

For Immediate Release
August 4, 2022
Postsecondary Electronic Standards Council
+1.202.261.6516
www.pesc.org
www.twitter.com/pescupdates
www.facebook.com/pescupdates
www.linkedin.com/company/pescinfo
Contact: Jennifer Kim, PESC
Contact: Penny Murray, A4L Community



SDPC Resource Registry
1st Place Award
Operational Privacy Role
23rd Annual Best Practices

STUDENT DATA PRIVACY CONSORTIUM RESOURCE REGISTRY AWARDED 1ST PLACE FOR “OPERATIONAL PRIVACY” IN PESC 23RD BEST PRACTICES

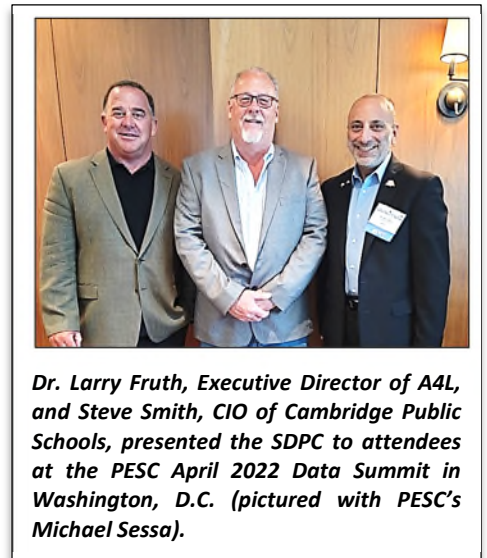
HUB’S COMPREHENSIVE REGISTRY OF VERIFIERS & PROVIDERS BUILDS TRUST

Washington, D.C. ~ The Board of Directors of the Postsecondary Electronic Standards Council (PESC) is pleased to announce the *Student Data Privacy Consortium* as 1st Place Winner for *Operational Privacy* role in PESC’s 23rd Annual Best Practices Competition.

The Access 4 Learning’s Special Interest Group, the Student Data Privacy Consortium (SDPC), is a unique collaborative of schools, districts, divisions, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns. The Consortium also leverages work done by numerous partner organizations but focuses on issues being faced by “on-the-ground” practitioners.

The SDPC Resource Registry has been developed to provide a framework for identifying solutions that have on-the-ground and real-world impact on student data privacy enabling schools, districts, state, and vendors find resources, adapt them to their unique context and implement needed protections.

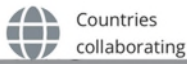
There are numerous organizations providing some great guidance, effective practices and/or tools to address various student data privacy issues. The challenge is that much of this work does not address many of the “immediate and on the ground” needs seen by schools, districts, divisions, states and territories each day. The SDPC calls these issues “tactical privacy” issues. The Consortium’s members address these day-to-day, real-world multi-faceted issues faced each day by privacy stewards in the protection of learner information.



Dr. Larry Fruth, Executive Director of A4L, and Steve Smith, CIO of Cambridge Public Schools, presented the SDPC to attendees at the PESC April 2022 Data Summit in Washington, D.C. (pictured with PESC’s Michael Sessa).

Welcome to the Student Data Privacy Consortium

Privacy By The Numbers...



4

35

States participating



Homepage of the Student Data Privacy Consortium Resource Registry (<https://privacy.A4L.org>).

The goals of the SDPC are:

- Establish a community of stakeholders who have various needs addressed through policy, technology and/or effective practice sharing around effective privacy management,
- Develop tools and resources to address operational issues not currently being addressed
- Develop a clearinghouse of student data privacy operational issues and resources to support schools, districts, states and vendors in managing those issues – no matter where the resources originate
- Identify projects that have on-the-ground and real-world impact on student data privacy enabling schools, districts, state and vendors find resources, adapt them to their unique context and implement needed protections
- Leverage partnership organizations working in the privacy space to have their good work utilized and no reinvention of existing work

“While I commend the various legislative and organizations beginning to address the issue of student data privacy, the ‘high level’ recommendations, guidance, certifications, etc. are difficult if not impossible to keep organized and more importantly implement at the district level. In my role as the CIO of Cambridge Schools in Massachusetts, I and my peers at the school level, need on the ground tactics and tools that help us reach the high bar set for us as student data stewards.”

