



Student Data Privacy Consortium

“Tactical” Student Data Privacy

SDPC Progression

Stats DC 2018





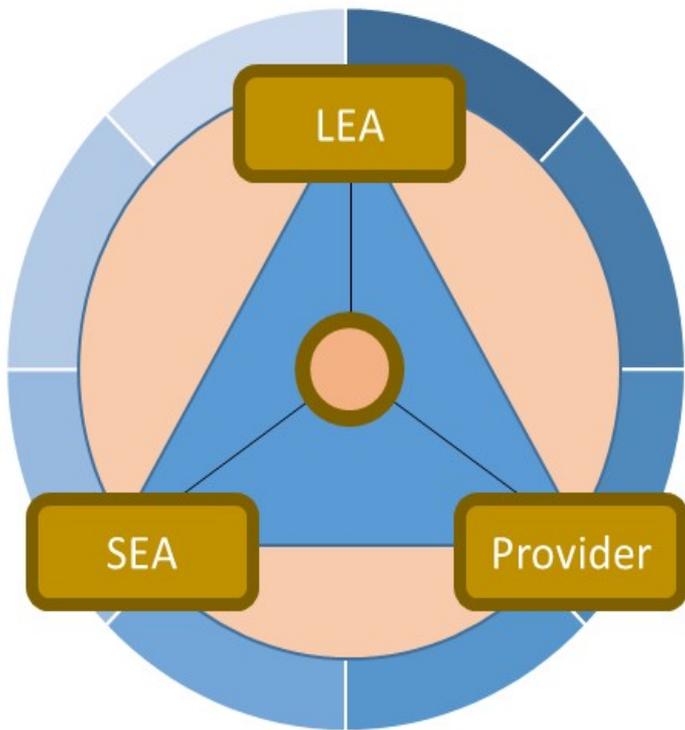
Student Data Privacy Consortium

Misc. “Stuff”

The SDPC:

- **Was started in 2015 due to numerous stakeholders addressing data privacy “Pain Points”**
- **Is organized as a Special Interest Group (SIG) under the Access 4 Learning Community (a 501c3 Member Tech Standards Organization)**
- **Maintains its own governance, oversight and resource support**
- **Has schools, districts, regional and state education agencies, other professional organizations and marketplace providers as members**
- **Is supported through membership dues**

“Big Picture” Strategy



-  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



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 Tactical Privacy Projects

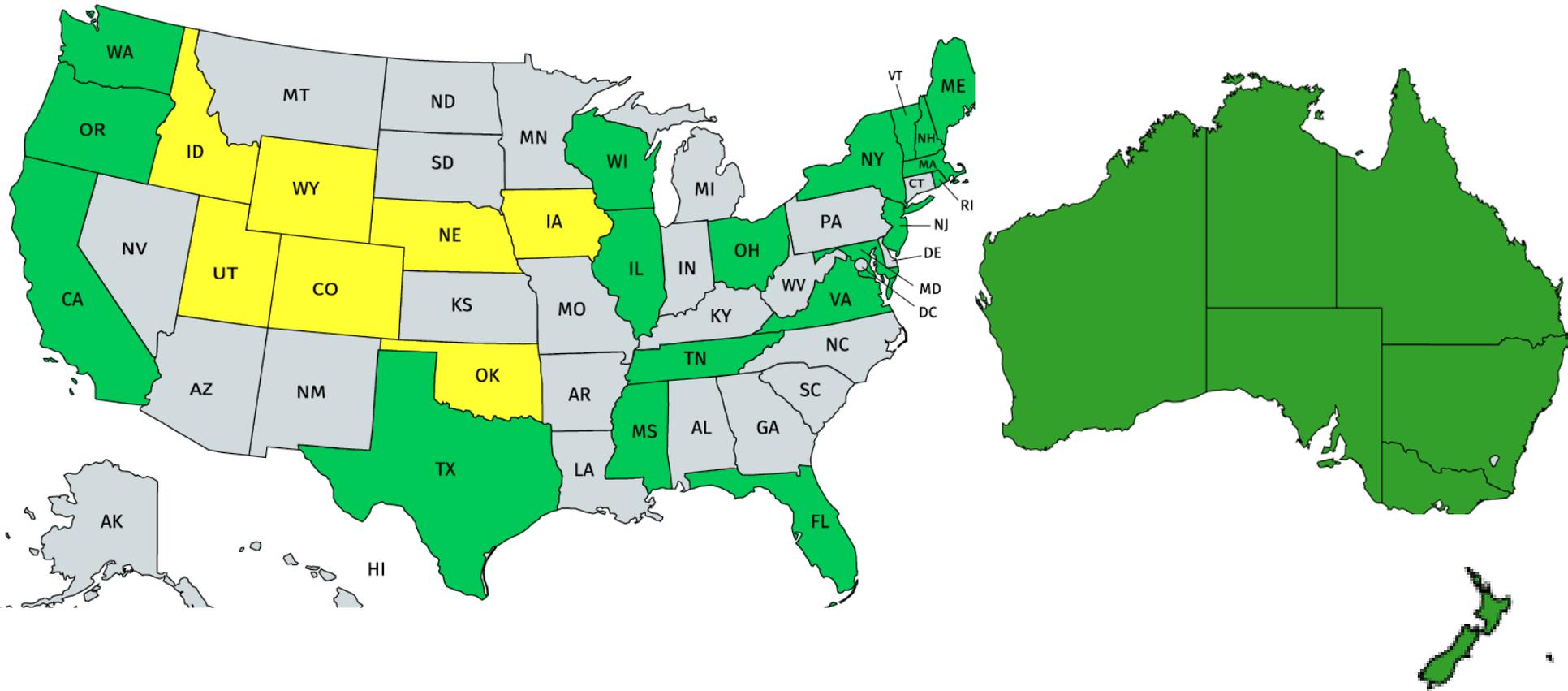
- **Project 1: Privacy Contract Framework**

- *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 20 million Students Impacted by over 1250 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 App”



[About the Consortium](#) [Projects/ Initiatives](#) [Get Involved](#) [Members/Partners](#) [SDPC App](#) [Login](#)



[About Student Data Privacy Consortium](#)

[View Participating Districts](#)

[Learn more about Joining the Alliance >>](#)
[Already a Member? District Login](#)
[Vendor Login](#)



Useful Links

- [California Student Privacy Alliance](#)
- [Maine Student Privacy Alliance](#)
- [Maryland Student Privacy Alliance](#)
- [Massachusetts Student Privacy Alliance](#)
- [Rhode Island Privacy Alliance](#)
- [Texas Student Privacy Alliance](#)
- [Virginia Student Privacy Alliance](#)
- [Washington/Oregon Student Privacy Alliance](#)

[Search the Database >>](#)



Are your students safe online? [Join us!](#)



