



Student Data Privacy Consortium

Student Data Privacy

What is Required

FAMIS

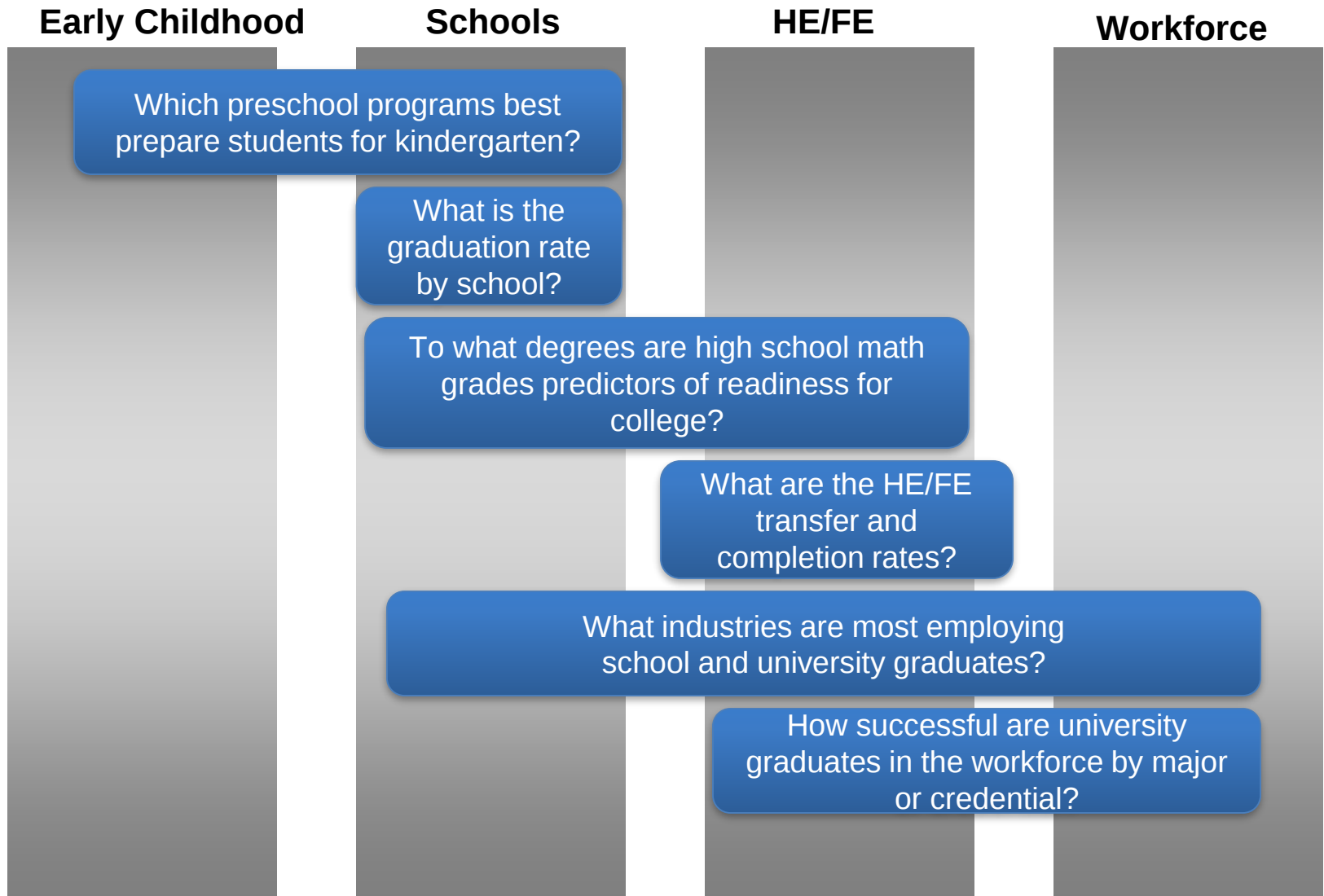
FLORIDA ASSOCIATION OF MIS





"Before I write my name on the board, I'll need to know how you're planning to use that data."

