Student Data Privacy
What is Required
“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

Early Childhood
- Which preschool programs best prepare students for kindergarten?

Schools
- What is the graduation rate by school?
- To what degrees are high school math grades predictors of readiness for college?

HE/FE
- What are the HE/FE transfer and completion rates?

Workforce
- What industries are most employing school and university graduates?
- How successful are university graduates in the workforce by major or credential?
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...

Government level data initiatives / reporting

Regional data initiatives / reporting

Local SIS / MIS

Attendance

HR & Reporting

Library

Grade Book

LMS / VLE

Assessment

Transport
Reality Check: In The News

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

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

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

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

InBloom’s Collapse Shines Spotlight on Data-Sharing Challenges – Education Week 5/21/14

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

Major School Research and Assessment Provider Suffers Data Breach – Education Week 5/21/14
Reality Check: In The News

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

Forty-three states are seeking transparency in student data by prohibiting companies from using it to market to students.

Reality Check: In The News

FTC Seek to Guarantee Consent for Students’ Personal Information - FTC 5/23/14

FTC ranked third in the list of agencies issuing the most identity theft red flag warnings in 2019.

Ed. Dept. Makes Protecting Student Data a High Priority - Education Week 5/21/14

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

FTC Seeks to Guarantee Consent for Students’ Personal Information - FTC 5/23/14

FTC ranked third in the list of agencies issuing the most identity theft red flag warnings in 2019.

Reality Check: In The News

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

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

Reality Check: In The News

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

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

Reality Check: In The News

Would support various proposals regulating how student data is used, including:

- Increasing transparency by requiring schools to notify parents before they share students' personal data with private companies (91%)
- Tighter security standards to protect students' private information that is stored "in the cloud" (89%)
- Making it illegal for schools and education technology companies to sell students' private information to advertisers (77%)
- Restricting companies from using students' online habits and searches on school computers to target online advertisements to them (74%)
- Restricting cloud services like Google from using students' email, online searches, and web history to build a profile of personal data and demographics over time (70%)
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
How are MA districts currently ensuring no student data is “leaking” from your districts?

- Do you have a process to vet and on board applications?
- Are all online applications vetted for privacy?
- Do you have data privacy agreements with all online providers?
- Do your teachers understand the importance of student data privacy?

What else do you lose sleep over?

40 States Have Passed 125 Laws Since 2013

[Map showing states with laws passed since 2013]
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
It's Not “One or the Other”!

Student Data Privacy Consortium

No One Gets It!

Everyone Gets It!

Access 4 Learning Community
Powered by SIF
**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...
<table>
<thead>
<tr>
<th>Year</th>
<th>BILL NUMBER</th>
<th>High Level Summary</th>
<th>Early Ed</th>
<th>K-12</th>
<th>Higher Ed</th>
<th>Vendors</th>
<th>SEAs</th>
<th>LEAs</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>SB 188</td>
<td>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.</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>2017</td>
<td>HB501</td>
<td>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.</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>2018</td>
<td>HB 731</td>
<td>This bill prohibits the state superintendent from storing any PII from students who are homeschooled. 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.</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>
HIPAA
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.

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.

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.)

https://www2.ed.gov/policy/gen/guid/fpco/ppra/parents.html
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
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

Let’s Discuss

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

Let’s Discuss
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.

Mark Williams F3 Law 2018
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

- https://ferpasherpa.org/state-laws/
- https://privacy.a4l.org/
"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
BREAK
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
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.
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
“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
• **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.*
Alliances, Alliances, …..

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

Currently 32 million Students Impacted by over 1650 Applications!
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

✓ **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.
SDPC Resource Registry

Are your students safe online? Join us!
### SDPC Tool

#### Student Data Privacy Consortium

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Application</th>
<th>Status</th>
<th>Agreement Type</th>
<th>Grade Level</th>
<th>Content Area</th>
<th>Data Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Achieve 3000</td>
<td>Achieve 3000</td>
<td>Active</td>
<td>Agreement v2a (includes Terms of Service)</td>
<td>6, 7, 8</td>
<td>English Language Arts</td>
<td>Coming Soon</td>
</tr>
<tr>
<td>Benefitent Technology</td>
<td>Benechet</td>
<td>Active</td>
<td>Legal Drafted Parent Release</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biblionasium</td>
<td>Biblionasium</td>
<td>Active</td>
<td>Legal Drafted Parent Release</td>
<td>K, 1, 2, 3, 4, 5</td>
<td>Library Media</td>
<td></td>
</tr>
<tr>
<td>Sunburst Digital, Inc.</td>
<td>Big Universe</td>
<td>Active</td>
<td>Agreement V1</td>
<td>K, 1, 2, 3, 4, 5</td>
<td>English Language Arts</td>
<td>Coming Soon</td>
</tr>
<tr>
<td>Google</td>
<td>Google</td>
<td>Active</td>
<td>Legal Drafted Parent Release</td>
<td>6, 7, 8, 9, 10, 11, 12</td>
<td>Instructional Technology</td>
<td>Coming Soon</td>
</tr>
<tr>
<td>BrainPOP</td>
<td>BrainPOP</td>
<td>Active</td>
<td>Agreement v2a (includes Terms of Service)</td>
<td>K, 1, 2, 3, 4, 5</td>
<td>Other</td>
<td>Coming Soon</td>
</tr>
<tr>
<td>McGraw Hill Education</td>
<td>Building Blocks</td>
<td>Active</td>
<td>District Modified Contract</td>
<td>K</td>
<td>Math</td>
<td>Coming Soon</td>
</tr>
</tbody>
</table>

#### Contract PDF

- [Contract Page](#)
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

Craft a Vision

- Ensure Accountability Mechanisms and Metrics are Working
- Monitor Metrics and Provide Feedback
- Adapt and Rework as Necessary

Assess the Terrain

- Tone at the Top?
- Policies in Place?
- Stakeholders?
- Risk and Liabilities?
- Ground View?
- Blind Spots?