Student Data Privacy Consortium

SDPC Tools for Districts

MSPA | Tools for Participating Districts

Secure | <https://secure2.cpsd.us/mspa/tools.php?districtID=457>

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](#)

https://secure2.cpsd.us/mspa/edit_agreement_info.php?districtID=457



Contract Management

MSPA | District Profile x

Secure | https://secure2.cpsd.us/mspa/edit_agreement_info.php?districtID=457

Apps | Bookmarks | Cambridge Public Sc | Google Drive | Supervisor Web Ser | Helpdesk | ASPEN | School Stream | The Boston Globe ef | Cambridge Chronicle | CD | Cambridge Day

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

Show 10 entries Search:

Software Name	Agreement Status	Agreement Type	Agreement Dates	Export All to Excel
AP Registration Service Company Name: Total Registration Requested by: Sherry Madden	Active	Agreement V4 School Year: 2016 - 2017 Location: CRLS	Approved: 2017-02-10	Agreement: Change Agreement Type Edit Other Info Delete Application: Edit Data Elements: Add Edit Upload Agreement: Signed Annotated Vendor-Specific
ABC Mouse Company Name: ABC Mouse Requested by: Siobhan Patterson	New Request Progress Update: Contract Sent Last Modified: 2017-07-31	Location: KLO	Approved: Expires:	Agreement: Change Agreement Type Edit Other Info Delete Application: Edit Data Elements: Add Edit Upload Agreement: Signed Annotated Vendor-Specific Progress Log: Add View
ACE ABA Software System Company Name: The New England Center for Children Requested by: Karyn Grace	New Request Progress Update: Contract Sent Last Modified: 2017-08-01	Location: FMA, King Open Cost: \$14,679	Approved: Expires:	Agreement: Change Agreement Type Edit Other Info Delete Application: Edit Data Elements: Add Edit Upload Agreement: Signed Annotated Vendor-Specific Progress Log: Add View

Progress:

Progress Admin:

Progress:

Progress Admin:

Achieve 3000 Active Agreement V2a Approved: Agreement: [Change Agreement Type](#) |



Student Data Privacy Consortium

Vendor Tools

The screenshot shows a web browser window with the following elements:

- Browser Tabs:** MSPA | Welcome, SDPC | Tools for Participa...
- Address Bar:** Secure | https://secure2.cpsd.us/a41/company_tools.php
- Navigation Menu:** About the Consortium, Projects/Initiatives, Get Involved, Members/Partners, SDPC App, Logout
- Header Image:** A grayscale photograph of hands typing on a keyboard.
- Breadcrumbs:** [Student Data Privacy Consortium](#) > Tools for Participating Vendors
- Section Header:** Tools for Participating Vendors
- List of Tools:**
 - [Vendor Marketplace](#)
 - [Breach Notification](#)
 - Project 2 Vendor Templates
 - [Email Districts with Signed Contracts](#)
- Vendor Area Card:**
 - Icon:** A blue square with a white person icon and the word "MEMBER" below it.
 - Title:** Vendors Area
 - Links:**
 - [Edit Account Information](#)
 - [Add Resource](#)
 - [View Agreements](#)
 - [Email Participants](#)
 - [Validate Resources](#)
 - [Tools for Vendors](#)
 - [Logout](#)



Student Data Privacy Consortium

Public Search

Steve

MSPA | Search

Secure | <https://secure2.cpsd.us/mspa/search.php>

Massachusetts Student Privacy Alliance > Search

Search the MSPA Database

Search By District Name

District:

Name:

Search By Resource Name

Resource Name:

Search By Agreement Type

Agreement Type:



How can we help you?

[Learn about MSPA](#)

[View Participating Districts](#)

Download Student Data Privacy Agreement

[Learn about Agreement Types >>](#)

Version 4: [pdf](#)

Version 3: [pdf](#)

Version 2a (includes Terms of Service): [pdf](#)

Version 1: [pdf](#)

[Member Login](#)



Student Data Privacy Consortium

SDPC Tactical Privacy Projects

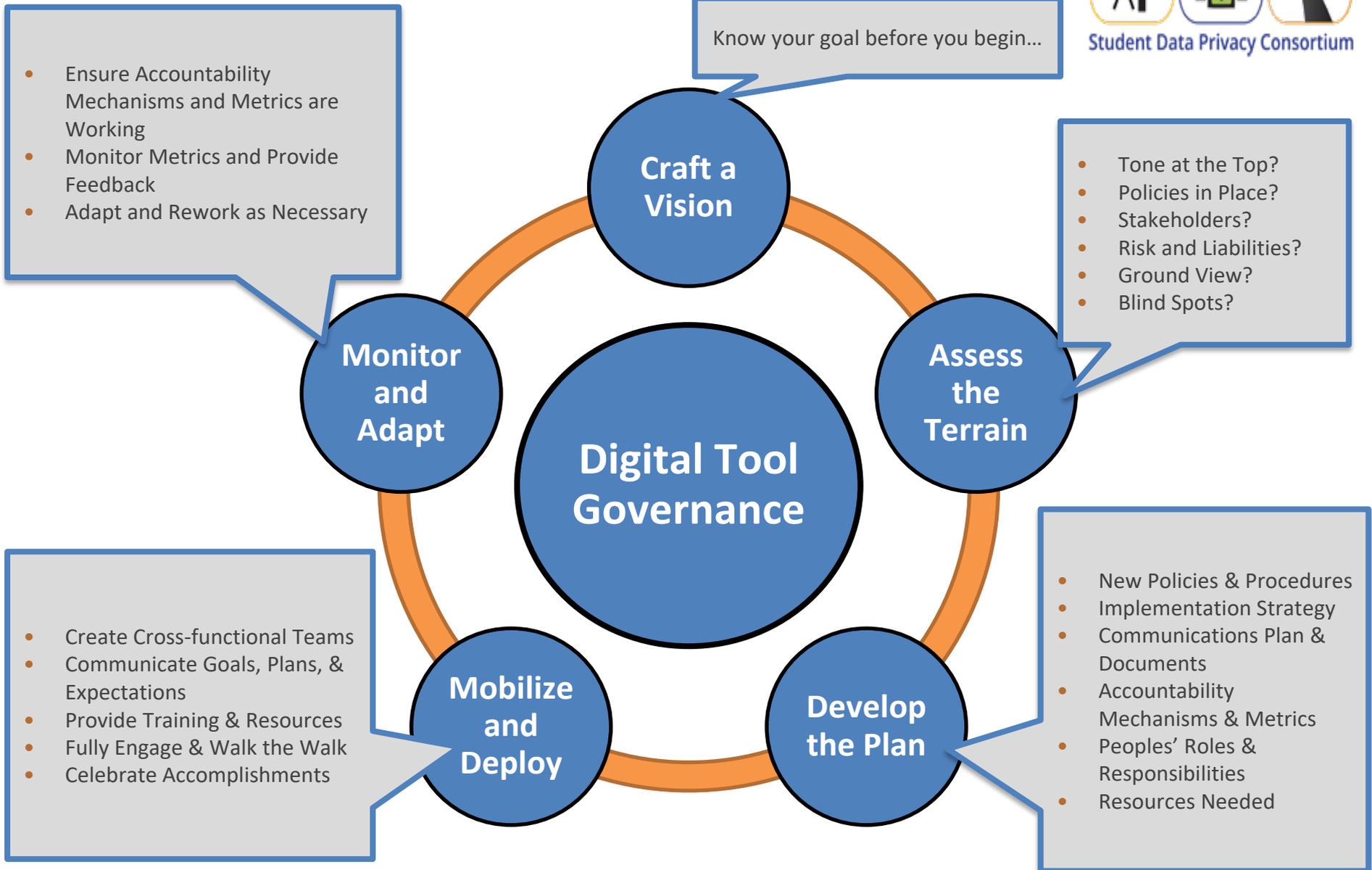
- **Project 1: Privacy Contract Framework**