Reality Check: Changing Questions



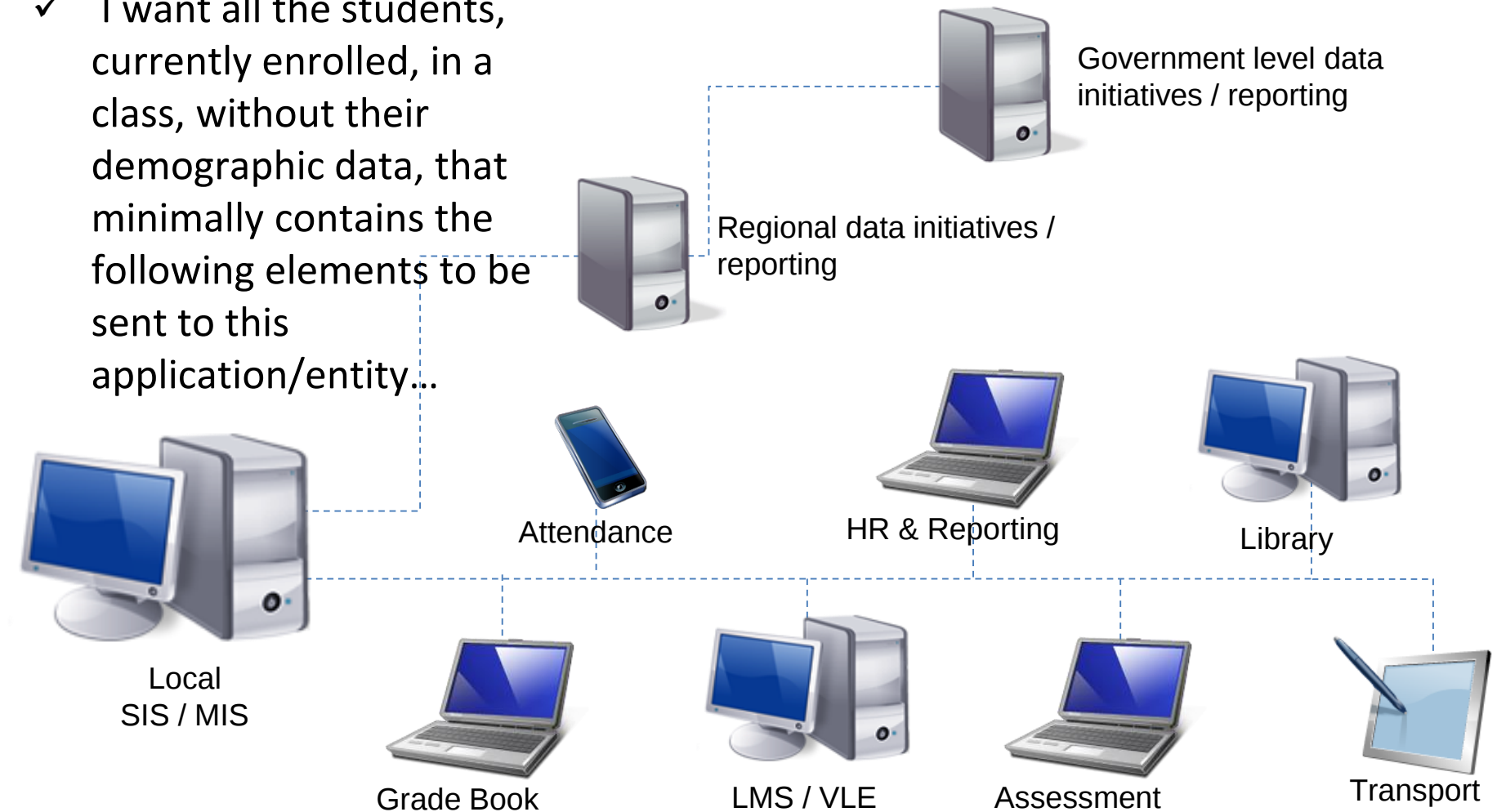
Reality Check: Education Demand



✓ I want all the students...

TO

✓ I want all the students, currently enrolled, in a class, without their demographic data, that minimally contains the following elements to be sent to this application/entity...



Reality Check: In The News

FTC Seeks Protection for Students' Personal Information in Education Technology Company ConnectEdu's Bankruptcy Proceeding – FTC 5/23/14

Marriott discloses massive data breach affecting up to 500 million guests- Washington Times 2018

Hundreds of millions of Facebook user records were exposed on Amazon cloud server - CBS News 2019

Quest Diagnostics says 12 million patients may have had their personal information exposed - CNN 2019

Concerns over Student Data Privacy Widespread Among Americans – THE Journal 01/22/14

Breech! Walmart exposed data of 1.3 million customers – UPI 2015

Major School Research and Assessment Provider Suffers Data Breach – Education Week 5/21/14

Ed. Dept. Makes Protecting Student Data a High Priority - Education Week 03/05/14

InBloom's Collapse Shines Spotlight on Data-Sharing Challenges – Education Week 5/2/14

Reality Check: In The News

FTC Seeks Information on Students' Personal Data - FTC 5/23/14
Would support various proposals regulating how student data is used, including:

Marriott discloses massive data breach - 500 million records exposed - Times 2018

FTC Seeks Information on Students' Personal Data - FTC 5/23/14

Quest Diagnostics may have exposed 1.3 million records - The New York Times 5/21/14

Breach! 1.3 million records exposed - The New York Times 5/21/14

Ed. Dept. Student Data a High Priority - Education Week 03/05/14



Spotlight on Data - Education Week 5/2/14

Reality Check: In The News

- **125 Student Privacy Bills in 36 States**
- **The Fall of In-Bloom**
- **Tons of Guidance**
 - Department of Education / FTC / White House Science and Technology / PTAC
 - DQC / COSN / SIIA / Fordham / Future of Privacy Forum / iKeepSafe / Foundation for Excellence in Education / Parent Coalition for Student Privacy / Electronic Privacy Information Center / Alliance for Excellence in Education
 - NYU / Harvard / Learnsphere
- **A4L Data Privacy Task Force**

40



Reality Check: Local “Control” Issues

- **Funding reductions at federal and state levels**
 - Local funding implications
- **87% of Districts in the US have less than 10,000 student enrolled**
 - IT oversight implications
- **91% of parents indicate that schools need to inform parents before personal student information is exchanged**
 - Data management and usage implications

Its Not “One or the Other”!



Student Data Privacy Consortium



No One Gets It!



Everyone Gets It!



Access 4 Learning
Community

Powered by:  **SIF**

Simple. Secure. Scalable. Standard.

A4L:

- 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 for data to move safely and securely between school software applications
- Used in every state and Communities in 4 Countries

SDPC:

- Special Interest Group of A4L Community started in 2015
- Maintains its own governance, oversight and resource support
- Numerous stakeholders addressing data privacy “Pain Points”
- Working on three projects identified and worked on by members:
 - Privacy Contract Framework
 - Digital Tools Governance
 - Global Education Privacy Standard

How is A4L “Different?”

How is A4L unique?

20 Years of Development Experience in K12 Interoperability

100% Membership Dues Funded – No Outside Funding Dependencies

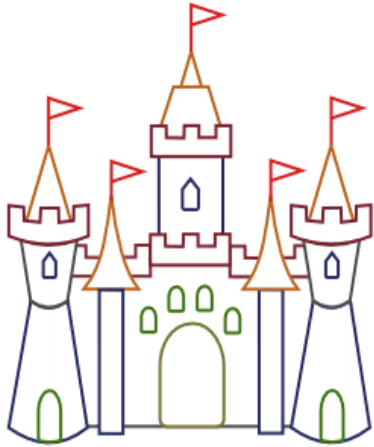
Expertise in Balancing BOTH Data Interoperability & Privacy

School, State, Government and Vendor Members Across 4 Global Communities

Well-established and Transparent, Governance, Finance and Development Processes

Leadership Committed to Using Multiple Standards Together to Address Any Use Case

So What Are The Issues?



Who Can Access?

