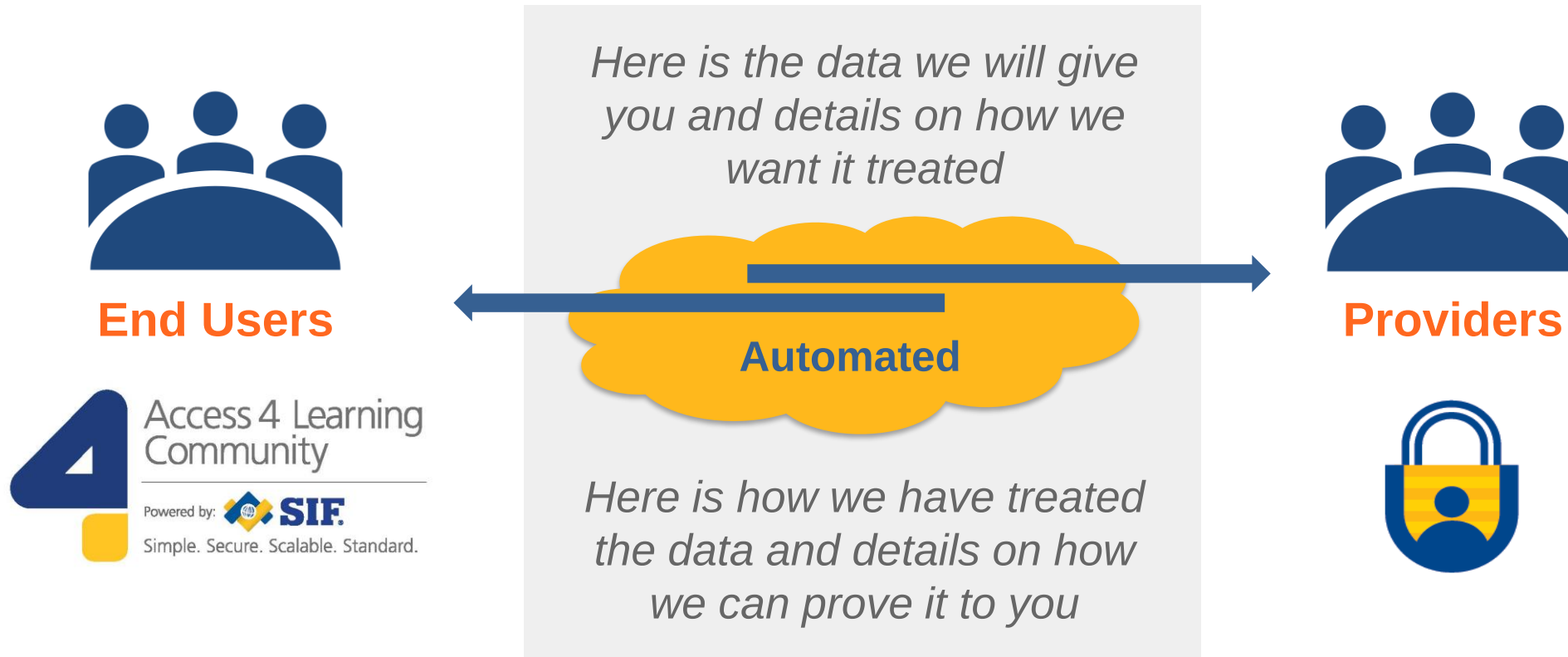


Are You Looking for Support In:

- ✓ **Application Vetting:** SDPC Resource Registry Workflow Tool
- ✓ **Contracting Process:** [National Data Privacy Agreement](#) (NDPA) *as part of Terms of Service*
- ✓ **App Agreement Management:** [SDPC Resource Registry](#)
- ✓ **Integration:** [Getting Started with Unity](#), [Ecosystem Empowerment Guide](#)
(Guide includes Implementation Planning Questions, RFP/RFI Language, Integrator Questions, Vendor Readiness Scoresheet)
- ✓ **Secure Data Exchange:** Ecosystem Empowerment Guide, [Unity Adoption Guidebook](#)
- ✓ **Quality Control:** [Certification Registry](#)
- ✓ **Leverage the Community's Work:** [Unity RFP](#) language and the NDPA



The Result: Common Expectations!



***Increased interoperability without the inclusion of privacy requirements = increased RISK.
Both data sharing and privacy parameters must be identified and communicated!***

Takeaways.....and Call to Action!

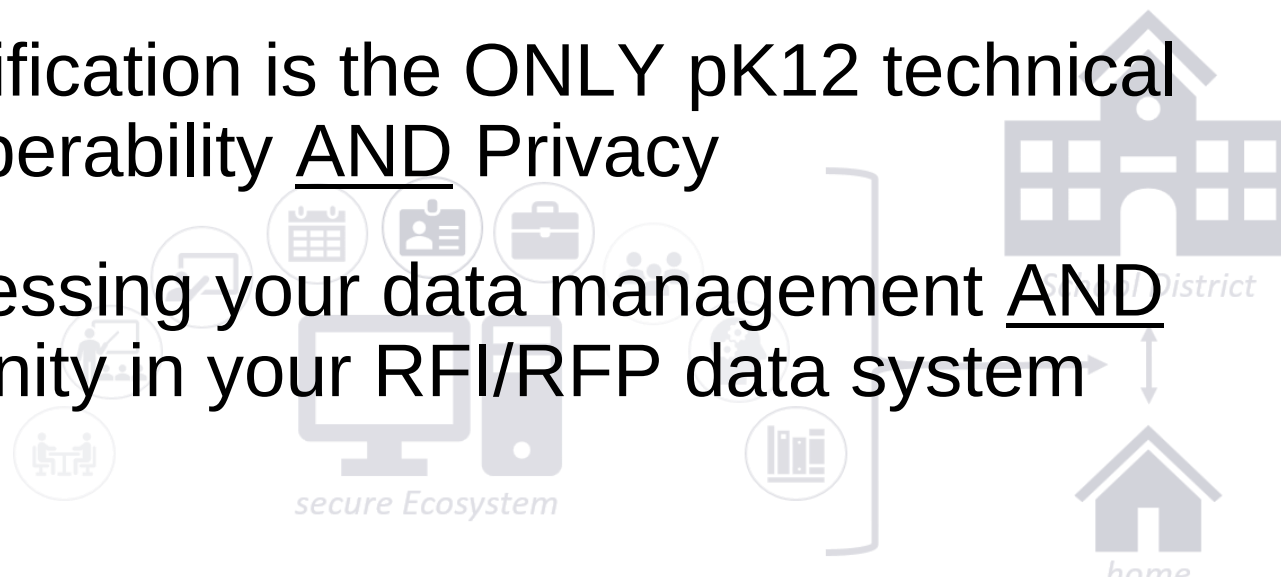


Knowing: Increased interoperability without the inclusion of privacy requirements = increased RISK.

Knowing: Both data sharing and privacy parameters must be identified and communicated!

Knowing: The A4L Unity Specification is the ONLY pK12 technical specification addressing Interoperability AND Privacy

Then: Take advantage of addressing your data management AND privacy needs by demanding Unity in your RFI/RFP data system maturation plans.





Access 4 Learning
Community

Powered by:  **SIF.**

Simple. Secure. Scalable. Standard.



Student Data Privacy Consortium

Q & A...