- *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.*

- **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



Example Use Case: District Data Privacy and Security Professional Learning

Craft a Vision	Assess The Terrain	Develop The Plan	Mobilize and Deploy	Monitor and Adapt
<p>Description: Develop a vision, mission, and goals to create awareness of the importance of data privacy and security program through professional learning for all staff</p>	<p>Description: Determine what practices are currently in place, and their effectiveness, in order to create a gap analysis that will guide planning for improvement, resource allocation and implementation.</p>	<p>Description: Establish roles, responsibilities, resources, and timelines for tasks required to establish or improve a formal data privacy and security professional learning program.</p>	<p>Description: Utilizing previously acquired information, and a documented implementation plan, launch formal awareness campaign and professional development activities</p>	<p>Description:</p>
<p>Characteristics: Focus on why a privacy program is important (communicate with different stakeholders (community, parents, staff) to promote transparency and responsible use of data to create confidence of stakeholders (not fear) is on culture change rather than compliance</p>	<p>Characteristics:</p> <ul style="list-style-type: none"> • What formal policies and procedures exist to address student data privacy? • Determine stakeholders that have access to student PII • Evaluate access to data systems to determine if either technical or administrative controls are in place • What existing PD resources/mechanisms currently exist to support professional learning, and what resources need to be acquired? 	<p>Characteristics:</p> <ul style="list-style-type: none"> • Training/Onboarding of new staff • Training of existing staff • What technical/administrative access controls need to be established? How will those be created? • Communication to parents, community, staff • Formal documentation of who has been trained 	<p>Characteristics:</p> <ul style="list-style-type: none"> • Establish formal responsibility to a district level position for implementation and sustainability • Communicate vision • Embed learning about responsible use of student data and privacy in any and all trainings, meetings, etc, where student data is used or referred to. • Provide various methods of PD/communication of information (video, FAQ, in person, meeting protocols, etc) • Signed data use agreements 	<p>Characteristics:</p> <ul style="list-style-type: none"> • Keep apprised of new policy (federal, state, local) that needs to be incorporated into training and reference resources. • Scenario based “quiz” to gauge understanding • Establish a means for receiving questions and providing answers ongoing • Update training and FAQ • Yearly “refresher” offered for existing staff • Track who has received PD and who has not

Framework for Transformative Digital Governance



Student Data Privacy Consortium

MSPA | Welcome x Digital Governance Tool x Steve

Secure | https://secure1.cpsd.us/dgt/

Apps Bookmarks Cambridge Public Sc Google Drive Supervisor Web Serv Helpdesk ASPEN School Stream The Boston Globe eF Cambridge Chronicle

About the Consortium Projects/Initiatives Get Involved Members/Partners SDPC App

Digital Governance Tool (DGT)

This 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.

Username Password

Login to the DGT

Framework for Transformative Digital Governance



MSPA | Welcome x Digital Governance Tool | x

Secure https://secure1.cpsd.us/dgt/home.php

Apps Bookmarks Cambridge Public Sc Google Drive Supervisor Web Serv Helpdesk ASPEN School Stream

About the Consortium Projects/Initiatives Get Involved Members/Partners SDPC App

Digital Governance Tool (DGT)

Student Data Privacy Consortium

Welcome to the DGT.

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



Policies

1 2 3 4 5



Resource Vetting

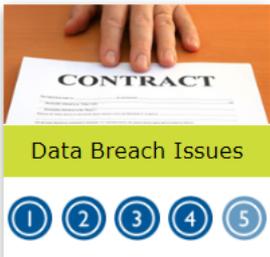
1 2 3 4 5



Staff PD

1 2 3 4 5

[View the Project Report](#)



Data Breach Issues

1 2 3 4 5



Technical Cyber Security

1 2 3 4 5



Procurement

1 2 3 4 5

[Shared Resources](#)

[My Shared Resources](#)

[Shared Digital Governance Plans](#)

View Your District's Digital Governance Plan →



Student Data Privacy Consortium

SDPC Tactical Privacy Projects

- **Project 3: Privacy Connect**

- *Teacher A finds the greatest application in the world to teach his/her subject matter to students. What does it take from him/her asking for the application to be used with his/her students to having students using the application?"*. This may include various owners (legal, technical, fiscal, etc.), critical areas of concern (privacy, security, parental notice, etc.) and impact (academic alignment, usage, other options, etc.). The “Connect” project’s focus is to see how many of these steps can be standardized, automated, or establish effective practices so we all are not starting from scratch each time. The goal is to streamline application selection, vetting, on boarding (sharing properly protected data elements), and final implementation with marketplace norms.



Project 3: SDPC Tactical Privacy “Connect”

Goal: *Support data stewards and their institutions to address student data privacy from application identification to application utilization.*

- **Application Vetting** (Digital Tools Governance/SDPC App)
- **Privacy Contract Wording** (Contract Builder)
- **Technical Requirements** (Technical Standards)
- **Workflow Automation** (SDPC Application)
- **Automate Data Exchanges via Privacy Requirements** (TBD)
- *Stakeholder Communications at Each Step*