- ✓ Need to consider both inside areas of the castle/school (between rooms and/or between apps) and outside access to the castle/school (moat and drawbridge and/or firewall and security)

What Can They Access?

- ✓ Once inside the castle/school where can they go? (i.e. to the butcher but not the church and/or to the SIS but not healthcare applications)

How Can They Access?

- ✓ Does everyone enter in their own manner (password and by horse and/or API and remote access) or do we all use the same mechanism?



Student Data Privacy



Current Status

Federal Legislation

FERPA, COPPA, PPRA, CIPA,
HIPAA

Guidelines & Resources

PTAC, CoSN, DQC, CSM,
FPF, etc...



FL Legislation

Year	BILL NUMBER	High Level Summary	Early Ed	K-12	Higher Ed	Vendors	SEAs	LEAs
2014	SB 188	Requires State Board to annually notify parents and students of their FERPA rights. Prohibits collection or retention of information such as political and religious affiliation, voting history, or biometric information of student, sibling, or parent. Prohibits use of a student's SSN as their identification number.	N	Y	N	N	Y	Y
2017	HB501	An Act relating to public records and public meetings – this bill creates an exemption from public records requirements for certain records held by a state university or Florida College System institutions which identify detection, investigation, or response practices for suspected or confirmed information technology security incidents and this bill authorizes disclosure of confidential and exempt information to certain agencies and officers.	N	N	Y	N	N	N
2018	HB 731	This bill prohibits the state superintendent from storing any PII from students who are home schooled. District school superintendents are prohibited from including social security numbers or any other personal information of students in any school district or school database unless the student chooses to participate in a school district program or service.	N	Y	N	Y	Y	N

HIPPA

Health Insurance Portability and Accountability Act of 1996

When does it apply in schools?

- In most cases, the *HIPAA* Privacy Rule does not apply to an elementary or secondary school because the school either: (1) is not a *HIPAA* covered entity or (2) is a *HIPAA* covered entity but maintains health information only on students in records that are by definition “education records” under *FERPA* and, therefore, is not subject to the *HIPAA* Privacy Rule.



<http://bit.ly/2ipV4ri>

CIPPA

The Children's Internet Protection Act

What does this CIPPA address?

- Federal Communications Commission (FCC) rule requires that K–12 schools and libraries in the United States use Internet filters and implement other measures to protect children from harmful online content as a condition for federal funding.

<https://www.fcc.gov/consumers/guides/childrens-internet-protection-act>



PPRA

Protection of Pupil Rights Amendment

What does this PPRA address?

Requires parental consent for any surveys that contain the following information;

- Political affiliations;
- Mental and psychological problems potentially embarrassing to the student and his/her family;
- Sex behavior and attitudes;
- Illegal, anti-social, self-incriminating and demeaning behavior;
- Critical appraisals of other individuals with whom respondents have close family relationships;
- Legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;
- Religious practices, affiliations, or beliefs of the student or student's parent*; or
- Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program.)

COPPA

Children's Online Privacy Protection Rule

- Who Does COPPA apply to?
 - FTC Rule
 - A Federal Trade Commission (FTC) Rule
 - COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

<https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>

FERPA

Family Educational Rights and Privacy Act of 1974

Who can describe FERPA
in layman's terms?



<https://www2.ed.gov/policy/gen/guid/fpco/brochures/parents.html>

FERPA

Family Educational Rights and Privacy Act of 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):

- School officials with legitimate educational interest;
- Other schools to which a student is transferring;
- Specified officials for audit or evaluation purposes;
- Appropriate parties in connection with financial aid to a student;
- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;
- To comply with a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies; and
- State and local authorities, within a juvenile justice system, pursuant to specific State law.

FERPA

Family Educational Rights and Privacy Act of 1974

How does this affect our
jobs in schools as IT
leaders?

Let's Discuss



FERPA

Family Educational Rights and Privacy Act of 1974

- 1) What role do you play in your District in ensuring FERPA requirements are being met?**
- 2) Who else in your District plays a role in protecting students' privacy?**
- 3) What do you feel you and your District do well in ensuring all student records/data are protected?**
- 4) What areas do you feel your District could improve in relation to ensuring the protection of your students' data?**

YOU ARE THE ONLY ONE DRIVING THE CAR!

- Neither the federal government nor most state governments have made the enforcement of student privacy laws a priority. Except perhaps for the FTC, very few lawsuits.
- Many persons in the business department or other senior school management will not have the expertise to understand student privacy issues.
- The battles for student privacy will be mostly fought for now by your IT department or your CTO.

The Questions.... Or “Mis-Questions”

- *I am a vendor who is FERPA Compliant*
- *My application does not contain personally identifiable (PII) information*
- *As a school I need to ensure COPPA compliance*
- *Teachers using made up IDs for apps is ok*
- *As a school, if I only share "Directory Information" with the App I'm OK*
- *As a vendor I believe the schools must collect parental consent to meet COPPA*



Privacy Law Resources

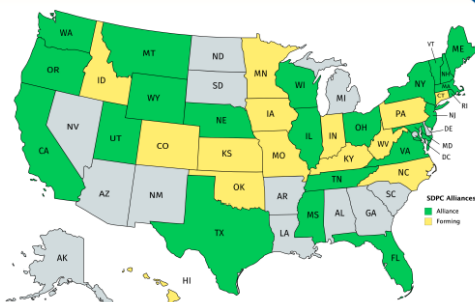
- <http://www.fldoe.org/core/fileparse.php/7674/urlt/0064538-ferpa.pdf>
- <https://ferpasherpa.org/state-laws/>
- <https://privacy.a4l.org/>



Privacy – By The Numbers...

the Student Data Privacy Consortium (SDPC)

25



State-wide Alliances

3



Contract Framework
Digital Tools Governance
Global Education Privacy Standard
Tactical Privacy Projects

32million



Students supported
by Projects

8400+



School Districts
represented

3



Countries Collaborating
on Privacy Issues

2765



Signed Vendor
Agreements

1900



Applications in
Database

>250



Signed "Piggyback"
Exhibit E

"The California Educational Technology Professionals Association (CETPA), 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 CA legislation."



