



Student Data Privacy Consortium

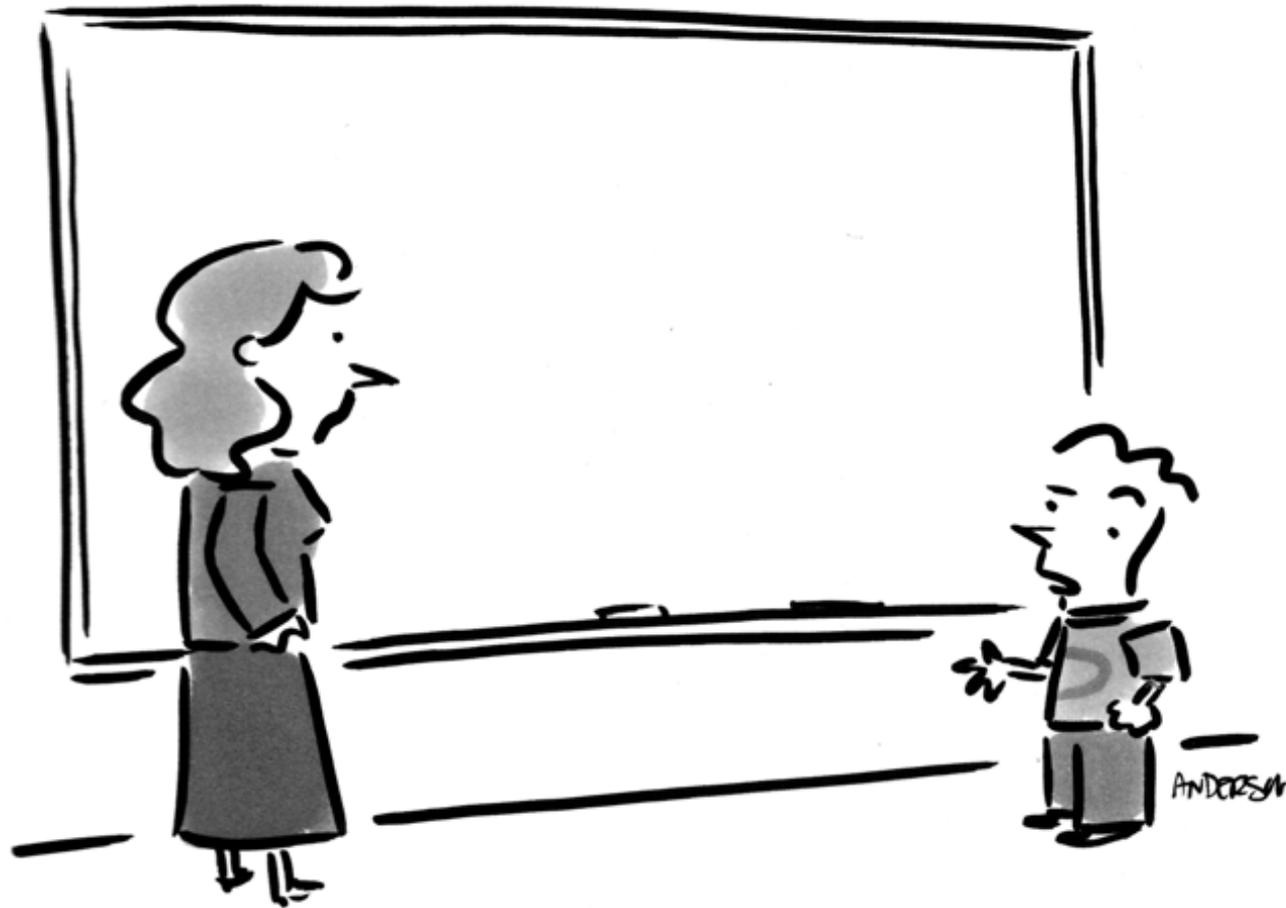
Wednesday, Feb 12, 2020
1:00 PM - 3:00 PM
B234

Student Data Privacy: What Are YOUR Obligations?

Steve Smith, CIO Cambridge Public Schools Cambridge MA
Larry Fruth II PhD, Executive Director/CEO Access 4 Learning

Feb 2020





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



Why Do I Have to Worry About Student Privacy?

- **The What: Student Data**
- **The Why: Legal Implications**
- **The How: Student Data Privacy Alliance and Partners**
- **The Where: Resources**



EDTech in Schools



Technology

Explosion of technology in schools



1:1 Programs

Most districts have some sort of 1:1 program



Chromebooks

Now in 70% of U.S. schools



2018 EdTech market

In the U.S it is worth over \$8.38B.



Online Resources

The average U.S. school employs 400 to 1000 online tools/apps (whether then know it or not)

.... and then there is.....

Student Privacy – The What



Information that is tied to individual students is referred to as personally identifiable information, or PII, and is subject to additional restrictions in laws and regulations.

- Any information about a student's identity, academics, medical conditions, or anything else that is collected, stored, and communicated by schools or technology vendors on behalf of schools that is particular to that individual student.
- This includes name, address, names of parents or guardians, date of birth, grades, attendance, disciplinary records, eligibility for lunch programs, special needs, and other information necessary for basic administration and instruction.
- It also includes the data created or generated by the student or teacher in the use of technology – email accounts, online bulletin boards, work performed with an educational program or app, anything that is by or about the student in the educational setting.
- Some student personal information such as social security number, is highly sensitive and collection may be barred by state law.

Student Privacy Laws – The Why



CIPA

Children's
Internet
Privacy Act

PPRA

Protection
of Pupils
Rights
Amendment

COPPA

Children's'
Online
Privacy &
Protection
Act

HIPAA

Health
Insurance
Portability &
Accountability
Act

FERPA

Family
Educational
Rights &
Privacy Act
(1974)

STATE LAW

Ohio
Legislation
Local Statutes
and
Regulations

Student Privacy Laws

CIPA

Children's Internet Privacy Act

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.



Student Privacy Laws

PPRA

Protection of Pupils Rights Amendment

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.)



Student Privacy Laws

COPPA

Children's' Online Privacy & Protection Act

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.