Student Data Privacy Consortium

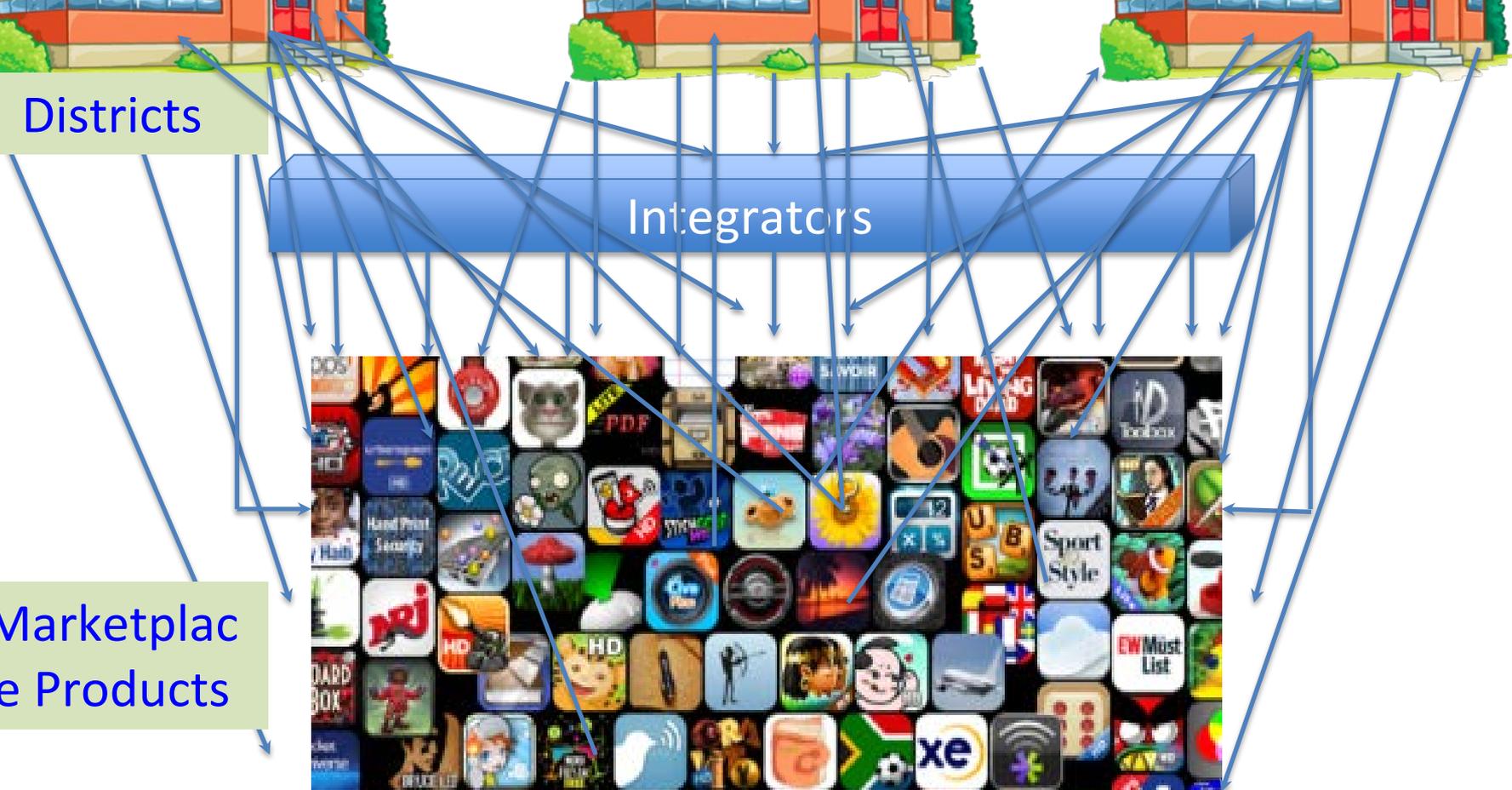
The Current World



Districts

Integrators

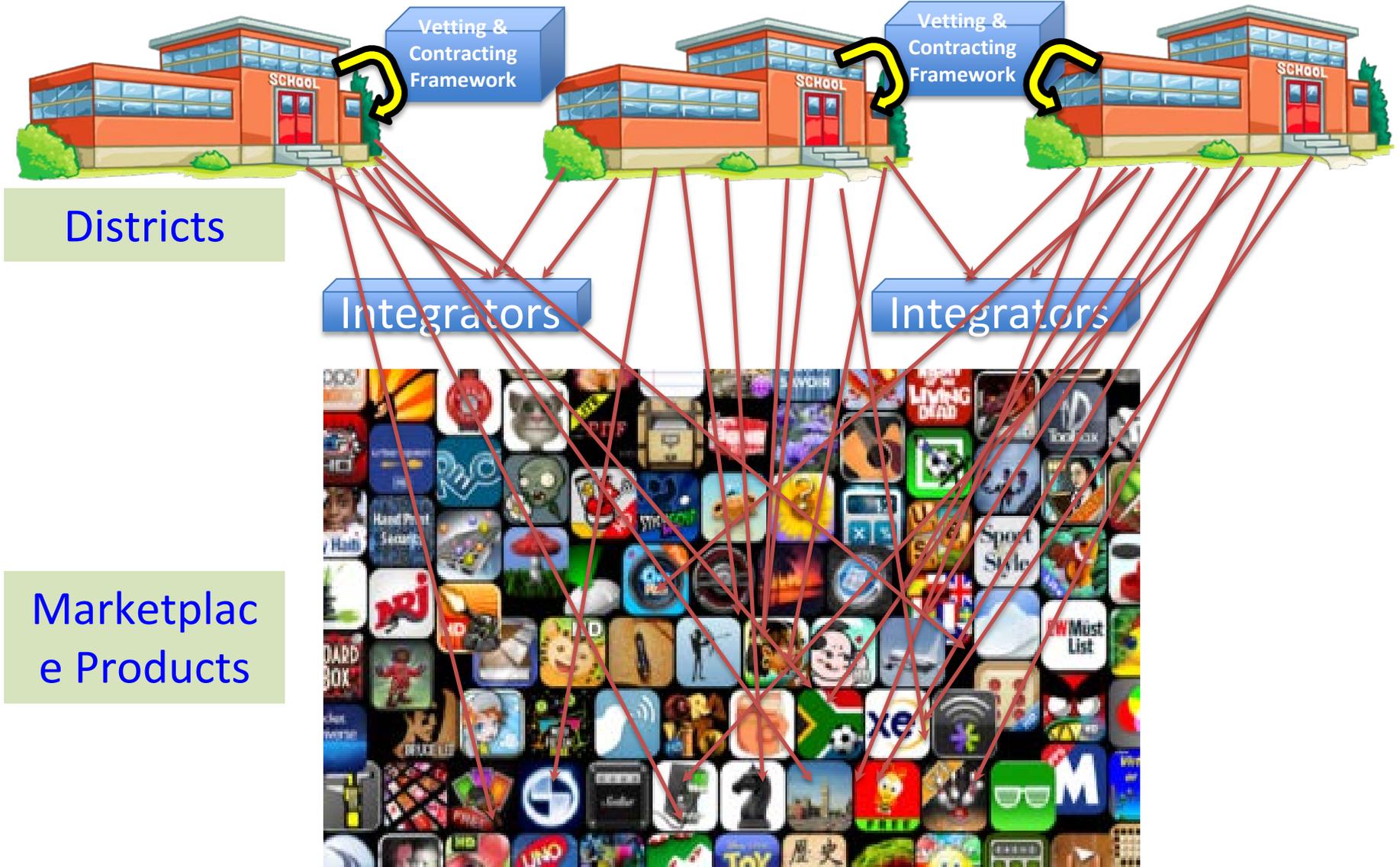
Marketplace Products





Student Data Privacy Consortium

SDPC Value Add 1



Districts