Student Data Privacy Consortium



FAMIS

FLORIDA ASSOCIATION OF MIS

BREAK



Student Data Privacy Consortium

The Student Data Privacy Consortium: The FL Alliance

FAMIS

FLORIDA ASSOCIATION OF MIS



A4L:

- 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 for data to move safely and securely between school software applications
- Used in every state and Communities in 4 Countries

SDPC:

- Special Interest Group of A4L Community started in 2015
- Maintains its own governance, oversight and resource support
- Numerous stakeholders addressing data privacy “Pain Points”
- Working on three projects identified and worked on by members:
 - Privacy Contract Framework
 - Digital Tools Governance
 - Global Education Privacy Standard

How is A4L “Different?”

How is A4L unique?

20 Years of Development Experience in K12
Interoperability

100% Membership Dues Funded – No Outside Funding
Dependencies

Expertise in Balancing BOTH Data Interoperability and
Data Privacy

School, State, Government and Vendor Members Across 4
Global Communities

Well-established and Transparent, Governance, Finance
and Development Processes

Leadership Committed to Using Multiple Standards
Together to Address Any Use Case



Student Data Privacy Consortium

SDPC Goals

Establish a community of stakeholders who have various needs addressed through policy, technology and/or effective practice sharing around effective privacy management,

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,

Development of **tools and resources** to address operational issues not currently being addressed,

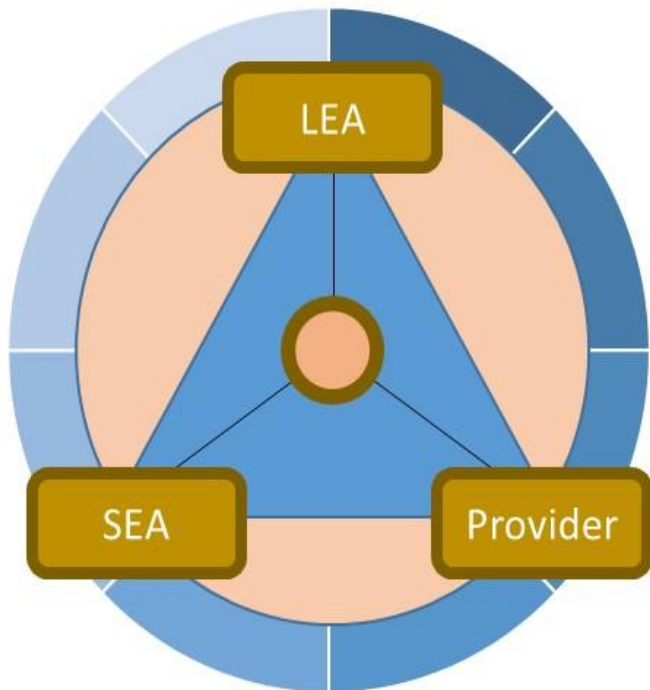
Leverage partnership organizations working in the privacy space to have their good work utilized and no reinvention of existing work,

Development of 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.



Student Data Privacy Consortium

SDPC Scope and Opportunity



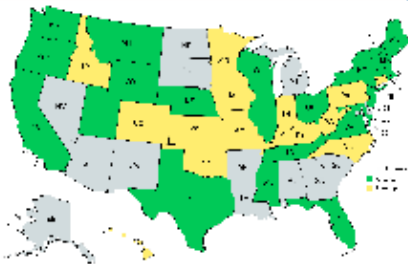
-  Consortia sponsored products/tools services
-  Consortia membership, ideals, mission
-  Tangential initiatives and groups, including privacy initiatives, funders, etc
-  Core stakeholder/consumer/client
-  Stakeholder relationship driving core directives through pain points



Privacy – By The Numbers...

the Student Data Privacy Consortium (SDPC)

25



State-wide Alliances

3



Contract Framework
Digital Tools Governance
Global Education Privacy Standard
Tactical Privacy Projects

32million



Students supported
by Projects

8400+



School Districts
represented

3



Countries Collaborating
on Privacy Issues

2765



Signed Vendor
Agreements

1900



Applications in
Database

>250



Signed "Piggyback"
Exhibit E

Learn about the new emerging "Global Education Privacy Standard" soon to change the way vendors & districts communicate and validate privacy requirements

Find out more: <https://privacy.A4L.org>

Information checked December 2018

"The California Educational Technology Professionals Association (CETPA), 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 CA legislation."

**Andrea Bennett, CETPA
Executive Director**



Student Data Privacy Consortium

SDPC Tactical Privacy Projects

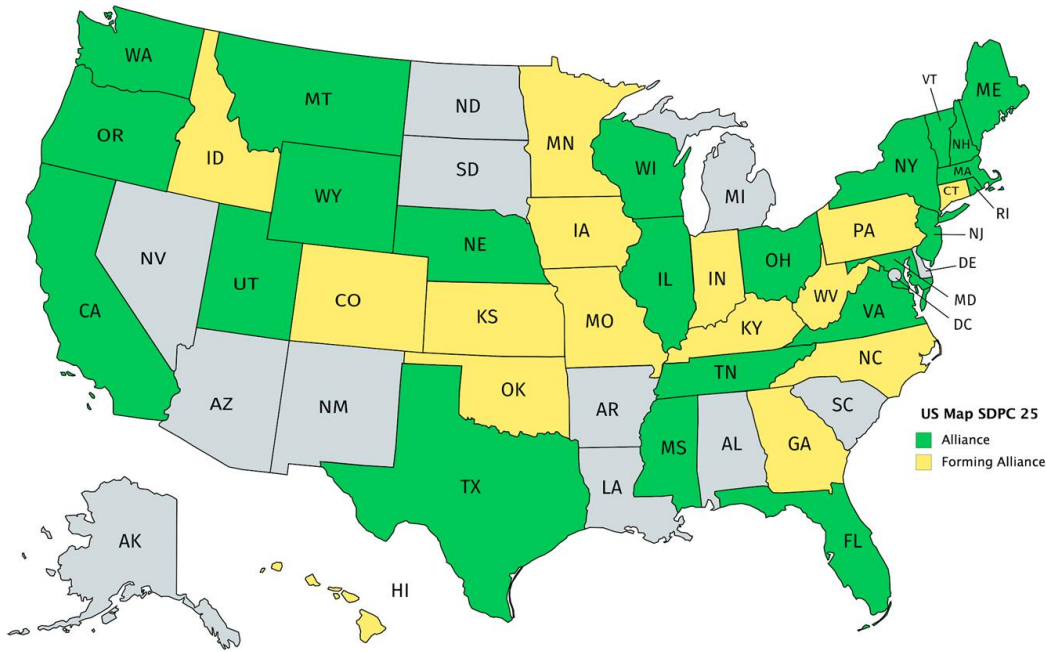
- **Project 1: Privacy Contract Framework**