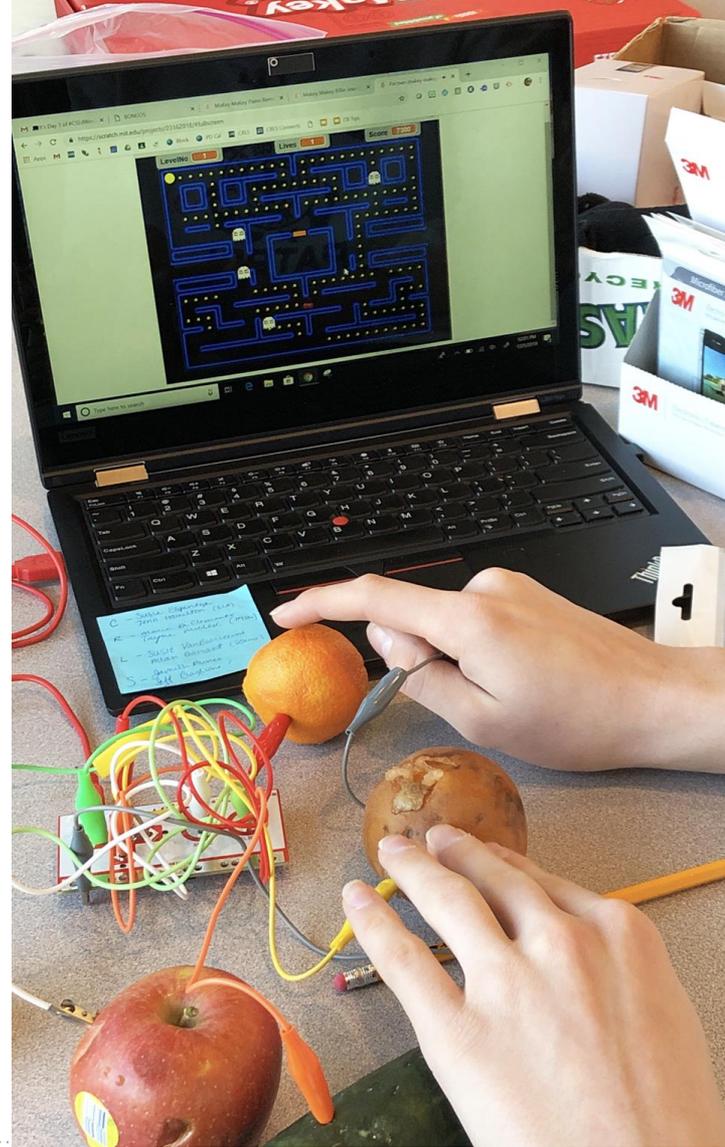


Student Privacy Laws

HIPAA

Health Insurance Portability & Accountability Act

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.

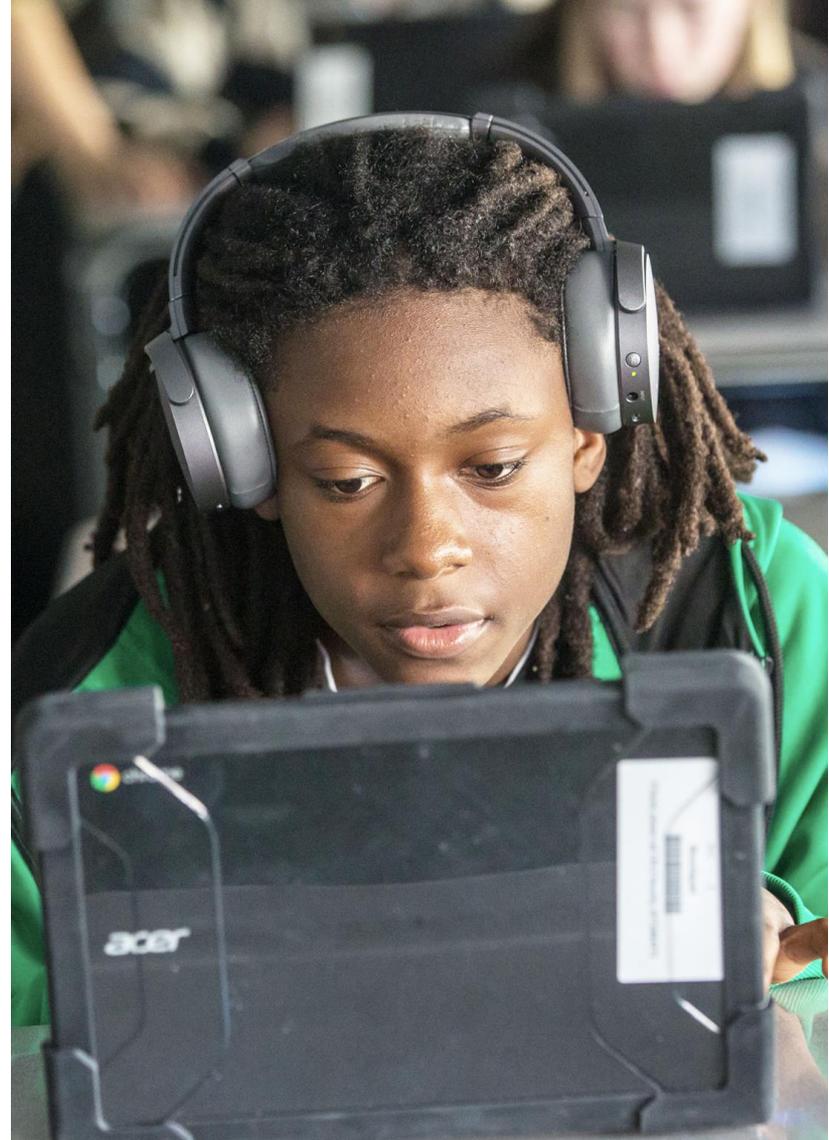


Student Privacy Laws

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).



FERPA (1974)



When FERPA was written....



....“cannot share records without parental consent”



FERPA Exceptions

Other schools to which a student is transferring;

1

Specified officials for audit or evaluation purposes;

2

Appropriate parties in connection with financial aid to a student;

3

Organizations conducting certain studies for or on behalf of the school;

4

Accrediting organizations;

5



To comply with a judicial order or lawfully issued subpoena;

6

State and local authorities, within a juvenile justice system, pursuant to specific State law.

7

Appropriate officials in cases of health and safety emergencies;

8

School officials with legitimate educational interest;

9

Student Privacy Laws



FERPA

School officials with legitimate educational interest;

- Performs an **institutional service** or function for which the school or district would otherwise use its own employees;
- Has been determined to meet the criteria set forth in in the school's or district's annual notification of FERPA rights for being a school official with a **legitimate educational interest** in the education records;
- Is under the **direct control of the school** or district with regard to the use and maintenance of education records; and
- Uses education records **only for authorized purposes** and may not re-disclose PII from education records to other parties (unless the provider has specific authorization from the school or district to do so and it is otherwise permitted by FERPA).

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.
- Indemnification and Warranty Provisions.

So what happens next?



InBloom

\$100M investment by Gates to solve K12 data management issue

Good idea right?