– *Steve Smith, CIO, Cambridge Public Schools*

“The California IT in Educational (CITE) Association, representing over 1,000 districts, has joined the Student Data Privacy Consortium. The Consortium has a mature process for establishing a statewide contract and a database for posting vetted applications and provides transparency to staff and community. Collaboratively working with our partners, we expect to build clear steps that will streamline the process in protecting our student’s data by having a state-wide contract demonstrating compliance with California legislation.”

– *Andrea Bennett, Executive Director, California IT in Education (CITE)*

The award-winning submission made by SDPC is posted on the PESC website with prior winners at www.pesc.org. An Awards Ceremony was held during the General Sessions at PESC’s April 2022 Data Summit held in Washington, D.C.

For more information about the Student Data Privacy Consortium (SDPC), please visit <https://privacy.A4L.org>.

For more information about PESC and the Annual Best Practices Competition, please visit <https://www.pesc.org>.

ABOUT THE ACCESS FOR LEARNING COMMUNITY

The Access 4 Learning (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. For further information, visit <https://www.A4L.org>.





ABOUT PESC ANNUAL BEST PRACTICES

PESC Annual Best Practices Competition recognizes, highlights and promotes innovation and ingenuity in the application and implementation of interoperable data standards for business needs. The Annual Best Competition is open to institutions (schools, colleges, universities), associations, organizations, government agencies and departments, districts, consortia, non-profit and commercial service providers and other education stakeholders that have collaborated to design and/or adopt an electronic standardization initiative (e.g. published articles, white papers, pilots, demonstrations and implementations).

Submissions can/may include documentation, artifacts and descriptions of the scope of a project, participants and partners, types of standards employed, relevant dates and project milestones, copies of articles (if an article submission), outline of mission/objectives and any related statistics (# of transactions transmitted, estimated cost savings, etc.).

HALLMARKS OF BEST PRACTICES: While innovation and meeting customer needs will continue to ensure the rapid evolution of systems, applications, networks, products and services, those PESC recognizes as 'Best Practice' all share the use and inclusion of: Common Data Standards; Unique Identifiers and Standardized Code Sets; Quality Control Measures; Controlled Access and Security; Comprehensive Management Support; Flexibility and Scalability; Student/Learner-Centric; Formal Data Governance

EXPANSION OF BEST PRACTICES IN 2021: The Annual Best Practices expanded in 2021 into three separate categories: by region, by role, by technology. Awards may be made each year for each of the three separate categories; and multiple awards may be made each year under each category. The PESC Board Review Committee makes all awards and may determine that no award be made in a given year under one or more categories.

ABOUT PESC

Established in 1997 at The National Center for Higher Education, the Postsecondary Electronic Standards Council (PESC) operates as an international 501(c)(3) non-profit, community-based, umbrella association headquartered in Washington, D.C. of: Data, Software, Technology Service Providers and Vendors; Schools, Districts, Colleges and Universities; College, University and State/Provincial Systems; Local, State/Provincial and Federal Government Offices; Professional, Commercial and Non-Profit Organizations; Non-Profit Associations and Foundations.

PESC leads the establishment and adoption of trusted, free and open data standards across the education domain by serving as an open standards-development and open standards-setting body (governed by a voluntary, consensus-based model), independently funded by annual membership dues, meetings and sponsorships, enabling PESC to support, publish and maintain PESC Approved Standards and technical information free and without charge. PESC celebrates its 25th year anniversary in 2022 having been founded in 1997 at the National Center for Higher Education in Washington, D.C. For more information, please visit www.pesc.org.