- *The Privacy Contract Framework project is focused on the development 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. Application Profiles will be developed to support “apples to apples” comparisons.*



Student Data Privacy Consortium

Alliances, Alliances,



SDPC State/Territory Alliances (Green) and in Process (Yellow)

Currently 32 million Students Impacted by over 1650 Applications!



Student Data Privacy Consortium

Alliances, Alliances,

Alliance Formation Models:

Top Down: *The State agency leading the charge to develop and grow the Alliance*

Bottom Up: *A LEA takes the lead to develop and grow the Alliance*

Middle Driven: *A regional service agency, professional association, or user group takes the lead to develop and grow the Alliance*

- CoSN, ISTE, SETDA, affiliates / Regional Service Agencies / Etc.

** All three models have examples of SEAs paying for Alliance Membership as a “value-add” to LEAs.*



Student Data Privacy Consortium

Alliances, Alliances,

Alliance Roles:

- ✓ **Participate** in the SDPC and interact with other Alliance members and SDPC Projects
- ✓ **Convene** stakeholders in their state to identify pain points and gauge the interest in developing a “common contract framework” and tools use as 16 other states have done to date.
- ✓ **Develop** contract wording that could be used by all districts with their vendors and provide transparent communications to parents and community members on application usage.
- ✓ **Advocate** for student data privacy and locally support the ongoing needs of the Alliance including bringing possible projects to the larger SDPC Consortium for review and vetting by other Alliances.



Student Data Privacy Consortium

SDPC Resource Registry

SDPC Resource Registry

https://sdpc.a4l.org

CPS CPS Facebook Twitter LinkedIn Today's Paper 07/1... Sentinel Verizon TD Bank Credit Card, Mortga... Wunderlist MyChart

About the Consortium Projects / Initiatives Get Involved Members and Partners Login

SDPC Resource Registry

Welcome | Login

About SDPC

The Student Data Privacy Consortium (SDPC) is an unique collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns. >>

[View Participating Districts](#)
[Learn about Joining the Alliance](#)
Already a member? [Login](#)

State Alliances

Select a state to visit their alliance website.

Select a State ▾

[Visit an Alliance >>](#)

Search the Database

Examine student data privacy agreement information from across the nation.

[Get started >>](#)

Quick Stats

We are overflowing with participation. Why not join us? [Learn more >>](#)

Nationwide SDPC Stats

of Countries Participating: 2
of States Participating: 22
of Districts Participating: 7533
of Vendors Participating: 26
of Resources: 2086

Are your students safe online? Join us!

PAGES CONTACT US



Student Data Privacy Consortium

SDPC Resource Registry



Search the Database

How can we help you?

[SDPC Home Page](#)

[Search National Database](#)

[Login](#)

State Alliances



Select a state to visit their alliance website.

Select a State

[Visit an Alliance >>](#)

Search by State

Select a State

[Search >>](#)

Search by District

Select a District

[Search >>](#)

Search by Resource

Select a Resource

[Search >>](#)

Search by Company Name

Select a Company

[Search >>](#)

Search by Grade Level & Content Area

Select a Grade

Select a Content Area

[Search >>](#)



Student Data Privacy Consortium

SDPC Tool

Show 10 entries

Search:

Company Name	Application	Status	Agreement Type	Grade Level	Content Area	Data
Achieve 3000 <i>Purpose: Achieve3000® provides the only patented, cloud-base solutions that deliver daily differentiated instruction for nonfiction reading and writing that's precisely tailored to each student's Lexile® reading level.</i>	Achieve 3000	Active	Agreement V2a (Includes Terms of Service)	6, 7, 8	English Language Arts	
Benetech <i>Purpose: Non-profit social entrepreneurial venture harnessing the power of technology for social benefit.</i>	Benetech	Active	Legal Drafted Parent Release			
Biblionasium <i>Purpose: Kids connect with friends, parents and teachers to share and recommend their favorite books</i>	Biblionasium	Active	Legal Drafted Parent Release	K, 1, 2, 3, 4, 5	Library Media	
 Sunburst Digital, Inc. <i>Purpose: Leveled online text library</i>	Big Universe	Active	Agreement V1	K, 1, 2, 3, 4, 5	English Language Arts	Coming Soon
 Google <i>Purpose: Free weblog publishing tool from Google, for sharing text, photos and video.</i>		Active	Legal Drafted Parent Release	6, 7, 8, 9, 10, 11, 12	Instructional Technology	Coming Soon
 BrainPOP <i>Purpose: Animated curricular content</i>		Active	Agreement V2a (Includes Terms of Service)	K, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12	Other	Coming Soon
 McGraw Hill Education <i>Purpose: Supplemental online activities for J.K. Math curriculum.</i>	Building Blocks	Active	District Modified Contract	K	Math	Coming Soon

Data Used

Contract PDF



Student Data Privacy Consortium

SDPC App “Tools”

Tools for Participating Districts

[Search the Database >>](#)



[Add Customized Resource
Listing to Your Website](#)



[Add Digital
Resource Request
Form to Your Website](#)



[Build a Contract Tool](#)



[Bulk Import Template](#)



[Export List of All Resources](#)



[Email MA Participants](#)
[Email All Participants](#)



[Statistics](#)



[Add Additional District
Account](#)