Integrators

Integrators

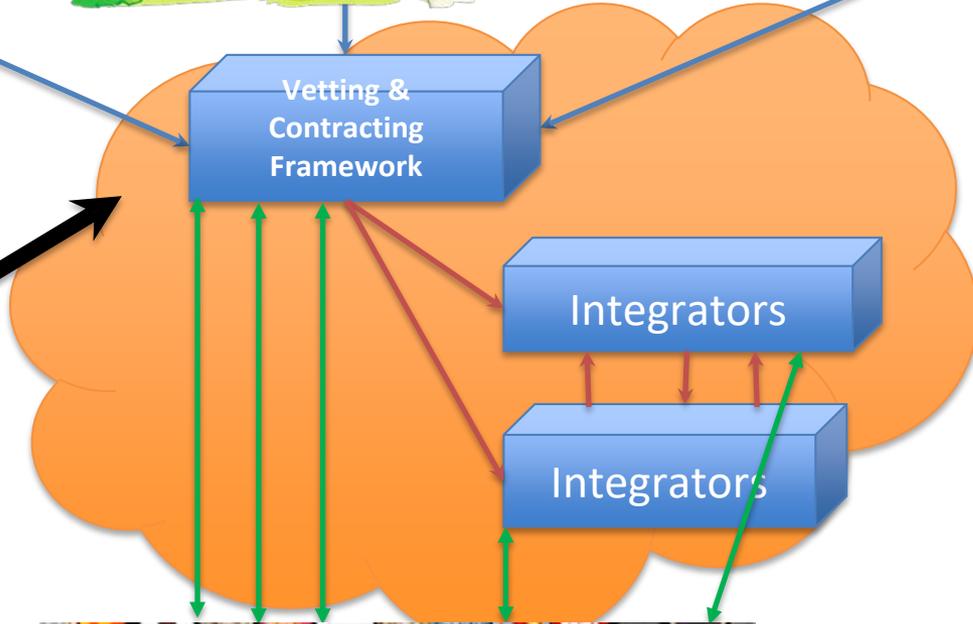
Marketplace Products

SDPC Value Add 2: Connected Privacy



Districts

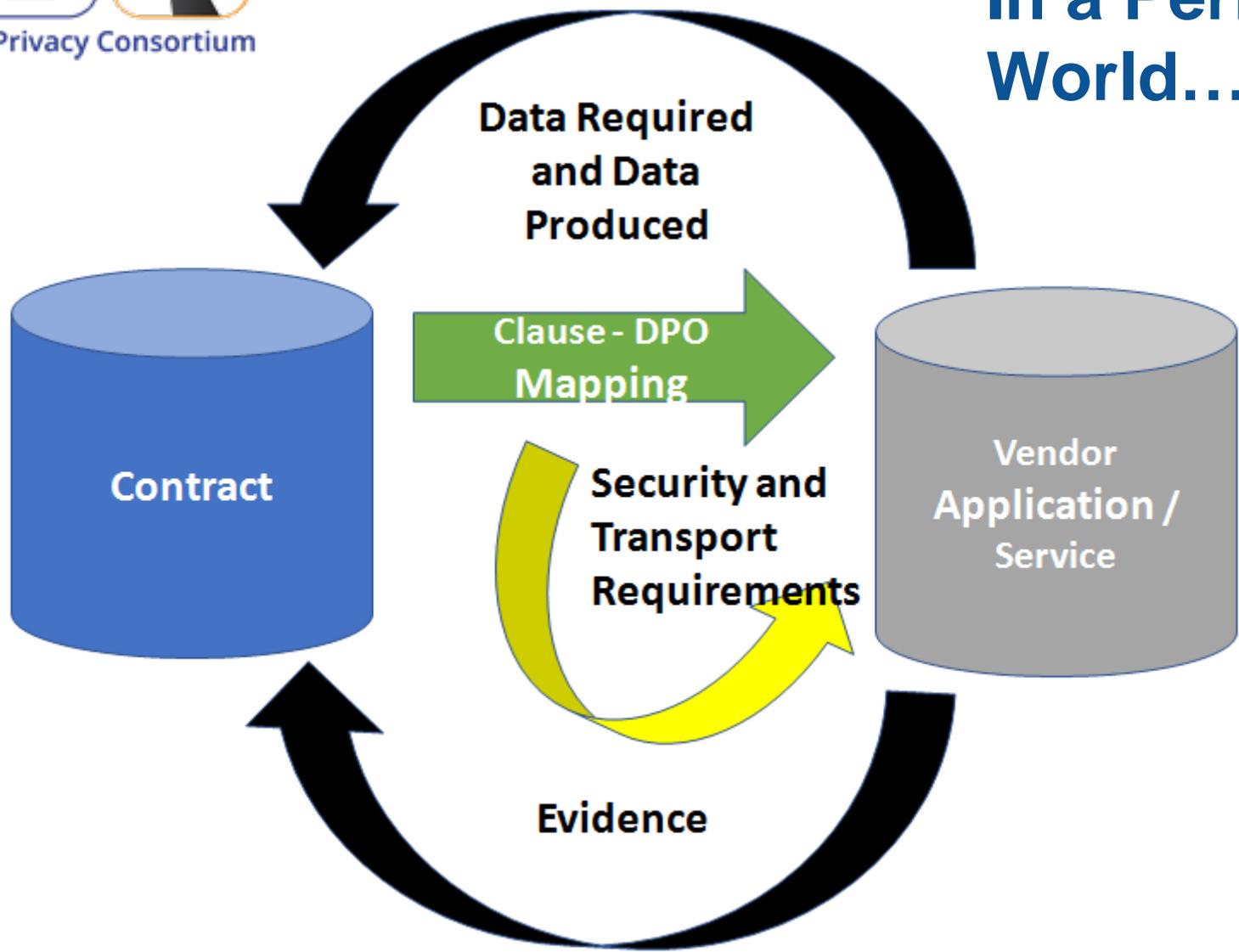
- “Secure/Quick Connections”
- Privacy Standards
- Certification