#





Student Data Privacy Consortium
Resource Registry
1st Place Award
Operational Privacy Role
23rd Annual Best Practices

PESC BOARD OF DIRECTORS

August 4, 2022

W. MATTHEW BEMIS
UNIVERSITY OF SOUTHERN CALIFORNIA

Steve Smith
Chief Information Officer
Cambridge Public Schools

KRISTI BLABAUM
NASLA NATIONAL ASSOCIATION OF
STUDENT LOAN ADMINISTRATORS

Dear Steve:

RUTH BLADES
CATNS COUNCIL ON ADMISSION &
TRANSFER FOR NOVA SCOTIA

On behalf of PESC and the PESC Board of Directors, I am pleased to notify you that your submission **Student Data Privacy Consortium Resource Registry** in PESC's 23rd Annual Best Practices Competition has been awarded **1st Place Winner** for "Operational Privacy" role.

DOUG FALK
NATIONAL STUDENT CLEARINGHOUSE

A multi-media press release will be issued by PESC announcing this 1st Place Award with this notification letter and your winning submission attached.

WILLIAM BRYANT FAUST
AACRAO AMERICAN ASSOCIATION OF
COLLEGIATE REGISTRARS &
ADMISSIONS OFFICERS

Your winning submission will also be posted prominently on the **Annual Best Practices** page of PESC's website along with all previous 1st Place Award Winners. Please note the actual award will be held and delivered to you personally.

ALEX JACKL
BARDIC SYSTEMS

Congratulations from PESC and the PESC Board of Directors! Thank you and please extend warm thanks and gratitude to all SDPC partners and the entire A4L team!

DAVID K. MOLDOFF
ACADEMYONE

MICHAEL D. SESSA
PESC

My best regards,

Michael D. Sessa
President & CEO
PESC

MONTEREY SIMS
UNIVERSITY OF PHOENIX

FRANCISCO VALINES
FLORIDA INTERNATIONAL UNIVERSITY

JASON WEAVER
PARCHMENT

VIVIAN W. WONG
ORACLE

DAVID YERG
ELLUCIAN

WWW.PESC.ORG

cc: [PESC Board of Directors](#)



SDPC RESOURCE REGISTRY



1ST PLACE WINNER

FOR OPERATIONAL PRIVACY

– PESC 23RD ANNUAL BEST PRACTICES –





The A4L Student Data Privacy Consortium



*Connecting and Securing
Effective Learning Ecosystems -
The Student Data Privacy Way!*

[HTTPS://PRIVACY.A4L.ORG](https://privacy.a4l.org)

Increased interoperability without the inclusion of privacy requirements = increased RISK

CONNECTING

YOUR data management



#1 Global Educational Data Blueprint

[FIND OUT MORE >>](#)

SECURING

YOUR data privacy



Tactical Student Data Privacy Support

[FIND OUT MORE >>](#)

The Basics...

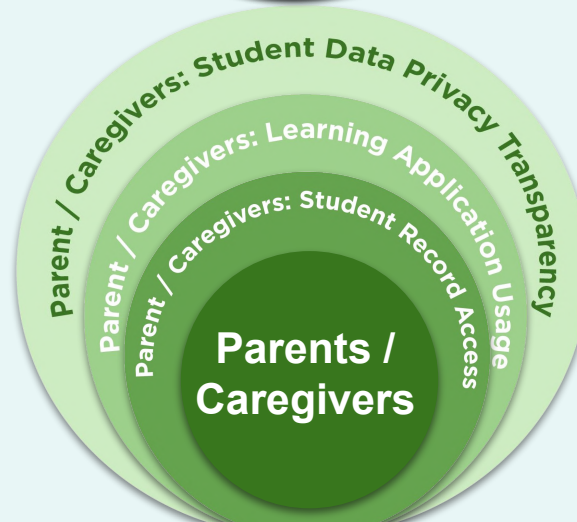
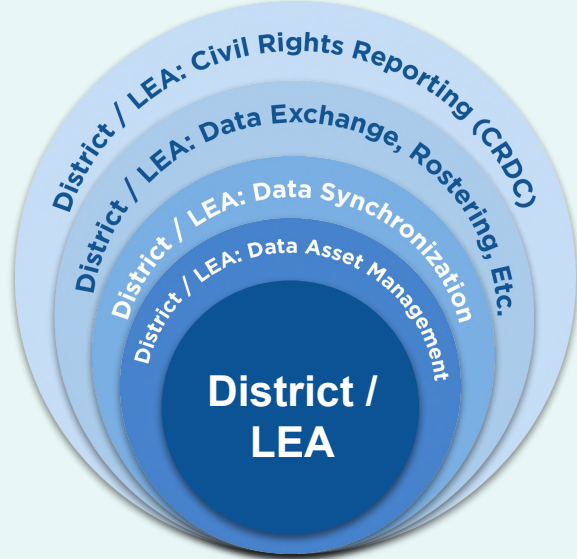