Members Area

[View All Participating
Districts >>](#)

Add: [Resource](#) | [Agreement](#)

[Manage Resource/Agreement
Information](#)

[Participating Districts](#)

Download Student Data Privacy
Agreement

Version 5: [pdf](#) | [doc](#)

Version 4: [pdf](#) | [doc](#)

[Add Additional District Account](#)

[Edit Account Information](#)

[Logout](#)



SDPC Tactical Privacy Projects

- **Project 1: Privacy Contract Framework**

- *The Privacy Contract Framework project is focused on the development 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. Application Profiles will be developed to support “apples to apples” comparisons.*

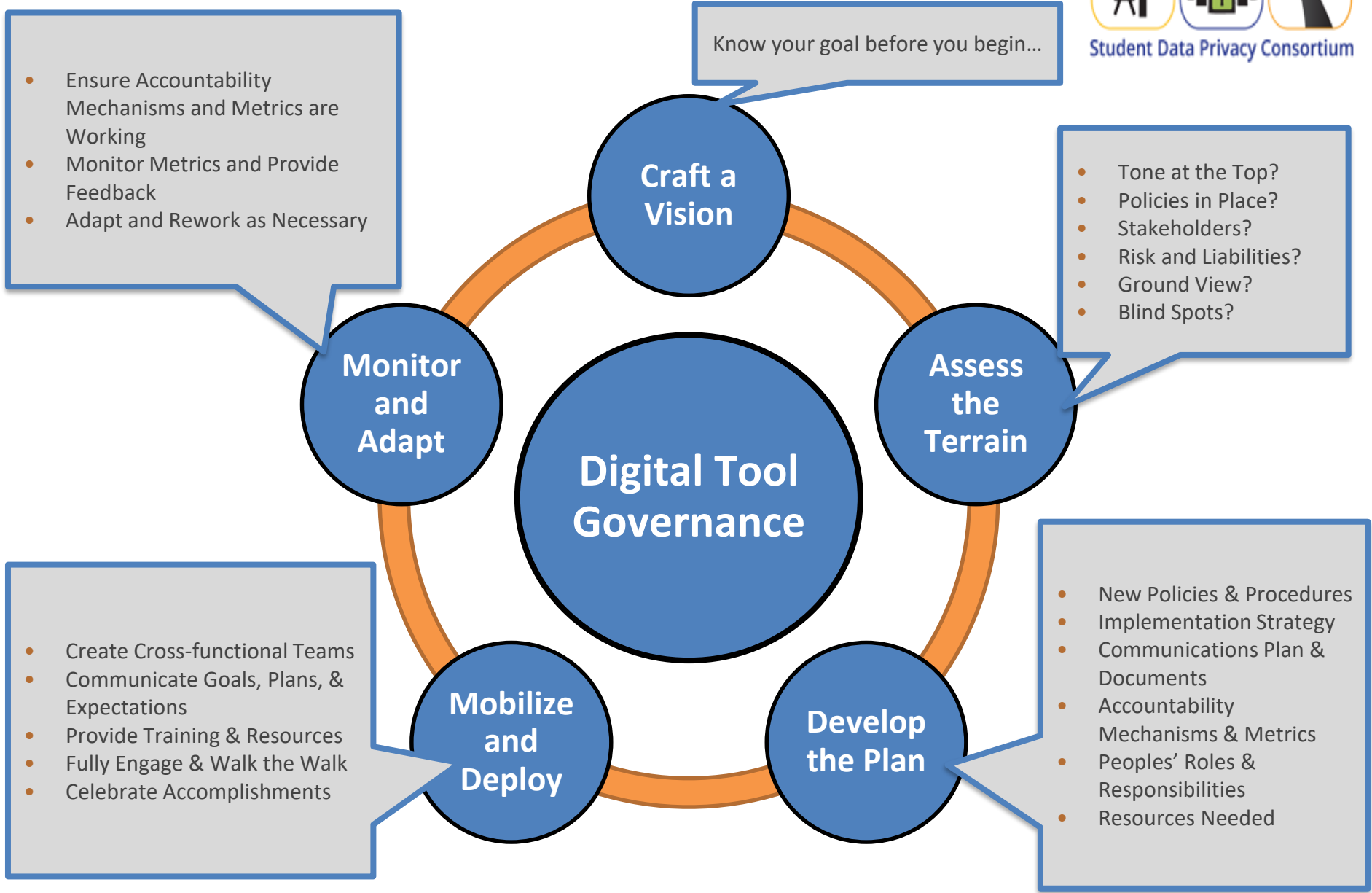
- **Project 2: Digital Governance Tool**

- *The Digital Tools Governance project centers around developing a comprehensive framework for aligning a school system’s policy landscape, strategic programming, tactical processes, and accountability mechanisms to support the system’s vision of how its digital tool ecosystem will advance its overall mission and goals while minimizing its risks of data privacy and security incidents.*

Framework for Transformative Digital Governance



Student Data Privacy Consortium



Digital Governance Tool (DGT)



Welcome to the DGT.

Below are the projects and your progress. Click on a project below to get started.

Privacy Policies

1 2 3 4 5

App Vetting

1 2 3 4 5

[View the Project Report](#)

Privacy Professional Learning

1 2 3 4 5

[Shared Resources](#)

[My Shared Resources](#)

[Shared Digital Governance Plans](#)

View Your District's Digital Governance Plan [→](#)

CONTRACT

Data Breach Issues

1 2 3 4 5

[View the Project Report](#)

Technical Cyber Security

1 2 3 4 5

Vendor-End User Engagement

1 2 3 4 5

[View the Project Report](#)



SDPC Tactical Privacy Projects

• Project 3: Global Education Privacy Standard (GEPS)

- *Contractual agreements over the protection of student data is only the first step - if/how providers are meeting the requirements in their solution*
- *In order to create a secure K-12 environment we need to connect the contractual obligations to real world technology solutions – not “industry best standards” as currently stated in many data privacy agreements (DPA).*



