“Tactical” Student Data Privacy

SDPC Progression

Stats DC 2018
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
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.
• **Project 1: Privacy Contract Framework**

  *The Privacy Contract Framework project is focused on the development of 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 20 million Students Impacted by over 1250 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.*
**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 App”

Are your students safe online? Join us!
SDPC Tools for Districts

Tools for Participating Districts

- 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

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
## Contract Management

### Application Information

<table>
<thead>
<tr>
<th>Software Name</th>
<th>Agreement Status</th>
<th>Agreement Type</th>
<th>Agreement Dates</th>
<th>Export All to Excel</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Registration Service,</td>
<td>Active</td>
<td>Agreement V4</td>
<td>2017-02-10</td>
<td></td>
</tr>
<tr>
<td>Company Name: Total Registration</td>
<td></td>
<td>School Year: 2016 - 2017</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requested by: Sherry Madden</td>
<td></td>
<td>Location: CRLS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ABC Mouse,</td>
<td>New Request</td>
<td>Agreement Type</td>
<td>Approved:</td>
<td></td>
</tr>
<tr>
<td>Company Name: ABC Mouse</td>
<td>Progress Update:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requested by: Slobhan Patterson</td>
<td></td>
<td>Contract Sent</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Modified:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2017-07-31</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACE ABA Software System,</td>
<td>New Request</td>
<td>Agreement Type</td>
<td>Approved:</td>
<td></td>
</tr>
<tr>
<td>Company Name: The New England Center for Children</td>
<td>Progress Update:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requested by: Kayn Grace</td>
<td></td>
<td>Contract Sent</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Modified:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2017-08-01</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Achieve 3000,</td>
<td>Active</td>
<td>Agreement V2a</td>
<td>Approved:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Additional Details

- **Application**: Edit | Other Info | Delete
- **Data Elements**: Add | Edit
- **Upload Agreement**: Signed | Annotated | Vendor-Specific
- **Progress Log**: Add | View
- **Progress Admin**: Elizabeth Mazzacappa
- **Progress**: Contract Sent | Update
- **Progress Admin**: Steve Smith
- **Progress**: Contract Sent | Update
Vendor Tools

Tools for Participating Vendors

- Vendor Marketplace
- Breach Notification
- Project 2 Vendor Templates
- Email Districts with Signed Contracts
SDPC Tactical Privacy Projects

• **Project 1: Privacy Contract Framework**
  
  The Privacy Contract Framework project is focused on the development of 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

Assess the Terrain

Monitor and Adapt

Digital Tool Governance

Develop the Plan

Mobilize and Deploy

Know your goal before you begin...

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

Know your goal before you begin...

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

Know your goal before you begin...

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

Know your goal before you begin...

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

Know your goal before you begin...
## Example Use Case: District Data Privacy and Security Professional Learning

<table>
<thead>
<tr>
<th>Craft a Vision</th>
<th>Assess The Terrain</th>
<th>Develop The Plan</th>
<th>Mobilize and Deploy</th>
<th>Monitor and Adapt</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>Characteristics:  - 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?</td>
<td>Characteristics:  - 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</td>
<td>Characteristics:  - 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</td>
<td>Description:</td>
</tr>
</tbody>
</table>

**Terminology:**
- Privacy, mission, and vision: create awareness of the importance of data privacy and security for all staff.
- Data Privacy Program: Establishes roles, responsibilities, resources, and timelines for tasks required to establish or improve a formal data privacy and security professional learning program.
- Utilizing previously acquired information, and a documented implementation plan, launch formal awareness campaign and professional development activities.
Framework for Transformative Digital Governance

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.

Login to the DGT
Digital Governance Tool (DGT)

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

- Policies
- Resource Vetting
- Staff PD
- Data Breach Issues
- Technical Cyber Security
- Procurement

Shared Resources
My Shared Resources
Shared Digital Governance Plans
View Your District’s Digital Governance Plan
View the Project Report
• **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**

*The “Last Mile”*
The Current World

Student Data Privacy Consortium

Districts

Integrators

Marketplace Products
SDPC Value Add 2: Connected Privacy

- “Secure/Quick Connections”
- Privacy Standards
- Certification
In a Perfect World.....
Global Education Privacy Standard (GEPS)

School / Department of Education (Data Controller)

- Written Contract
  - Clause 1
  - Clause 2

Contract Obligations Pool

- Contract Obligations
  - Obligation 1
  - Obligation 2

Legal / Policy

Control Benchmark Sets

- SDPC Set
- Set 2

Technical

Privacy Object Document (POD)

- Obligation 1 XML
- Obligation 2 XML

Vendor (Data Processor)

- NIST/ISO/IEEE
  - "Other" standards

Global Education Privacy Standard (GEPS)
GEPS Workflow

Select Clause from National Set

MASSACHUSETTS STUDENT DATA PRIVACY AGREEMENT

VERSION (2018)