Each of the More Than 13,000 School Districts/Divisions in the US Are Still Finding Challenges in Getting Applications Into and Managed in Their *Digital Ecosystems*

The **MAJORITY** of End User-Vendor Issues Arise From The Lack of Common and Clear Expectations! *You Ever Experience This?*

More and More Stakeholders Are Aware of **Privacy and Security** Issues Especially in Schools - *More Critical Consumers!*





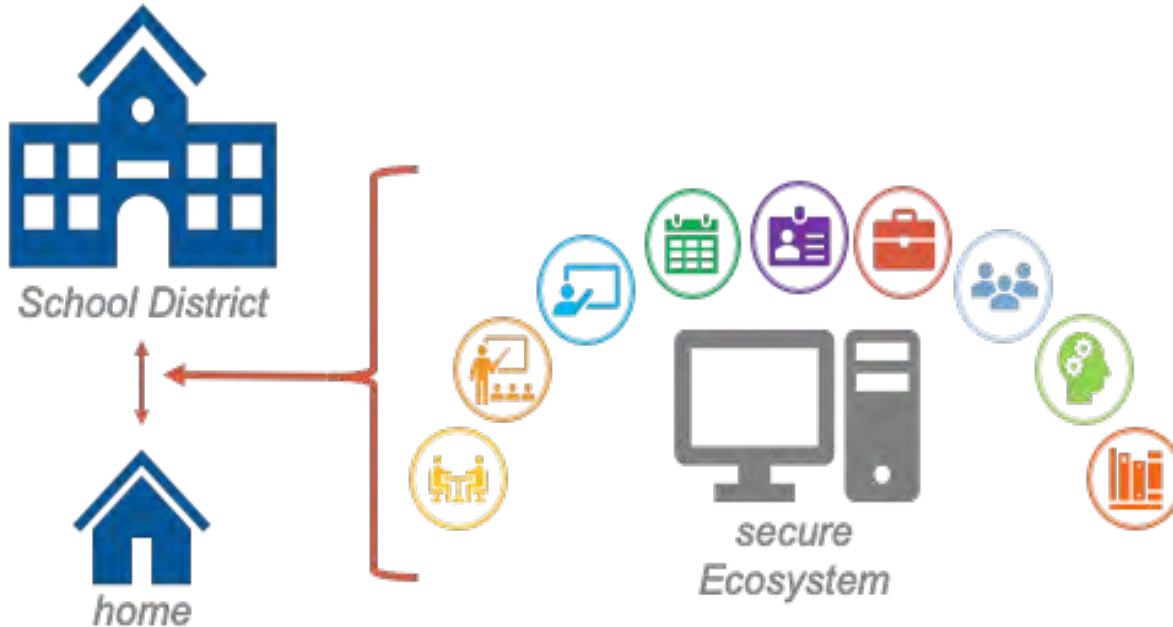
What's needed is a **connected, secure, and effective** learning ecosystem



Student Data Privacy Consortium



“Connecting and Securing Effective Learning Ecosystems®”



You MUST Address

- **Application Vetting**
- **Contracting Process**
- **Application Management**
- Integration
- Data Exchange
- Quality Control
- **Professional Learning**



District /
LEA

State
Agencies

Privacy Enforcement

Greater Marketplace Presence

Statewide Implementation

Standard Agnostic Exchange

CEDS DW, Generate & EdFacts

Validation & State Reporting

Student Data Privacy Transparency

Learning Application Usage

Student Record Access

Civil Rights Reporting (CRDC)

Data Exchange, Rostering, Etc.