National Data Privacy Agreement Clause Set

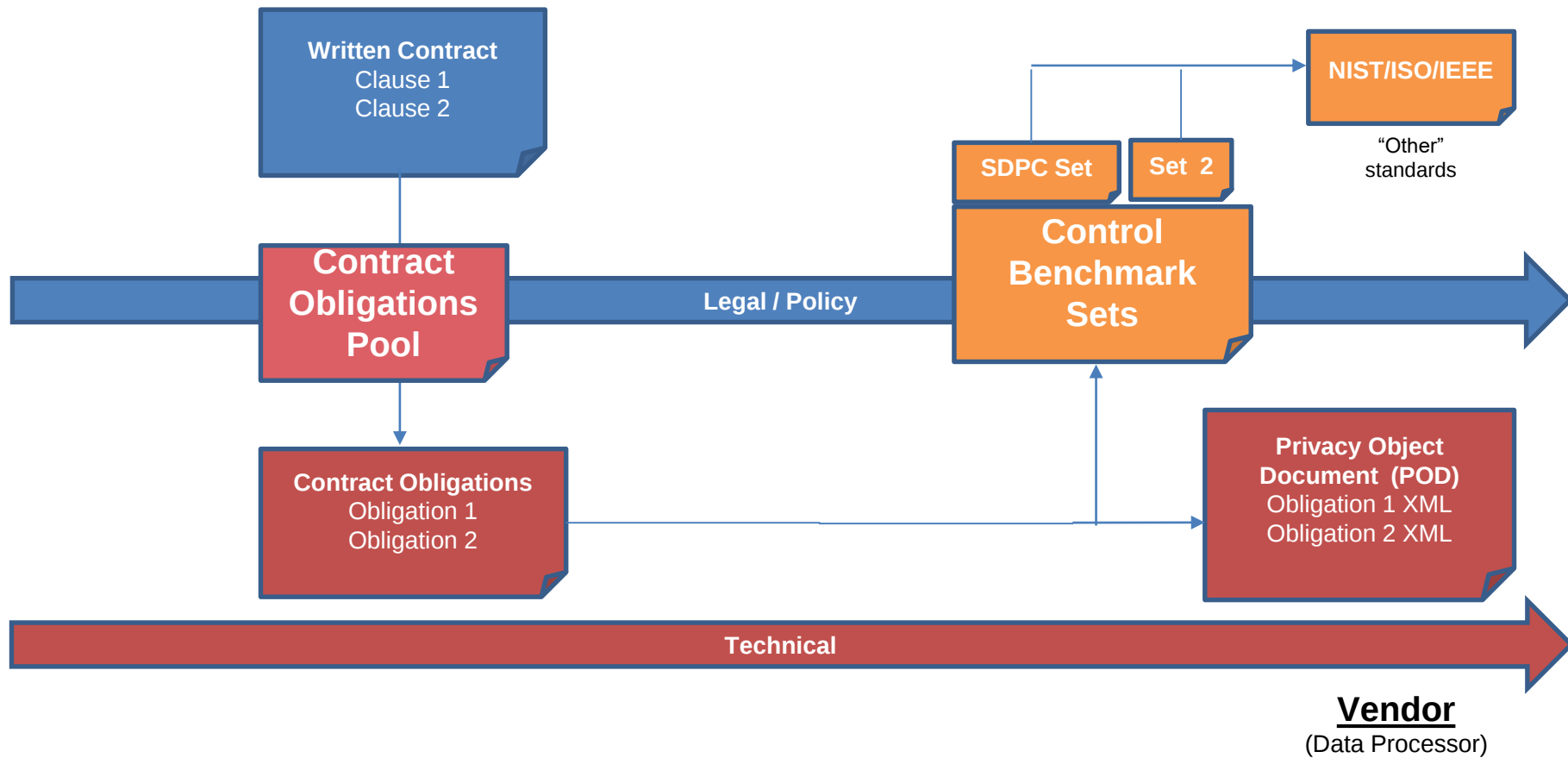
Purpose of DPA	Nature of Services Provided
Student Data to Be Provided	Student Data Property of LEA
Parent Access	Separate Account
Third Party Request	Subprocessors
Privacy Compliance	Authorized Use
Employee Obligation	Non Disclosure
Disposition of Data	Advertising Prohibition
Data Security	Passwords and Employee Access
Destruction of Data	Security Protocols.
Employee Training	Security Technology.
Security Coordinator	Subprocessors Bound.
Periodic Risk Assessment	Data Breach
Privacy Compliance	Annual Notification of Rights
Reasonable Precautions	Unauthorized Access Notification.



Global Education Privacy Standard (GEPS)

School / Department of Education

(Data Controller)