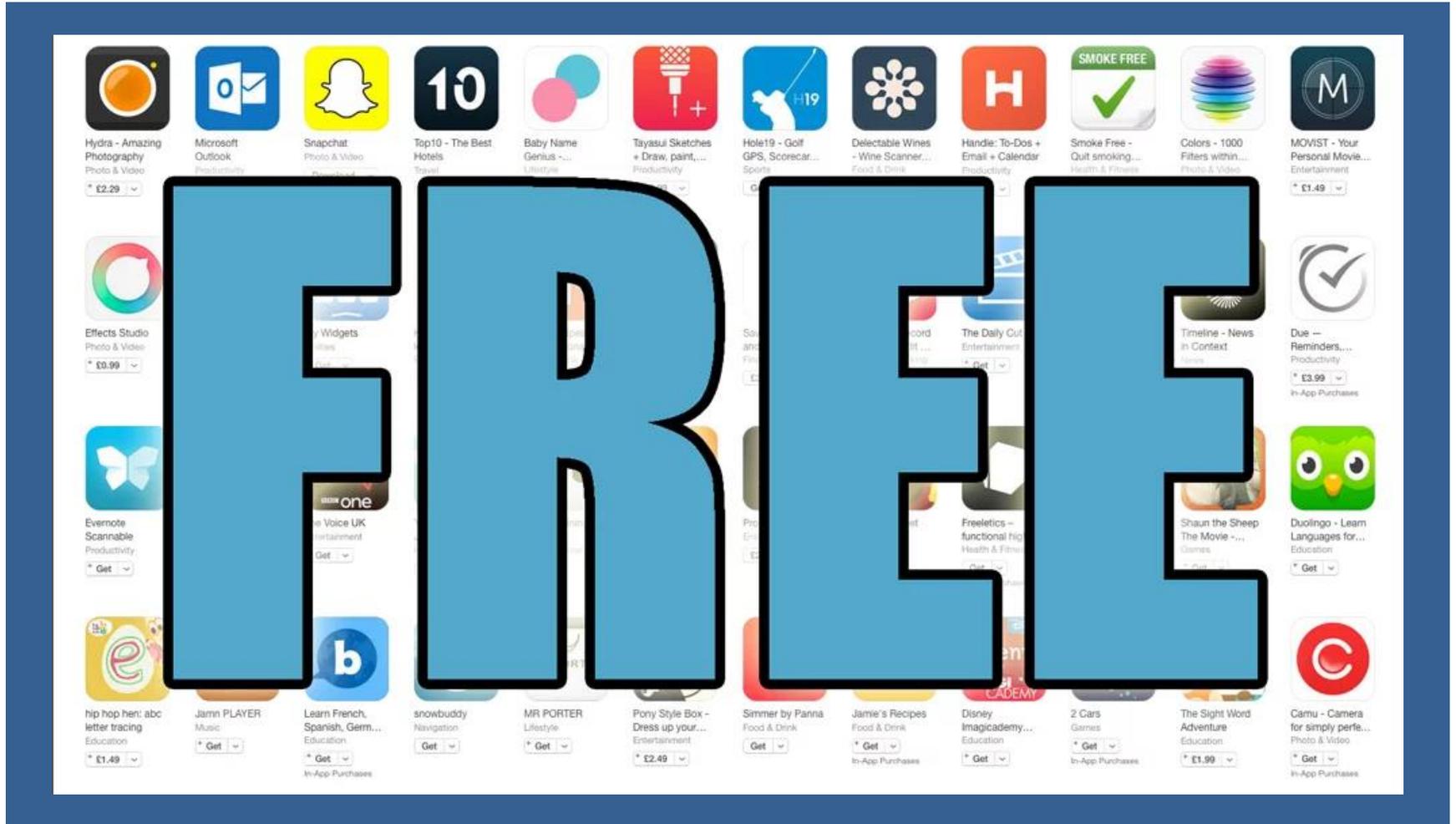


InBloom =



**Privacy
Explosion
in USA**

The BIG Question:



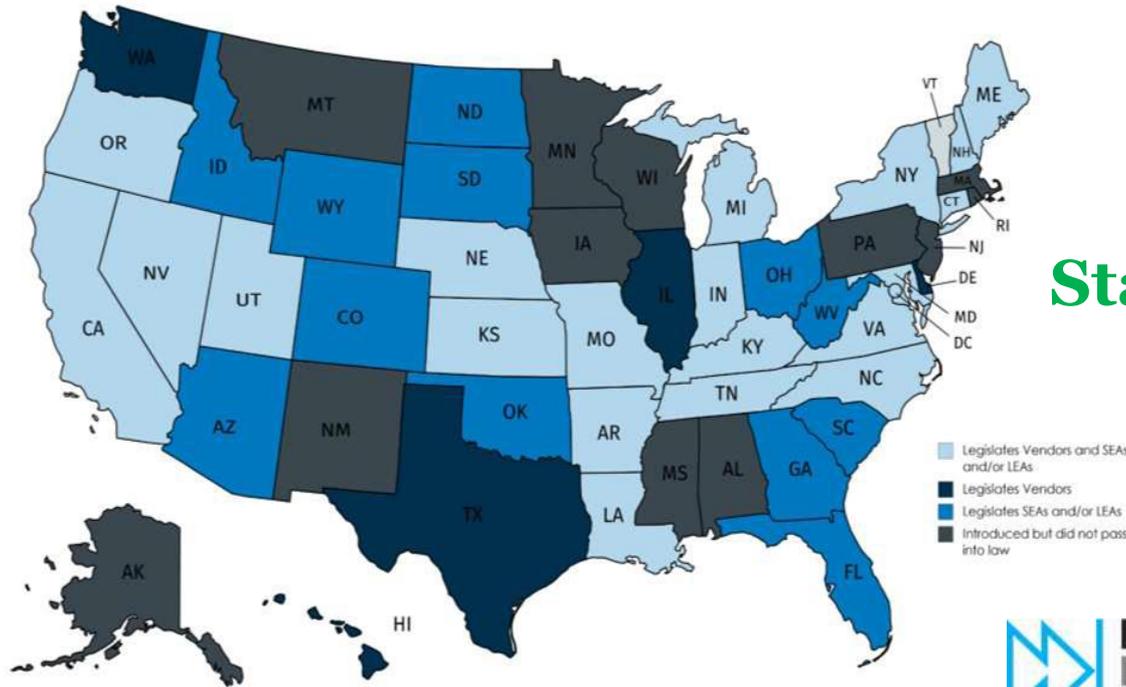


Student Privacy Laws

STATE LAW

40

States Have Passed 125
Laws Since 2013



What Would You Do?