Data Synchronization

Data Asset Management

 Access 4 Learning
Powered by:  SIF

Parents /
Caregivers

Vendors /
Providers

Connected and Secure Effective Learning Ecosystem TM

 Access 4 Learning
Powered by:  SIF



Student Data Privacy Consortium



Student Data Privacy Consortium

Quick Privacy 101



[HTTPS://SDPC.A4L.ORG](https://sdpc.a4l.org)

The Why: Student Privacy Laws



CIPA

Children's Internet Protection Act

Internet filters for K–12 schools and libraries to protect children from harmful online content as a condition for federal funding.

PPRA

Protection of Pupils Rights Amendment

Requires parental consent for any surveys that contain political, sexual, mental state, relationships, religious information

COPPA

Children's' Online Privacy & Protection Act

Requires operators of websites or online services for children under 13 that they are collecting personal information

HIPAA

Health Insurance Portability & Accountability Act

Usually HIPAA does not apply because information by definition is part of "education records" under FERPA and, therefore, is not subject to the HIPAA

FERPA

Family Educational Rights & Privacy Act (1974)

Schools must have written permission to release any information but allows schools to disclose under certain conditions

STATE

Legislation as well as Local Statutes and Regulations

40 states have passed 125 student privacy laws since 2013 laws

Student Privacy Laws

FERPA

Family Educational Rights & Privacy Act (1974)

Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31).





Student Privacy Laws

FERPA

School officials with legitimate educational interest.

Data Privacy Agreements (DPA) should cover;



- Security and Data Stewardship Provisions.
- Collection Provisions.
- Data Use, Retention, Disclosure, and Destruction Provisions.
- Data Access Provisions.
- Modification, Duration, and Termination Provisions.

The What?

Now that you know you **SHOULD** have a Data Privacy Agreement (DPA) – What’s Next?

The Facts:

- 13,000+ US Public School Districts
- 85% of Them Have <5,000 students – Many CIO’s Teach Daily!
- The Avg US School Has Anywhere Between 400 and 1,000 Apps
- “Freeware” or “Freemium” Products Are Exploding

Wouldn’t it Be Great If You Could:

- Save Resources (time, money, etc.) With ONE Data Privacy Agreement with Vendors
- “Piggyback” Off Other Agreements By Districts in Your Alliance?
- Seamlessly and Transparently Communicate Those Agreements to Staff, Parents, Etc.

Application and Agreement Management



Student Data Privacy Consortium



Contract/App Management

Under "Your Resources" Tab



Transparency – Put in Your Website!

"Customized Resource Listing" Under "Tools" Tab

Software Name	Agreement Status	Agreement Type	Agreement Dates	Grade Level	Content Area	Data
123apps	Vendor Unresponsive			K, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12	Instructional Technology	
ABC Mouse	Active	TEC Vendor-Specific Agreement with Exhibit Location: KLO	Approved: 08/02/2018 Expires: 08/02/2021	K	English Language Arts, Instructional Technology, Math, Science, Other	
ABC-Clio, LLC	Active	TEC Agreement V5B with Exhibit	Approved: 08/15/2018 Expires: 08/15/2021			

Wythe County Example

Introducing...