Marketplace Products



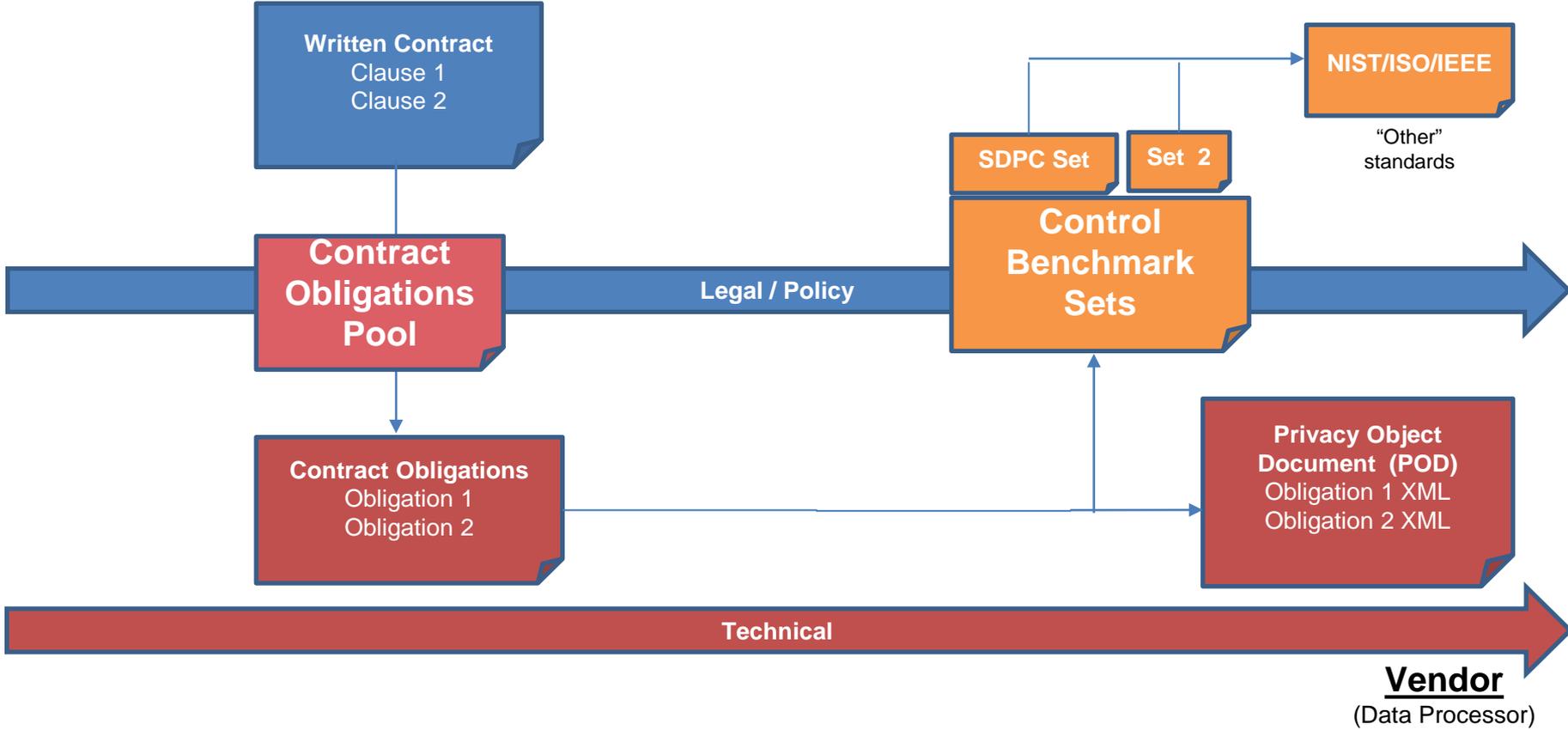
In a Perfect World.....



Global Education Privacy Standard (GEPS)



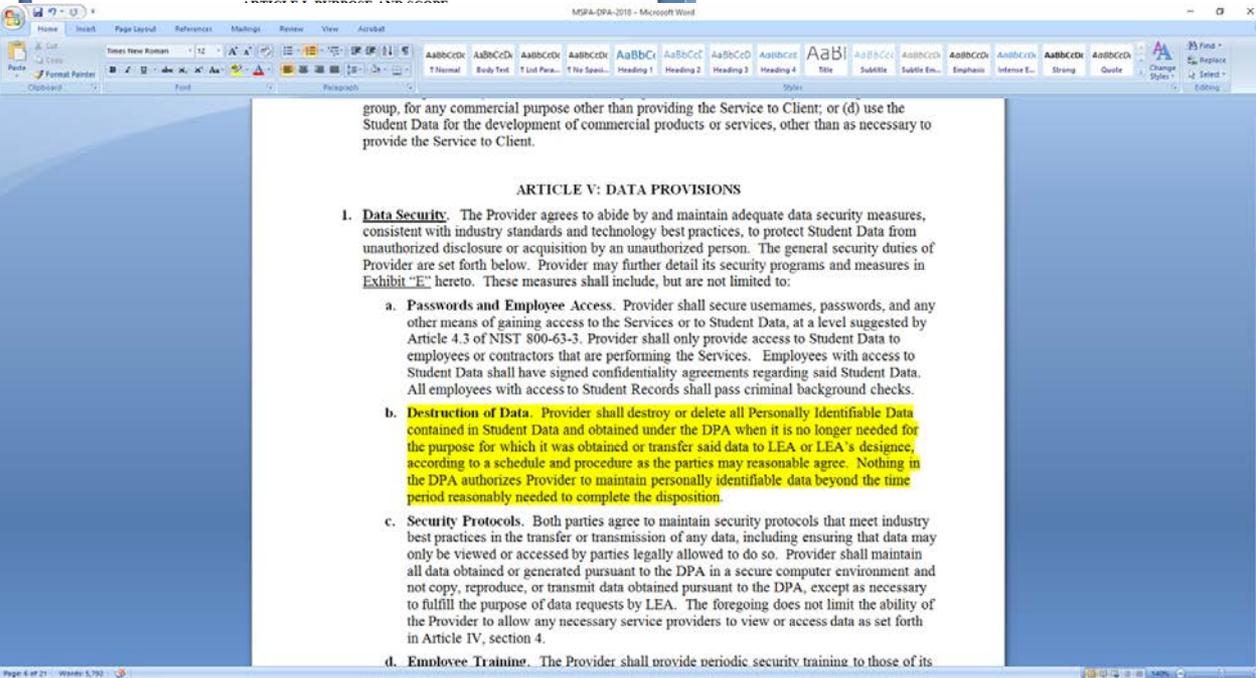
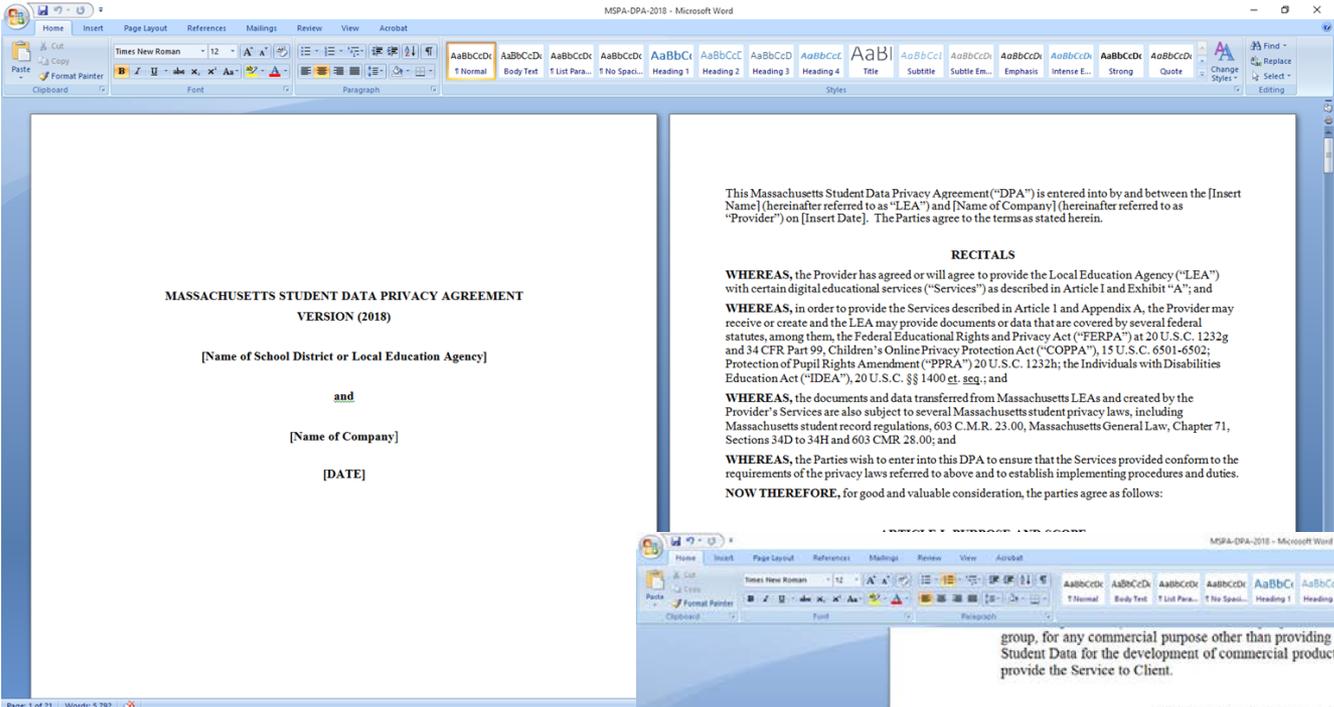
School / Department of Education
Education
(Data Controller)





