A Model Now Proven

The Free/Open Privacy Standard Driving Relationships to Compliance

Scott Gallant, Keyed Systems/Webshiled
Steve Smith, Cambridge Public Schools
Aish Agrawal, HMH CO
Mike Reynolds, Cedar Labs
AGENDA

- Student Data Privacy Consortium Background
- Global Education Privacy Standard
- MA Data Hub Services
- Edtech Provider Challenges
- Common Requirements, Streamlined Solutions
- Q & A
The SDPC:
• Started in 2015 to address stakeholders data privacy “Pain Points”
• Organized as a Special Interest Group (SIG) of 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
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 Background

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

The Student Data Privacy Consortium
12/18
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.
Global Education Privacy Standard

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
- Subject specific obligations
- Condition list
- Data deletion obligations

Data controller obligations

Data processor obligations

Data processor details

Default can be set
Can repeat if fine grained controls required
Global Education Privacy Standard

DEMO
MA Data Hub Services

MA Data Hub
Market Provider Challenges

- Many to Many contractual relationships
- Use of data is growing across programs and platforms
- Lack of standardization across contracts when it comes to privacy
- Different privacy requirements at State, Regional, District level
- Time and resource intensive to fulfil all these obligations individually
- Prevents a quick and effective turnaround and implementation
- Significant advantage to receiving technical benchmarks over the wire
Common Requirements, Streamlined Solutions

BACKGROUND:

• Orgs lack $$ to understand and interpret requirements. There is knowledge and response gap.
• Innovation is driving more and more data uses. The gap is growing faster than we can plug it.
• Sectoral involvement drives state privacy regulation. We are not adequately filling this role.
• Provider tools and services do not scale to all K12. The cost of compliance is high.
• People consider data risk in their digital experiences. Public expectation of trust has changed.

PROBLEM:

The advent of multiple security/privacy one-pagers, guidelines, laws, and industry solutions led us from barren landscape to the wild west in 6 years. The cost falls to the people, student safety is at risk, and accountable entities need support.
Common Requirements, Streamlined Solutions

A RECENT KEYED SYSTEMS STUDY

- NH RSA 189:66 (32 clauses)
  - #24: ‘department shall establish minimum standards’

- NH DOE Minimum Standards (44 items)
  - … with references to NIST 800-171
  - … a derivation of NIST 800-53

- Done? NOPE! At least 9 more state laws.
- And of course federal COPPA/FERPA/PPRA/etc
- Then any obligations to Privacy Pledge, TLE, or industry initiatives
- And don’t forget parsing through your contracts...

- SDPC Contract DPA Draft (47 Provisions)
### A RECENT KEYED SYSTEMS STUDY

<table>
<thead>
<tr>
<th>SDPC Common Contract DPA [draft]</th>
<th>Minimum Standards for Privacy and Security of Student and Employee Data (NH DOE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>● 47 DPA provisions</td>
<td>● 44 LEA standard requirements to be implemented by LEAs and Service Providers</td>
</tr>
<tr>
<td>● 33 Not covered by NH Minimum</td>
<td>○ Due to NIST security origin lacks specific privacy direction for notices, limited use, subject rights, 3rd party usage and assessments, marketing, research, etc</td>
</tr>
<tr>
<td>○ 7-8 n/a</td>
<td>○ Some are direct legalease required not relevant to controls</td>
</tr>
<tr>
<td>○ 2-3 somewhat ‘catch all’ for the ‘standards’</td>
<td></td>
</tr>
<tr>
<td>○ Some</td>
<td></td>
</tr>
</tbody>
</table>

- NH RSA 189:66 (32 clauses)
  - #24: ‘department shall establish minimum standards
- NH DOE Minimum Standards (44 items)
  - … with references to NIST 800-171
  - … a derivation of NIST 800-53

125 pages
9 pages

Done? NOPE! At least 9 more state laws.
And of course federal COPPA/FERPA/PPRA/etc
Then any obligations to Privacy Pledge, TLE, or industry initiatives
And don’t forget parsing through your contracts...

SDPC Contract DPA Draft (47 Provisions)
SDPC Common Contract DPA [draft]
Minimum Standards for Privacy and Security of Student and Employee Data (NH DOE)

- 47 DPA provisions
- 33 Not covered by NH Minimum
  - 7-8 n/a
  - 2-3 somewhat ‘catch all’ for the ‘standards’
  - Some are direct legalease required not relevant to controls
- 44 LEA standard requirements to be implemented by LEAs and Service Providers
  - Due to NIST security origin lacks specific privacy direction for notices, limited use, subject rights, 3rd party usage and assessments, marketing, research, etc
It's been an opportunistic time for many organizations! There are tools and services to make your life easier.
It's been an opportunistic time for many organizations! There are tools and services to make your life easier.
OPPORTUNITY
Support districts/vendors protect people by maintaining a proprietary framework of security/privacy expectations leading to our best-practice and marketplace solution.
Edspex Introduction

OPPORTUNITY
Support districts/vendors protect people by maintaining an open framework of security/privacy expectations leading to best-practice and marketplace solutions.

- Affirm our responsibility: Safety/Protection of Students
- Build knowledge and response: Privacy & Security Content
- Use our best capability: Community
Edspex Introduction

Get Engaged...
www.edspex.com

(Workgroup calls every other week)
(Webinar training event early Sept)
Edspex Introduction

- An attainable set of control guidelines
- Alignment to industry & external models
- Addressing requirements for all states
- Room for local loosening or tightening
- Supportive of a maturity model over time
- Security and Privacy
- Agency and Provider
- Support of a Community.
Questions