The National Data Privacy Agreement V1



✓ **Goals:**

- **Further increase consistency across Alliance DPAs**
- **Standardize the DPA Format so it looks the same across Alliances**
- **Ease logistics of implementing**
- **Identify common legal requirements across jurisdictions**
- **Provide mechanism to add other jurisdiction specific requirements**
- **Standardize terminology & definitions across jurisdictions and working groups (Legislative)**
- **Greater impact on, and buy in from, the vendor marketplace = Adoption**

Making Agreements “Simple”



NDPA Feature	Description
Section	Cover Page
Section	Page 2 - Options
Section	Page 3 - Signatories
Section	Standard Clauses
Section	<p>Exhibits</p> <ul style="list-style-type: none"> - 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

and is entered into by and between:

[School District Name], located at [Street, City, State] (the “Local Education Agency” or “LEA”) and [Provider Name], located at [Street, City, State] (the “Provider”).

WHEREAS, the Provider is providing educational or digital services to LEA.

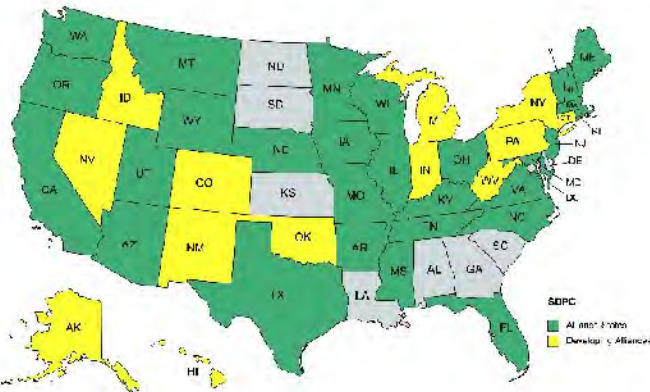
WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“COPPA”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
 - If checked, the Supplemental State Terms and attached hereto as Exhibit “G” are hereby incorporated by reference into this DPA in their entirety.
 - If checked, LEA and Provider agree to the additional terms or modifications set forth in Exhibit “H”. (Optional)
 - If Checked, the Provider, has signed Exhibit “E” to the Standard Clauses, otherwise known as General Offer of Privacy Terms

QUIZ TIME: Privacy..... By the Numbers!



33..... Participating States

88..... Participating Vendor Members

8,000..... Resources in the Registry

11,000..... Participating Districts

60,972..... Signed Exhibit E's

68,000..... Signed Agreements

34,000,000..... Students Impacted

And Research.....



National Research Data Privacy Agreement

- Leverages National Data Privacy Agreement (NDPA) template but for Researchers
- Developed with Foundations, Universities, Researchers, State and Local Ed Agencies



[About](#) [Resource Registry](#) [Resource Center](#) [Join the Community](#) [News/Events](#) [Login](#)

National Research Data
Privacy Agreement



The Basics...



Each of the More Than **13,000** School Districts/Divisions in the US Are Still Finding Challenges in Getting Applications Into and Managed in Their *Digital Ecosystems*

The MAJORITY of End User-Vendor-Research Issues Arise From The Lack of Common and Clear Expectations! *You Ever Experience This?*

More and More Stakeholders Are Aware of **Privacy and Security** Issues Especially in Schools - *More Critical Consumers!*



It's A Huge Community Partnership....



- Like it or not, technology usage for learning has only more recently become a required **“core competency”** of schools
- The DPA/NRDPA establishes required expectations of both parties - but ongoing communication and a closer partnership benefits everyone. NDPA/NRDPA developed with vendors/researchers at the table - a “give and take”!
- No more dealing with 13,000 potential schools
- Vendors/Researchers push the NDPA especially Exhibit E usage (piggy-back” agreement)
- **Strength in numbers!!!!!!!!!!!!**



“Common Expectations”

SDPC REsource Registry Tools:

- Communications
 - Between end users, providers, parents, policymakers, etc.
- Workflow tools
 - Teacher makes the ask, process is set in motion
- Automated Agreement Generation
 - Streamlines the “back in forth” between end users and providers
- Features and Functionality Suggestions
 - A “wish list” place for usage

The Basics...