- 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?**
-

BREAK

SDPC Origin

The SDPC:

- Built upon work done in CPS
- 12+ years working with vendors
- Developed in house tools
- Awareness building
- Standardized DPAs
- Expanded across MA

The screenshot shows the Cambridge Public Schools website's Student Data Privacy page. The browser address bar displays the URL: cpsd.us/cms/One.aspx?portalId=3042869&pag.... The website header includes the Cambridge Public Schools logo and navigation links for School Registration, Calendar, Employment, and Contact CPS. A secondary navigation bar lists STUDENTS & FAMILIES, TEACHERS & STAFF, and WORK FOR CPS. The main navigation menu includes HOME, SCHOOLS, CURRICULUM, ADMINISTRATION, and SCHOOL COMMITTEE. The page title is "Student Data Privacy" under the "Privacy" sub-section. The content area features six resource icons: Request New Resource (For Staff Only), Professional Development, CPS Digital Resource List, Legal Resources, Student Use of Computers at Home, and Forms, Policies & Procedures. Below these are sections for "FOR STAFF" and "FOR FAMILIES". The "FOR STAFF" section includes "Why Student Data Privacy Matters" (Cambridge Public Schools privacy and data policies ensure that the District is ethically and legally protecting student safety and student information, including student work. Protecting students from harm—identity theft, harassment and unauthorized data collection—are critical concerns. As an educator, it is our job to ensure our students are protected in this manner. [Read FAQs >>](#)), "Latest CPS Approved Resources" (Assess Assessment, O'Conner Studies, Cofield, Gekko Photography, and Inqury (Video game for Declaration of Independence, 8th grade civics course) [View full list >>](#)), and "Trusted Learning Environment" (CPS strives to ensure the protection of our students' privacy while at the same time enabling innovative uses of technology to support teaching and learning. [Read on >>](#)). The "FOR FAMILIES" section includes "Why Student Data Privacy Matters" (In today's world of advancing online resources teachers, students, and parents are benefiting from an ever-increasing wealth of tools to support teaching and learning. The growth in these tools is extraordinary with great potential to improve student outcomes. Along with this explosion in growth of online learning tools, comes the inherent risks of leakage of student data and understandable concerns over student privacy. [Read FAQs >>](#)) and "5 Top Student Data Privacy Resources" (1. [Family Policy Compliance Office](#), 2. [Student Privacy 101: FERPA for Parents and Students](#), 3. [A Parents Guide to Student Data Privacy](#), 4. [Why Education Data?](#), 5. [Privacy Initiative](#)). The footer contains the Cambridge Public Schools contact information (135 Berkshire Street, Cambridge, MA 02141, 617.549.8400), a CONTACT US button, and social media links for Facebook, Twitter, Instagram, LinkedIn, and YouTube. It also includes a Privacy Policy, Web Accessibility Statement, Disclaimer, City of Cambridge's Website, and Webmaster links, along with a copyright notice: Website by [GlobeNewswire/Phonix](#) © 2019 Intra Corporation. All rights reserved.



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

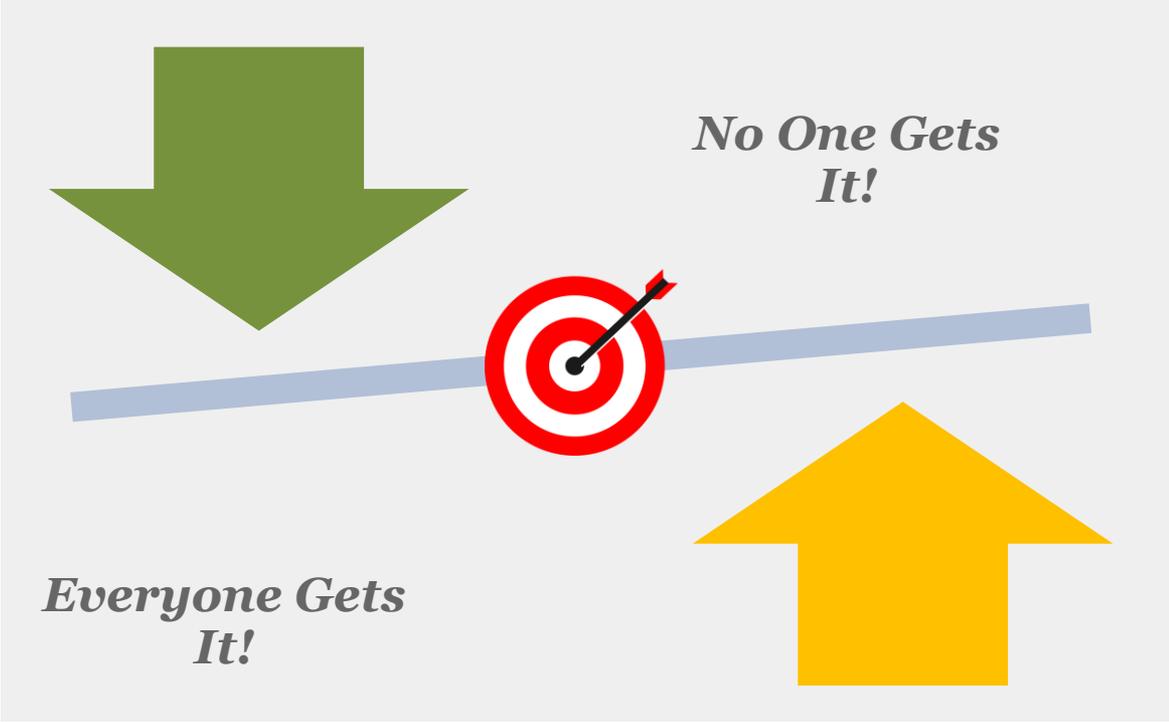
SDPC:

- 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

Its Not "One or the Other"!



Student Data Privacy Consortium



SDPC Goals

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

4 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

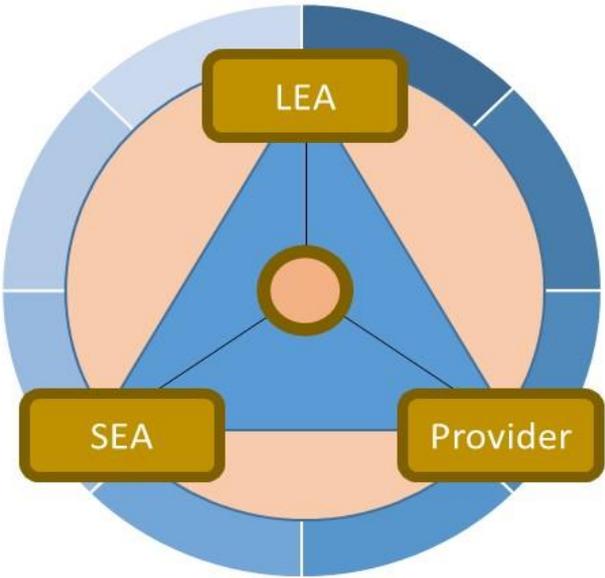
2 Development of **tools and resources** to address operational issues not currently being addressed

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

3 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



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

SDPC Origin

1

2015

Began due to numerous stakeholders addressing data privacy “Pain Points”