GEPS Workflow

Select Clause from National Set





Example Contract Obligation Crosswalk

Obligation	US Privacy	AU Privacy	EU GDPR	Discussion	DPO Terms & Application
<p><i>Data cannot be used for advertising or marketing purposes</i></p>	<p>Article IV, Section 6. Advertising Prohibition. Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose</p>	<p>APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing.</p>	<p>Rec.70; Art.21(2)-(3) Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling</p>	<p>The limitation on the use of data by Data Processors for marketing or advertising purposes in consistent in all locales.</p> <p>In the U.S. agreement it is prevented outright, in the AU whilst limited, exceptions do apply. The GDPR provides individuals with the right to opt out.</p>	<p>“Data able to be used for marketing purposes: “Yes/No”, Data Processor Marketing contact name, Marketing contact email, Marketing contact phone number”</p> <p>The “Data able to be used for marketing purposes: Yes/No” and Data Processor marketing contact details would be a series of elements in the DPO object.</p> <p>Technically Data Processors would do nothing however the contents of this entry (as part of the DPO) could be made available to the Data Subjects (eg via the SDPC website) and allow them to contact the Data Processor and opt out from marketing/advertising processes.</p>



Student Data Privacy Consortium

GEPS Workflow

Align Privacy Clause to Obligations

SDPC: Privacy Tools x

Not secure | www.keyedsystems.com/GRC/login/

SDPC TOOLS: CAMBRIDGE PUBLIC SCHOOLS

Scott Gallant Log Out

DISCOVER **GAUGE** **CONTROL** **EVIDENCE**

Home

Components

Catalogs

Classification Schemas

UseCase

Laws / Regulations / Policies

Controls

Contracts / Agreements

Organizations

Training / Resources

Documents

Reports

Powered by: **Keyed Systems**

Control Framework

Control Framework Data

Name* : Education Privacy Standards (GEPS SAMPLE- Destruction of Data) Version* : 0.02

Organization* : Student Data Privacy Consortia (SDPC) Description* : Consorted Obligations, Benchmarks, and References for the Education Sector aligned to cross-industry requirement pertaining to the protection of data. As managed by the Student Data Privacy Consortia.

Type* : Standard

Owner* : Scott

Long Description :
 (Sample is single Clause extraction of legalese to real-world Obligations and related Benchmarks. Each Benchmark is aligned to one or more internal/external references, such as NIST)

Education Privacy Standards (GEPS SAMPLE- Destruction of Data)

- Education Privacy Standards (GEPS SAMPLE- Destruction of Data)
 - Maintain an accessible practice of destruction of data with adequate reference to definitions and policies in presenting general data retention guidelines
 - D01a- Present a data retention policy which identifies data classifications, retention schedule, and destruction process in line with data classification level.
 - D01b- Properly address and agree to the definition of delete [link: Talk to making unrecoverable, discuss extent such as backups/etc].
 - Acknowledge and register adequate signals for the interpretation, operational execution, and notice of deletion requests.
 - Recognize and plan for limits of data destruction
 - Identify the operational parties and processes to facilitate the destruction of data

Control Objective

Name* : Maintain an accessible practice of destruction of data with a

Description* : Maintain an accessible practice of destruction of data with adequate reference to definitions and policies in

Identifier* : D01

Domains : Deletion & Retention

Categories : None selected

Label* : Principle

Types : None selected

Priority :

Similar Objectives : Select Similar Objectives

Controls : D01a- Present a data retention policy which identifies data classifications, retention schedule, and destruction process in line with data classification level.

Control

Name* : D01a- Present a data retention policy which identifies data

Description* : Present a data retention policy which identifies data classifications, retention schedule,



Student Data Privacy Consortium

GEPS Workflow

Align Obligations to Control Benchmarks

The screenshot displays the SDPC Privacy Tools interface for Cambridge Public Schools. A modal window titled "All Control Frameworks" is open, allowing the user to select control objectives. The "Select Control Objectives" list includes:

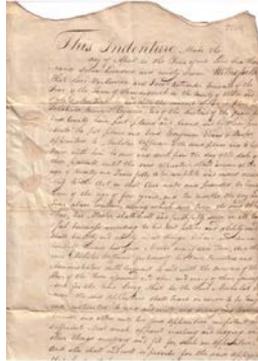
- The Student Data Principles
- ISO/IEC 27001 - Information Security Management
- NIST Special Publication 800-53
 - Access Control
 - AU - Audit and Accountability
 - AT - Awareness and Training
 - CM - Configuration Management
 - CP - Contingency Planning
 - IA - Identification and Authentication
 - IR - Incident Response
 - IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES
 - IR-2 INCIDENT RESPONSE TRAINING

The "Saved Control Objectives" list is currently empty. The background interface shows a control configuration page for "D01a" with fields for Identifier, Domains, Categories, Label, Types, Priority, Similar Objectives, and Controls. The "Control" section at the bottom shows the Name and Description for the selected control.