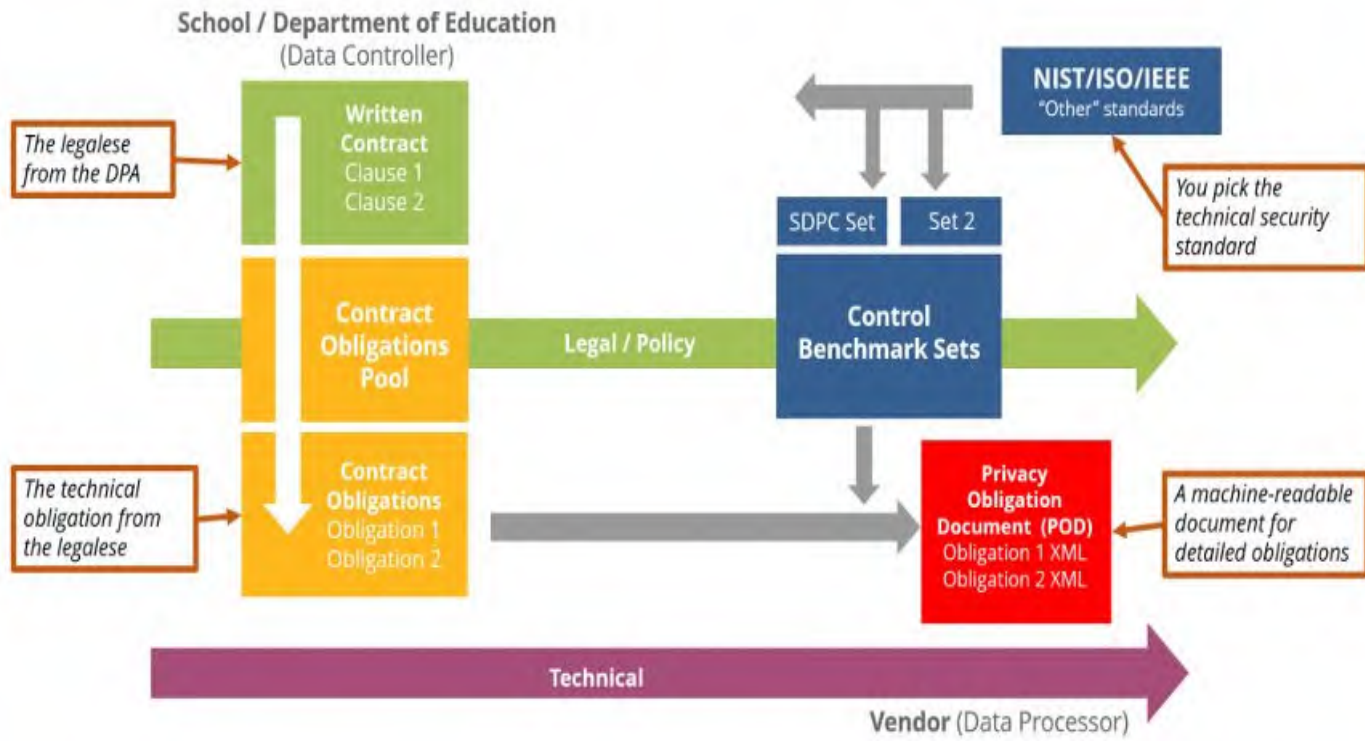
Each of the More Than **13,000** School Districts/Divisions in the US Are Still Finding Challenges in Getting Applications Into and Managed in Their *Digital Ecosystems*

The **MAJORITY** of End User-Vendor Issues Arise From The Lack of Common and Clear Expectations! *You Ever Experience This?*

More and More Stakeholders Are Aware of Privacy and Security Issues especially in Schools - *More Critical Consumers!*



End-to-End Privacy Solution?



Automate Contract Clause Expectations Exchange and Vendor Verification

The "POD" (Privacy Obligation Document)



What's Coming From the SDPC?