2

Guidance

Maintains its own governance, oversight, and resource support

3

Supported

Through membership dues

4

SIG

Organized as a Special Interest Group (SIG) under the Access 4 Learning Community (a 501c3 Member Tech Standards Organization)

5

Members

Include schools, districts, regional and state education agencies, other professional organizations, and marketplace providers



Student Data Privacy Consortium

- ✓ Application Resource Registry – Check the Apps!
- ✓ National Data Privacy Agreement Clause Set
- ✓ Automate and Certify Software Contract Privacy Obligations
- ✓ Privacy Effective Practice Sharing Tools
- ✓ A Growing International Community Setting Clear Expectations Between Vendors and Customers
- ✓ Three dozen vendor members

Privacy – By The Numbers...

the Student Data Privacy Consortium (SDPC)

28



32million



Students supported
by Tools

8750+



School Districts
represented

4



Countries Collaborating
on Privacy Issues

5332



Signed Vendor
Agreements

3618



Applications in
Database

4108



Signed "Piggyback"
Exhibit E

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.*

Alliances, Alliances,

Alliance Roles

Participate

in the SDPC and interact with other Alliance members and SDPC Projects

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.

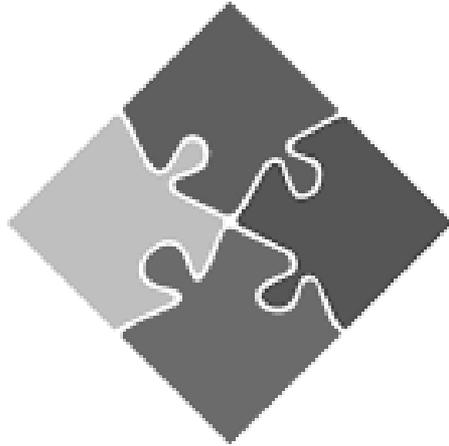
Convene

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.

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.

The Ohio Alliance



Learn21

Leadership · Learning · Logistics

Mission

Learn21 is a nonprofit agency who provides cost-effective instructional technology support, services, and solutions to member educational organizations.



<https://www.learn21.org>

Leveraging Each Other's Work

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.

SDPC Resource Registry

The screenshot shows the SDPC Resource Registry website. The browser address bar displays <https://sdpc4.org>. The website header includes navigation links: "About the Consortium", "Projects / Initiatives", "Get Involved", "Members and Partners", and "Login". Below the header is a green banner with the text "SDPC Resource Registry" and a photograph of students working at computers. A green bar below the banner contains the text "Welcome | Login". The main content area is divided into four columns:

- About SDPC:** A section with a small image and text describing the Student Data Privacy Consortium (SDPC) as a unique collaboration of schools, districts, regional, territorial and state agencies, policy makers, trade organizations and non-profits providing addressing real-world, adaptable, and repeatable solutions to growing data privacy concerns. It includes links for "View Participating Districts" and "Learn about joining the Alliance", and a "Login" button for existing members.
- State Alliances:** A section with a blue icon and text "Select a state to visit their alliance website." Below this is a "Select a State" dropdown menu and a blue button labeled "Visit an Alliance >>".
- Search the Database:** A section with a small image of people at a table and text "Examine student data privacy agreement information from across the nation." It includes a blue button labeled "Get started >>".
- Quick Stats:** A section with a blue icon and text "We are overflowing with generation. Why not join us? Learn more >>". Below this is a table of statistics: "Nationwide SDPC Stats" showing "# of Countries Participating: 2", "# of States Participating: 22", "# of Districts Participating: 7533", "# of Vendors Participating: 26", and "# of Resources: 206".

At the bottom of the page, there is a blue banner with the text "Are your students safe online? Join us!". The footer contains the words "PAGES" and "CONTACT US" on the left, and social media icons for Facebook, Twitter, LinkedIn, and YouTube on the right.

QUICK
DEMO



Professional Learning.....

Framework for Digital Governance



“The Digital Tools Governance project focuses on developing a comprehensive framework for aligning a school system’s policy landscape, strategic programing, 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.”

Task	Craft a Vision	Assess The Terrain	Develop The Plan	Mobilize and Deploy	Monitor/Adapt
App Vetting	Norming session with identified stakeholders to establish a goal for the identified activity with measurable deliverables, scope and progress data checks	Establish a comprehensive (curriculum, admin, finance, purchasing, etc.) inventory of applications in use including grade level, content area and functional area	Process Steps Established: <ul style="list-style-type: none"> • Approved list check • Assessment Tool • Request Form • Reviewer Descriptions, Process Steps and Timelines 	Communicate and provide training and resources for plan implementation	At contract/agreement end teacher and IT staff review apps/site for continued usage
	Where does application vetting fit in your organization? Develop a stepped centralized process that is simple to follow but allows for multiple, and often, communications	What are other entities doing regarding this task Determine what needs to be vetted; Privacy / alignment accessibility/proper use etc...	Budget implications of the plan <ul style="list-style-type: none"> - Required resources - Consider other vetting resources - e.g. 	Inform staff in process is a tool to cover their legal obligations, best use of school resources and enabling the most learning impact and safety for their students	Direct practitioners to any “approved application” list in use
	Identify the accountability measures and owners and incorporate their ideas, thoughts and brainstorming results	What considerations may impact the developing plans (industry guidance, laws, effective practices, etc.)	What strategies work in the setting you have regarding resources, expertise, time, etc. <ul style="list-style-type: none"> - Include procurement /purchasing office - What to ask – districts need directions 	Generate a simple to simple graphics, modules, etc. used for transparency with admin and public	Application usage information gathered

Framework for Transformative Digital Governance



Professional Learning.....

Framework for Digital Governance

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](#)