GEPS Workflow

Capture & Transfer Obligations & Benchmarks in XML (PODs)

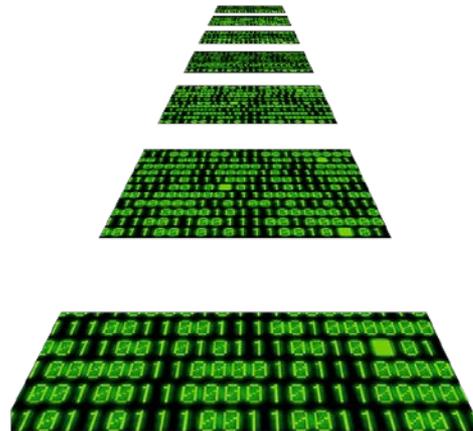
CONTRACT



IV.5 Disposition of Data. Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any Student Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means.....



PRIVACY OBLIGATION DOCUMENT POD - XML



```
<dataDeletionObligation>  
  <clauseList>  
    <clause>The vendor shall purge all data related upon request.</clause>  
  <fields>  
    <field>/StudentPersonal/LocalId</field>  
    <field>/StudentPersonal/FirstSchoolEnrol</field>  
    <deleteData>Y</deleteData>  
    <dataRetention>30</dataRetention>  
    <deleteBy>2018-07-01</deleteBy>  
  </dataDeletionObligation>
```



Student Data Privacy Consortium

Find Out More

<https://privacy.a4l.org>

Larry L Fruth II, Ph.D.

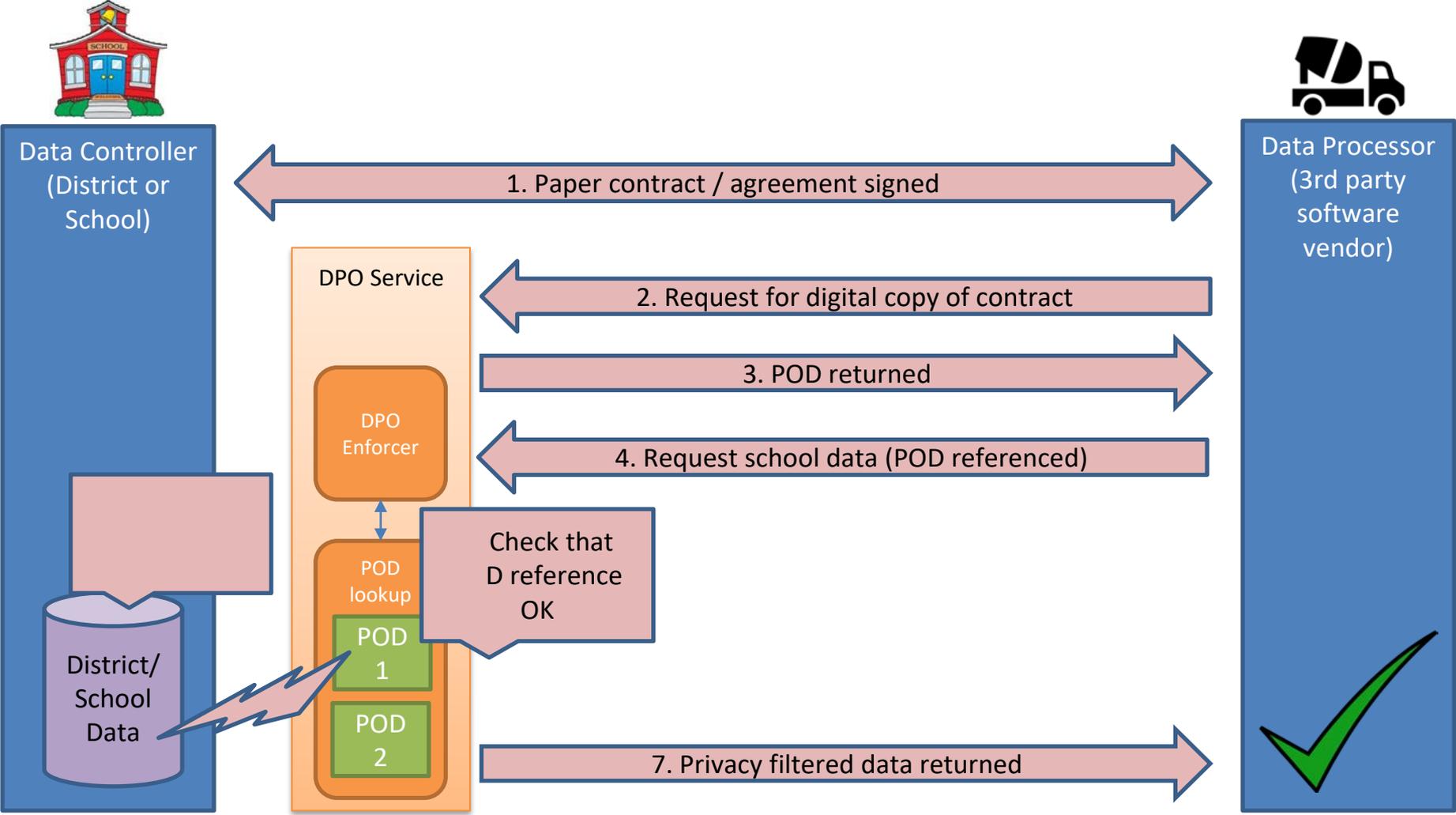
lfruth@A4L.org

Steve Smith

ssmith@cpsd.us

Membership Category	SDPC	SDPC+A4L
Schools	\$200	\$500
Districts	\$400	\$750
University	\$800	\$1,250
Alliances (Reg Agency / SEA)	\$3,000	\$5,000
Vendors: \$0-\$1 million	\$500	\$2,500
Vendors: \$2-\$3 million	\$1,000	\$5,000
Vendors: \$4-\$7 million	\$2,500	\$7,500
Vendors: \$8-\$10 million	\$5,000	\$10,000
Vendors: \$11-\$50 million	\$10,000	\$15,000
Vendors: \$51-\$250 million	\$15,000	\$22,000
Vendors: \$251-\$750 million	\$25,000	\$35,000
Vendors: Over \$750 million	\$50,000	\$60,000

How do PODs work to support private secure data transfer?





How do PODs work to prevent inappropriate data transfer?