[Name of School District or Local Education Agency]

and

[Name of Company]

[DATE]

RECEIPTS

WHEREAS, the Provider has agreed or will agree to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") as described in Article 1 and Exhibit A; and

WHEREAS, in order to provide the Services described in Article 1 and Appendix A, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Federal Educational Rights and Privacy Act ("FERPA") at 34 C.F.R. § 99.822 and 34 C.F.R. Part 99, Children’s Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501 - 6502; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. § 1232h; the Individuals with Disability Education Act ("IDEA"), 20 U.S.C. §§ 1400 et seq.; and

WHEREAS, the documents and data transferred from Massachusetts LEA and owned by the Provider’s Services are also subject to several Massachusetts student privacy laws, including Massachusetts student record regulations, 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 35D to 4-H and 603 CMR 25.00; and

WHEREAS, the Parties wish to enter into the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties.

NOW THEREFORE, for good and valuable consideration, the Parties agree as follows:

ARTICLE V: DATA PROVISIONS

1. Data Security. The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit B, if any. These measures shall include, but are not limited to:

a. Passwords and Employee Access. Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, as at a level specified by Article 1.4 of NIST 800-63. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall pass criminal background checks.

b. Destruction of Data. Provider shall destroy or delete all Personally Identifiable Data contained in Student Data and obtained under the DPA when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA’s designated according to a schedule and procedure as the parties may reasonably agree. Nothing in the DPA authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

c. Security Protocols. Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all obtained and generated pursuant to the DPA in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the DPA, except as necessary to fulfill the purpose of data requests by LEA. The foresees does not limit the ability of the Provider to allow any necessary service providers to view or access data as set forth in Article IV, section 4.

d. Employee Training. The Provider shall provide periodic security training to those of its
<table>
<thead>
<tr>
<th>Obligation</th>
<th>US Privacy</th>
<th>AU Privacy</th>
<th>EU GDPR</th>
<th>Discussion</th>
<th>DPO Terms &amp; Application</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data cannot be used for advertising or marketing purposes</strong></td>
<td>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</td>
<td>APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing.</td>
<td>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</td>
<td>The limitation on the use of data by Data Processors for marketing or advertising purposes in consistent in all locales. 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.</td>
<td>“Data able to be used for marketing purposes: “Yes/No”, Data Processor Marketing contact name, Marketing contact email, Marketing contact phone number” 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. 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.</td>
</tr>
</tbody>
</table>
GEPS Workflow

Align Privacy Clause to Obligations
GEPS Workflow
Align Obligations to Control Benchmarks
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.....
Find Out More

https://privacy.a4l.org

Larry L Fruth II, Ph.D.
lfruth@A4L.org

Steve Smith
ssmith@cpsd.us

<table>
<thead>
<tr>
<th>Membership Category</th>
<th>SDPC</th>
<th>SDPC+A4L</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schools</td>
<td>$200</td>
<td>$500</td>
</tr>
<tr>
<td>Districts</td>
<td>$400</td>
<td>$750</td>
</tr>
<tr>
<td>University</td>
<td>$800</td>
<td>$1,250</td>
</tr>
<tr>
<td>Alliances (Reg Agency / SEA)</td>
<td>$3,000</td>
<td>$5,000</td>
</tr>
<tr>
<td>Vendors: $0-$1 million</td>
<td>$500</td>
<td>$2,500</td>
</tr>
<tr>
<td>Vendors: $2-$3 million</td>
<td>$1,000</td>
<td>$5,000</td>
</tr>
<tr>
<td>Vendors: $4-$7 million</td>
<td>$2,500</td>
<td>$7,500</td>
</tr>
<tr>
<td>Vendors: $8-$10 million</td>
<td>$5,000</td>
<td>$10,000</td>
</tr>
<tr>
<td>Vendors: $11-$50 million</td>
<td>$10,000</td>
<td>$15,000</td>
</tr>
<tr>
<td>Vendors: $51-$250 million</td>
<td>$15,000</td>
<td>$22,000</td>
</tr>
<tr>
<td>Vendors: $251-$750 million</td>
<td>$25,000</td>
<td>$35,000</td>
</tr>
<tr>
<td>Vendors: Over $750 million</td>
<td>$50,000</td>
<td>$60,000</td>
</tr>
</tbody>
</table>
How do PODs work to support private secure data transfer?

1. Paper contract / agreement signed
2. Request for digital copy of contract
3. POD returned
4. Request school data (POD referenced)

Check that D reference OK

5. POD lookup
6. Raw data filtered as per POD rules
7. Privacy filtered data returned
How do PODs work to prevent inappropriate data transfer?

1. Paper contract / agreement signed

2. Request for digital copy of contract

3. POD returned

4. Request school data (POD not referenced or incorrect)

Check that POD OK

5. Error returned – POD not valid. No data provided.