Automation

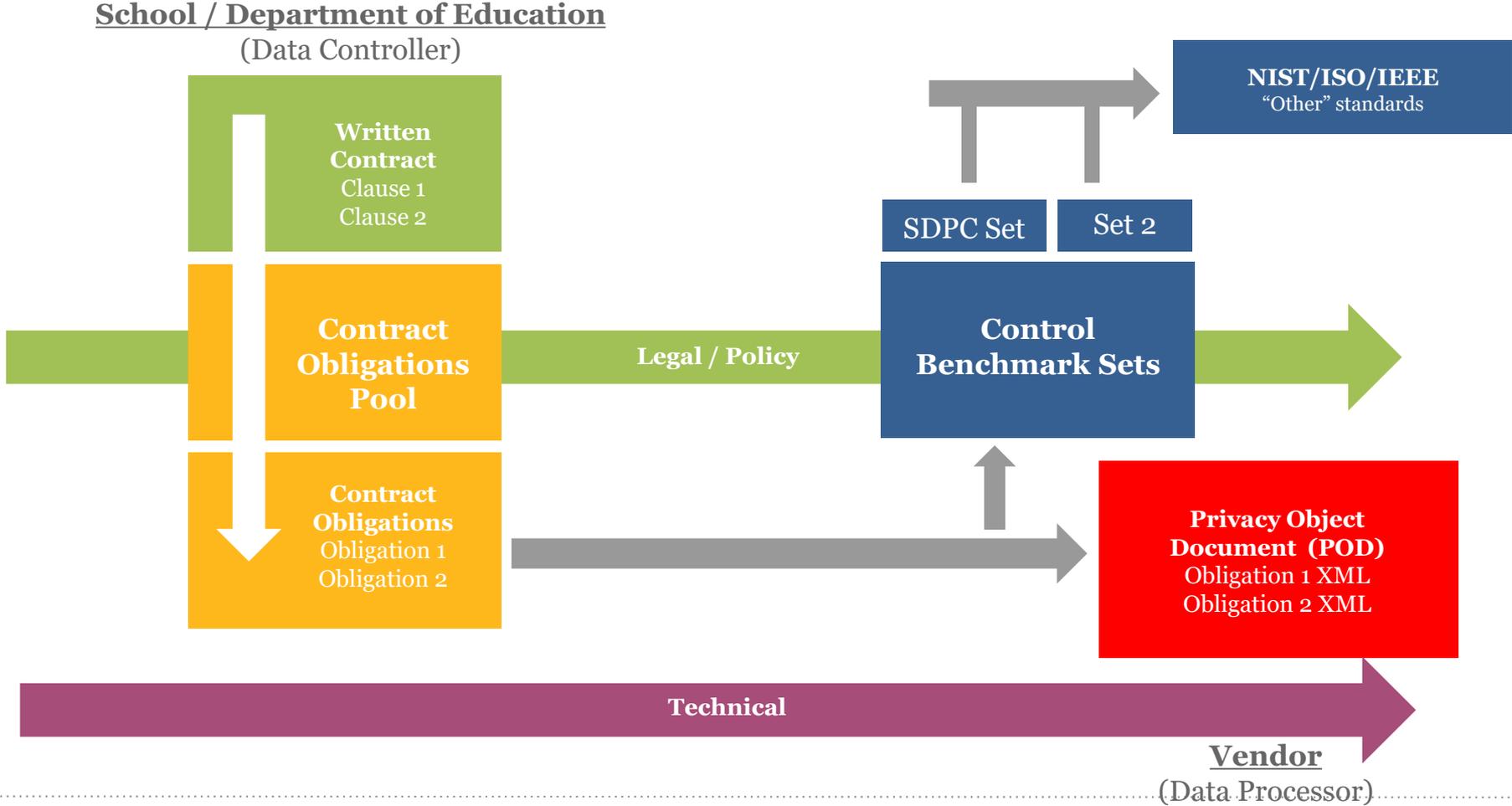
Global Education Privacy Standard (GEPS)

OK the contract is all signed between marketplace provider and customer, the deliverables are clearly outlined and everything is outlined in the roles and responsibilities of each party.

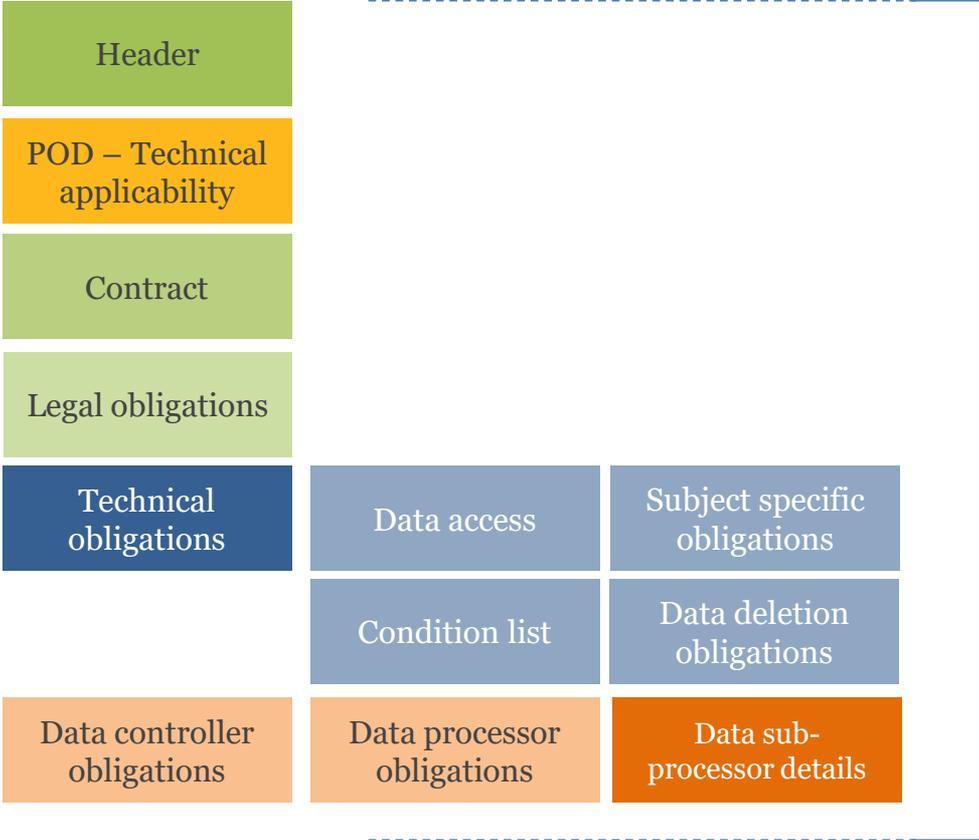
Ready to go, right? No. In most cases the next call between the two parties to answer the question “**How do you want us to deliver on X, Y and Z?**”. This is especially true when it comes to student data privacy issues which usually outlines the need for vendors to use “industry established best practices/standards”. The issue is that for the education vertical, no practices or standards exist.

The **Global Education Privacy Standard (GEPS)**, is a PK-20 global set of data privacy obligations (obligations) that can be aligned to contractual clauses as well as technical control benchmarks. GEPS includes open XML code (PODS) to transfer privacy obligations between controllers and processors to bridge the gap in understand of education data protection expectations. GEPS allows for organizations to choose the SDPC standard suggestions or use other existing standards, (i.e. IEEE, NIST, ISO, etc.) to set their own expectations between vendors and customers on managing student data.