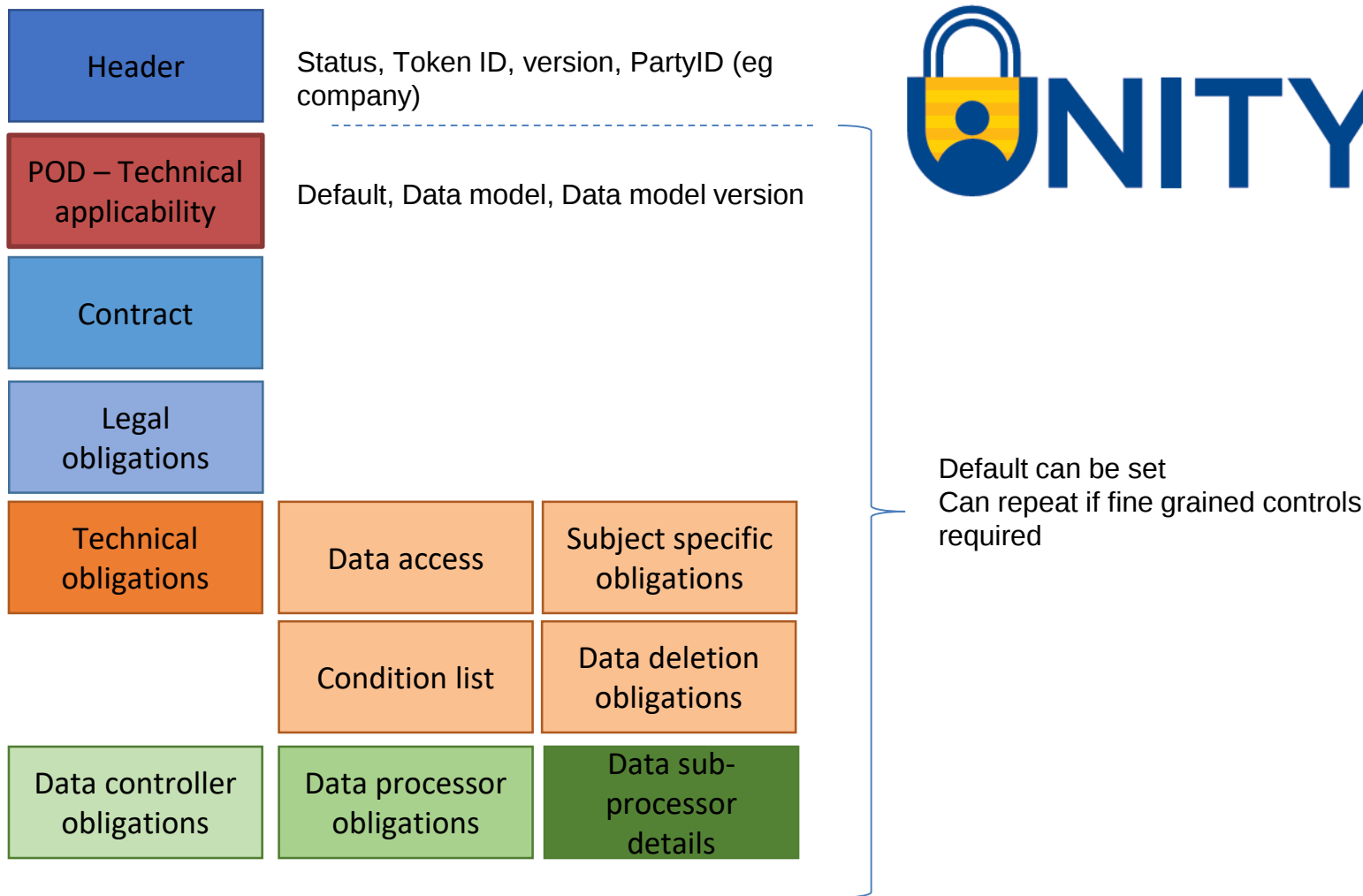


Destruction of Data. Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA’s designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.



OBLIGATION	Maintain an accessible practice of destruction of data with adequate reference to definitions and policies in presenting general data retention guidelines	Alignment to Known Standards
Benchmark	Present a data retention policy which identifies data classifications, retention schedule, and destruction process in line with data classification level.	NIST 800- 53 (Rev. 4) System And Information Integrity Control Family SI-12 Information Handling and Retention. NIST 800-88 R1 are the data delete definition guidelines to be referenced against the legal requirements for retention and data classification and definitions as required by specific local standards (state, provinces, territory)
Benchmark	Properly address and agree to the definition of delete [link. Talk to making unrecoverable, discuss extent such as backups/etc].	
OBLIGATION	Acknowledge and register adequate signals for the interpretation, operational execution, and notice of deletion requests.	Alignment to Known Standards
Benchmark	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.
Benchmark	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.	

POD contents (SIF Infrastructure)





*The MOST complete
standardized roster
solution for K12
usage*



*The MOST
implemented K12
Interoperability
Specification*



*The REST
Infrastructure that
starts simply and
scales easily*



*The BEST
Implementable
Specification for
CEDS Utilization*



*The FIRST Interoperable
Specification allowing for
great privacy control and
the Global Education
Privacy Standard (GEPS)*



*The FIRST
Standardized API
for Individual
Education Plans*



Introducing “Unity”!

Its Not “One or the Other”!



Student Data Privacy Consortium



No One Gets It!



Everyone Gets It!



Access 4 Learning
Community

Powered by:  **SIF**

Simple. Secure. Scalable. Standard.



Student Data Privacy Consortium



FAMIS

FLORIDA ASSOCIATION OF MIS

What Can I Do Now?

- Start an inventory
- Start a conversation in your district
- Begin building awareness
- Become involved in FLPA
- Become familiar with FPA Registry



Student Data Privacy Consortium

SDPC Resource Registry

SDPC Resource Registry

https://sdpc.a4l.org

CPS CPS Facebook Twitter LinkedIn Today's Paper 07/1... Sentinel Verizon TD Bank Credit Card, Mortga...

About the Consortium Projects / Initiatives Get Involved Members and Partners Login

SDPC Resource Registry



2019 2nd Annual SDPC Meeting

APRIL 3, 2019 | PORTLAND, OR

- Contract Framework Update
- Digital Governance Tool Update
- Workshop on the SDPC Global Education Privacy Standard
- Student Privacy Boot Camp for non-SDPC members

*Begins immediately following the CoSN closing ceremony.

[Register >](#)

Welcome

About SDPC



The Student Data Privacy Consortium (SDPC) is an unique collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns. >>

[View Participating Districts](#)
[Learn about Joining the Alliance](#)
Already a member? [Login](#)

State Alliances



Select a state to visit their alliance website.

Select a State

[Visit an Alliance >>](#)



Search the Database

Examine student data privacy agreement information from across the nation.

[Get started >>](#)

Quick Stats



We are overflowing with participation. Why not join us? [Learn more >>](#)

Nationwide SDPC Stats

# of Countries Participating:	1
# of States Participating:	21
# of Districts Participating:	6967
# of Vendors Participating:	20
# of Resources:	1618

Are your students safe online? Join us!

PAGES

About the Consortium

CONTACT US

A4L Community



Get Involved!

- www.privacy.a4l.org
- www.a4l.org



- **Larry Fruth PhD – A4L Community**
 - lfruth@a4l.org
- Go to the [FL Alliance page](#) > Click on Join Now > Select your district and fill out the form. The account request will go to the Alliance admin for approval. When filling out the form, you choose your own username and password.