Monitor and Adapt

- New Policies & Procedures
- Implementation Strategy
- Communications Plan & Documents
- Accountability Mechanisms & Metrics
- Peoples’ Roles & Responsibilities
- Resources Needed

Develop the Plan

- Create Cross-functional Teams
- Communicate Goals, Plans, & Expectations
- Provide Training & Resources
- Fully Engage & Walk the Walk
- Celebrate Accomplishments

Mobilize and Deploy

Know your goal before you begin…
Welcome to the DGT.
Below are the projects and your progress. Click on a project below to get started.
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

<table>
<thead>
<tr>
<th>Purpose of DPA</th>
<th>Nature of Services Provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student Data to Be Provided</td>
<td>Student Data Property of LEA</td>
</tr>
<tr>
<td>Parent Access</td>
<td>Separate Account</td>
</tr>
<tr>
<td>Third Party Request</td>
<td>Subprocessors</td>
</tr>
<tr>
<td>Privacy Compliance</td>
<td>Authorized Use</td>
</tr>
<tr>
<td>Employee Obligation</td>
<td>Non Disclosure</td>
</tr>
<tr>
<td>Disposition of Data</td>
<td>Advertising Prohibition</td>
</tr>
<tr>
<td>Data Security</td>
<td>Passwords and Employee Access</td>
</tr>
<tr>
<td>Destruction of Data</td>
<td>Security Protocols.</td>
</tr>
<tr>
<td>Employee Training</td>
<td>Security Technology.</td>
</tr>
<tr>
<td>Security Coordinator</td>
<td>Subprocessors Bound.</td>
</tr>
<tr>
<td>Periodic Risk Assessment</td>
<td>Data Breach</td>
</tr>
<tr>
<td>Privacy Compliance</td>
<td>Annual Notification of Rights</td>
</tr>
<tr>
<td>Reasonable Precautions</td>
<td>Unauthorized Access Notification.</td>
</tr>
</tbody>
</table>
Global Education Privacy Standard (GEPS)

School / Department of Education
(Data Controller)

Written Contract
Clause 1
Clause 2

Vendor
(Data Processor)

Contract Obligations Pool

Contract Obligations
Obligation 1
Obligation 2

Legal / Policy

Control Benchmark Sets

SDPC Set
Set 2

NIST/ISO/IEEE
"Other" standards

Technical

Privacy Object Document (POD)
Obligation 1 XML
Obligation 2 XML

Global Education Privacy Standard (GEPS) (GEPS)
**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.

<table>
<thead>
<tr>
<th>OBLIGATION</th>
<th>Maintain an accessible practice of destruction of data with adequate reference to definitions and policies in presenting general data retention guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alignment to Known Standards</strong></td>
<td>Present a data retention policy which identifies data classifications, retention schedule, and destruction process in line with data classification level.</td>
</tr>
<tr>
<td><strong>Benchmark</strong></td>
<td>NIST 800-53 (Rev. 4) System And Information Integrity Control Family SI-12 Information Handling and Retention.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OBLIGATION</th>
<th>Properly address and agree to the definition of delete [link. Talk to making unrecoverable, discuss extent such as backups/etc].</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alignment to Known Standards</strong></td>
<td>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).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OBLIGATION</th>
<th>Acknowledge and register adequate signals for the interpretation, operational execution, and notice of deletion requests.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alignment to Known Standards</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Benchmark</strong></td>
<td>NIST 800-53 (Rev. 4) System And Information Integrity Control Family SI-12 Information Handling and Retention.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OBLIGATION</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alignment to Known Standards</strong></td>
<td>NIST 800-53 (Rev. 4) System And Information Integrity Control Family SI-12 Information Handling and Retention.</td>
</tr>
</tbody>
</table>
POD contents (SIF Infrastructure)

- **Header**: Status, Token ID, version, PartyID (e.g., company)
- **POD – Technical applicability**: Default, Data model, Data model version
- **Contract**
- **Legal obligations**
- **Technical obligations**
  - Data access
  - Condition list
- **Data controller obligations**
- **Data processor obligations**
- **Data sub-processor details**

Default can be set. Can repeat if fine grained controls are required.
Introducing “Unity”!

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
It's Not “One or the Other”!

Everyone Gets It!

No One Gets It!
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
SDPC Resource Registry

SDPC Resource Registry

Welcome

About SDPC

The Student Data Privacy Consortium (SDPC) is an unique collaborative of schools, districts, regional, state, and federal partner agencies, policy makers, and schools and districts to address and implement 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 cohosting with participation. Why not join us?

Nationwide SDPC Stats
# of Countries Participating: 1
# of States Participating: 21
# of Districts Participating: 8997
# of Vendors Participating: 20
# of Resources: 1618

Are your students safe online? Join us!

Contact Us

About the Consortium

A4L Community

Are your students safe online? Join us!

About the Consortium

Projects / Initiatives

Get Involved

Members and Partners

Login

Student Data Privacy Consortium
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.