FYI: The Global Education Privacy Standard (GEPS)



Unity Enabling Privacy Expectations



**Automate Contract
Clause Expectations
Exchange and Vendor
Verification**

The “POD”
(Privacy Obligation Document)

Global Education Privacy Standard

POD Creation from Resource Registry

The screenshot shows the homepage of the SDPC Resource Registry. At the top, there is a dark blue navigation bar with icons for home, about, projects, get involved, members, and login. Below this is a green header with the text "SDPC Resource Registry". The main content area features a large banner for the "2019 2nd Annual SDPC Meeting" on April 3, 2019, in Portland, OR. The banner includes a list of topics: Contract Framework Update, Digital Governance Tool Update, Workshop on the SDPC Global Education Privacy Standard, and Student Privacy Boot Camp for non-SDPC members. A "Register" button is also present. Below the banner is a "Welcome" section with four columns of content: "About SDPC" (describing the consortium), "State Alliances" (with a dropdown menu and "Visit an Alliance" button), "Search the Database" (with a "Get started" button), and "Quick Stats" (showing participation numbers for countries, states, districts, vendors, and resources). A yellow banner at the bottom asks "Are your students safe online? Join us!". The footer contains "PAGES" (About the Consortium, A4L Community), "CONTACT US", and social media icons for Facebook, LinkedIn, Twitter, YouTube, and Instagram.

SDPC Resource Registry

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

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

[Register >](#)

**Begins immediately following the CoSN closing ceremony.*

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 A4L Community

CONTACT US

Facebook LinkedIn Twitter YouTube Instagram

GEPS
Manager



Automation & Enforcement

The screenshot shows the SDPC Resource Registry website. At the top, there is a navigation bar with links: "About the Consortium", "Projects / Initiatives", "Get Involved", "Members and Partners", and "Login". Below this is a green banner with the text "SDPC Resource Registry". The main content area features a large image of students working on laptops. Below the image is a green bar with "Welcome | Login". The main content is divided into several sections: "About SDPC" (describing the consortium), "State Alliances" (with a dropdown menu and a "Visit an Alliance >>" button), "Search the Database" (with a "Get started >>" button), and "Quick Stats" (displaying nationwide SDPC statistics). A yellow banner at the bottom reads "Are your students safe online? Join us!". The footer contains "PAGES", "CONTACT US", and social media icons.

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

Leverage SDPC

GEPS
PODS
Integration



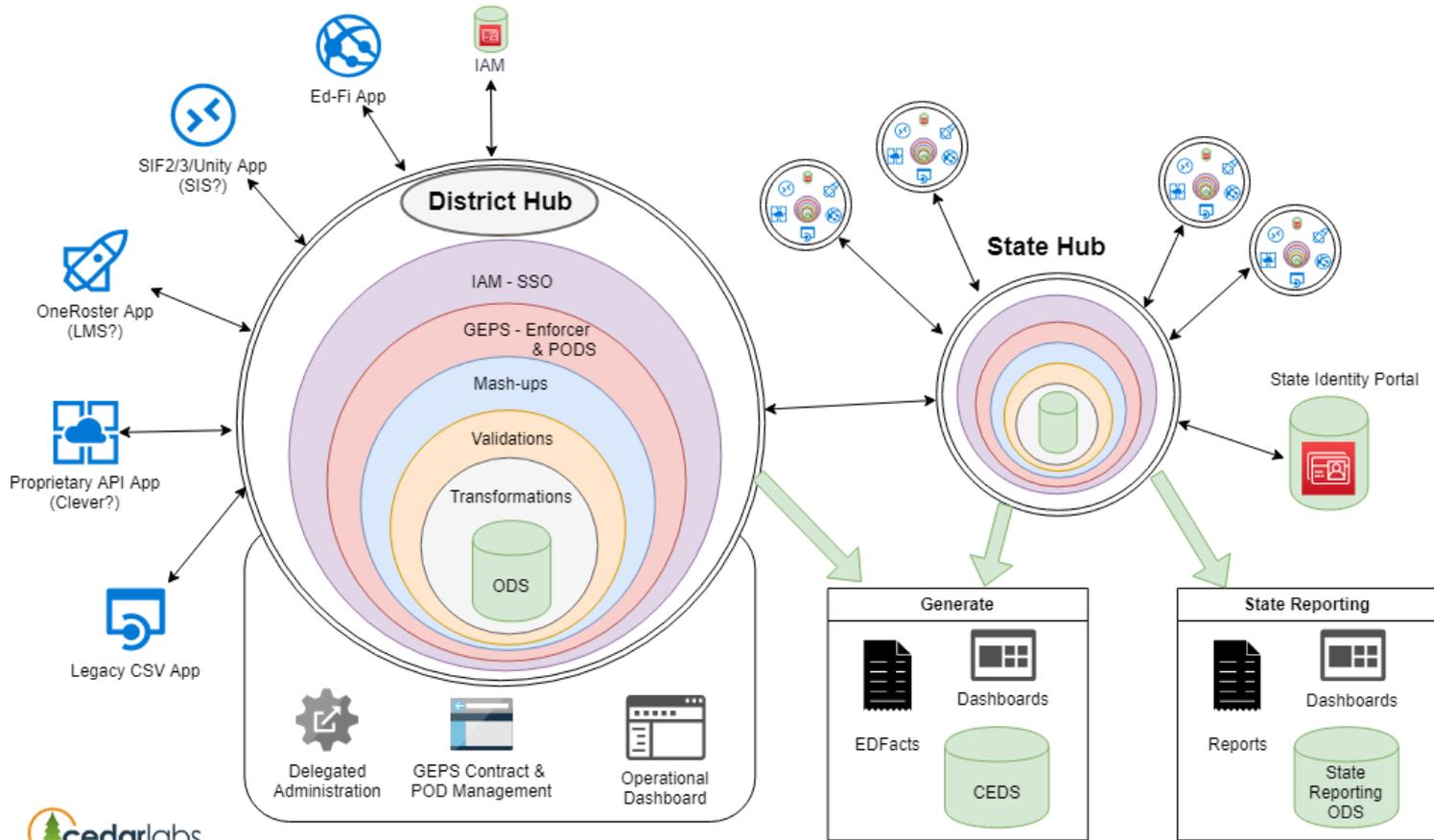
Security Requirements



Enforcement &
Automation

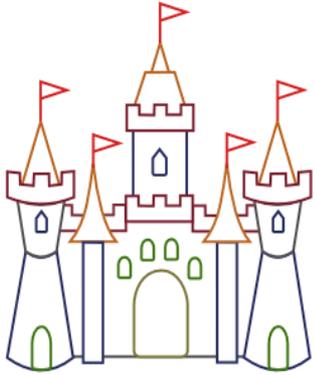
MA Data Hub Services

MA Data Hub





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 Privacy – The How: Questions



Questions:

- Does the product collect Personally Identifiable Information?
- When you cancel the account or delete the app, will the vendor delete all the student data that has been provided or created?
- Do reviews or articles about the product or vendor raise any red flags that cause you concern?
- Does the vendor/product:
 - promise that it provides appropriate security for the data it collects?
 - commit not to further share student information other than as needed to provide the educational product or service? (Such as third-party cloud storage, or a subcontractor the vendor works with under contract.) **The vendor should clearly promise never to sell data.**
 - create a profile of students, other than for the educational purposes specified?
 - show ads to student users? Ads are allowed, but many states ban ads *targeted* based on student data or *behavioral ads* that are based on tracking a student web use.
 - allow parents to access data it holds about students or enable schools to access data so the school can provide the data to parents in compliance with FERPA?
 - claim that it can change its privacy policy without notice *at any time*?
 - say that if the company is sold? The policy should state that any sale or merger will require the new company to adhere to the same protections.