- SDPC successes has detoured legislative activity on privacy requirements
- The NDPA left security choice up to providers - “pick the one you used.....”
- Choices out there are “round peg in square hole” for K12 technologies
- Also the AU SDPC Community has a national project coming to the states - [Safer Technology 4 Schools \(ST4S\)](#) - vetting applications for privacy and security
- The SDPC Management Board just approved a new Project Team - **Global Education Security Standard** - tapping into existing Standards Orgs





Student Data Privacy Consortium

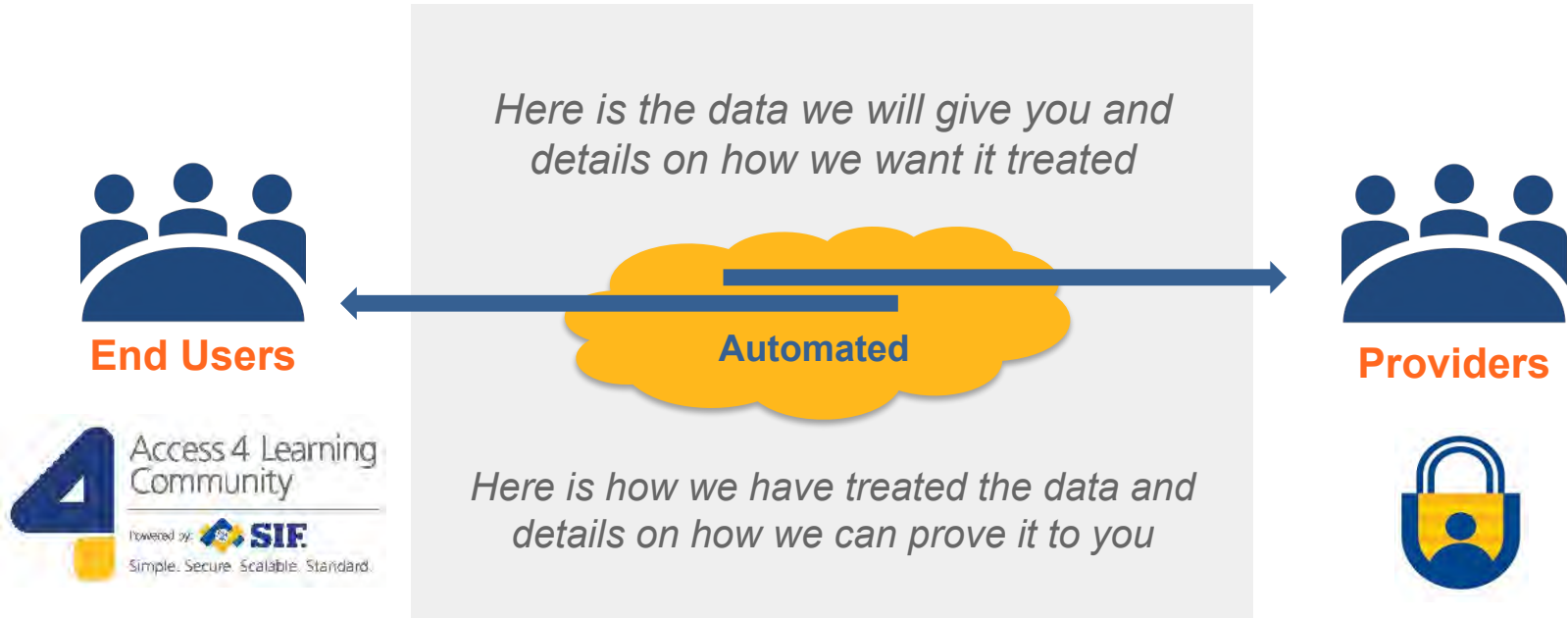
LEARNING
TECHNOLOGY
CENTERS of ILLINOIS

Q and A and Wrap



[HTTPS://PRIVACY.A4L.ORG](https://privacy.a4l.org)

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.*



Find Out More

- **Dr. Larry Fruth**
 - Ifruth@A4L.org
- **Steve Smith**
 - Ssmith@cpsd.us

<https://privacy.A4L.org>