Student Privacy – The Where



[ConnectSafely Educator's Guide to Social Media](#) explains how educators can use social media in the classroom without risking their professional reputation.

[FERPA | SHERPA](#) specific resources for classroom practitioners inside a much larger site that provides service providers, parents, school officials, and policymakers with easy access to materials and resources to help guide responsible uses of student's data.

[Department of Education PTAC](#) videos resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems and other uses of student data.

[Protecting Student Data](#) – Common Sense Media Brief and short checklists for teachers

[Utah Board of Education Privacy Videos](#) - GREAT video resources for all audiences

Join the Ohio Alliance Work



Learn 21

Leadership · Learning · Logistics

1. Check out the Resource Registry – No Password Needed!

www.SDPC.A4L.org

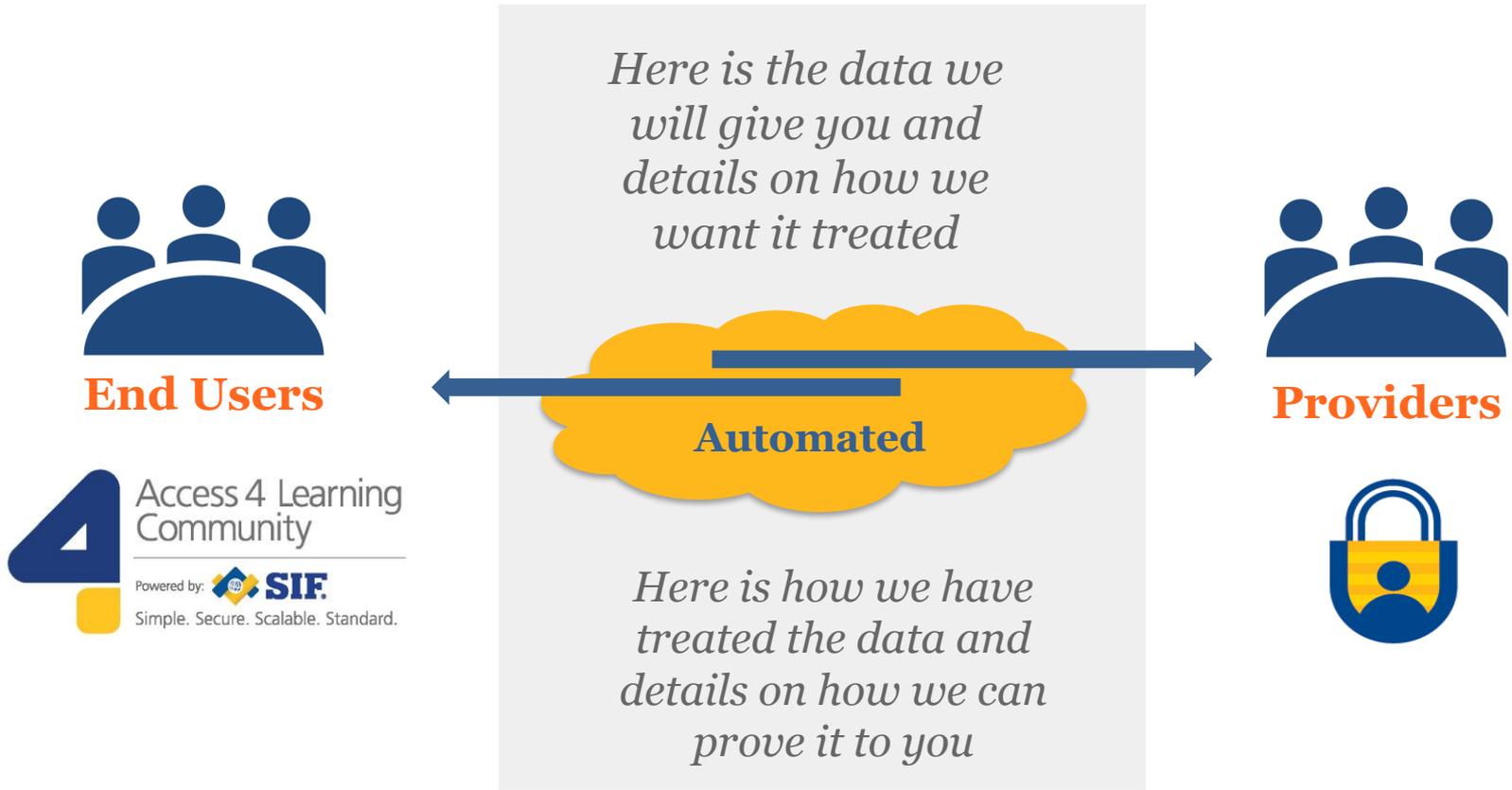
2. Check the Ohio Alliance Site

https://sdpc.a4l.org/view_alliance.php?state=OH

3. Request – or push your tech support – to get an account and join free! https://sdpc.a4l.org/add_district_account.php?state=OH

4. Email sent to Learn 21 and will provide you with account info to Access the Digital Governance Tools

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.*

Resources



Student Data Privacy Consortium

TRAINING: District Admins
February 25, 2019

**Student Data Privacy Consortium (SDPC)
Application / Resource Registry**



Student Data Privacy Consortium

Student Data Privacy Consortium

Alliance 101 Handbook



A4L



Student Data Privacy Consortium

Student Data Privacy Consortium

'Tactical' Privacy for the Front Lines

<https://privacy.A4L.org>

Over the past 2 years there have been more than 100 student data privacy legislative efforts crafted in more than 35 states with even more activities going on internationally. While most federal, state and territory education agencies voice that they want to support their school's privacy issues, most realize these needs are best addressed locally by practitioners who are most vested in keeping student data secure and private.



In 2015 the non-profit **Student Data Privacy Consortium (SDPC)** was established to address these "tactical" and "on the ground" needs. Formed after a year of research, outreach surveys, and one-on-one conversations, the SDPC is now made up of thousands of schools, regional and state/territory education agencies and marketplace providers identifying common privacy issues and developing solutions that can be put in place at all levels of the education data continuum. Much of the work of the Community is done in formed (green) or forming

Frequently Asked Questions

Find Out More



● **Steve Smith**

ssmith@cpsd.us

● **Larry Fruth II, PhD**

lfruth@a4l.org

<https://privacy.a4l.org>