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
“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
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.......
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.)
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.
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.

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

1. Other schools to which a student is transferring;
2. Specified officials for audit or evaluation purposes;
3. Appropriate parties in connection with financial aid to a student;
4. Organizations conducting certain studies for or on behalf of the school;
5. Accrediting organizations;
6. To comply with a judicial order or lawfully issued subpoena;
7. State and local authorities, within a juvenile justice system, pursuant to specific State law.
8. Appropriate officials in cases of health and safety emergencies;
9. School officials with legitimate educational interest;
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 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?
Privacy Explosion in USA
The BIG Question: FREE
Student Privacy Laws

STATE LAW

40

States Have Passed 125 Laws Since 2013
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
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”!

No One Gets It!

Everyone Gets It!
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.

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

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.

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.

5. Leverage partnership organizations working in the privacy space to have their good work utilized and no reinvention of existing work.
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
Privacy – By The Numbers...
the Student Data Privacy Consortium (SDPC)

Tools for:
Privacy Contract Building
Application Inventory & Searchable Database
Application Contract Management
Global Education Privacy Standard (GEPS)

'Tactical' Privacy Information
– contract to implementation

28 State-wide Alliances

32 million
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

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
Alliances, Alliances, .....  
**Alliance Formation Models**

<table>
<thead>
<tr>
<th><strong>Top Down</strong></th>
<th><strong>Bottom Up</strong></th>
<th><strong>Middle Driven</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The State agency leading the charge to develop and grow the Alliance</td>
<td>A LEA takes the lead to develop and grow the Alliance</td>
<td>A regional service agency, professional association, or user group takes the lead to develop and grow the Alliance</td>
</tr>
</tbody>
</table>

- 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 used 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.
The Ohio Alliance

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

Are your students safe online? Join us!
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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Craft a Vision</th>
<th>Assess The Terrain</th>
<th>Develop The Plan</th>
<th>Mobilize and Deploy</th>
<th>Monitor/Adapt</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Vetting</td>
<td>Norming session with identified stakeholders to establish a goal for the identified activity with measurable deliverables, scope and progress data checks</td>
<td>Establish a comprehensive (curriculum, admin, finance, purchasing, etc.) inventory of applications in use including grade level, content area and functional area</td>
<td>Process Steps Established: • Approved list check • Assessment Tool • Request Form • Reviewer Descriptions, Process Steps and Timelines</td>
<td>Communicate and provide training and resources for plan implementation</td>
<td>At contract/agreement end teacher and IT staff review apps/site for continued usage</td>
</tr>
<tr>
<td></td>
<td>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</td>
<td>What are other entities doing regarding this task Determine what needs to be vetted; Privacy / alignment accessibility/proper use etc…</td>
<td>Budget implications of the plan - Required resources - Consider other vetting resources - e.g.</td>
<td>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</td>
<td>Direct practitioners to any “approved application” list in use</td>
</tr>
<tr>
<td></td>
<td>Identify the accountability measures and owners and incorporate their ideas, thoughts and brainstorming results</td>
<td>What considerations may impact the developing plans (industry guidance, laws, effective practices, etc.)</td>
<td>What strategies work in the setting you have regarding resources, expertise, time, etc. - Include procurement/purchasing office - What to ask – districts need directions</td>
<td>Generate a simple to simple graphics, modules, etc. used for transparency with admin and public</td>
<td>Application usage information gathered</td>
</tr>
</tbody>
</table>
Framework for Transformative Digital Governance

Craft a Vision
Know your goal before you begin...

Monitor and Adapt
• 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?

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

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

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

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

NIST/ISO/IEEE “Other” standards

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

Technical

Vendor (Data Processor)
Unity Enabling Privacy Expectations

<table>
<thead>
<tr>
<th>Header</th>
</tr>
</thead>
<tbody>
<tr>
<td>POD – Technical applicability</td>
</tr>
<tr>
<td>Contract</td>
</tr>
<tr>
<td>Legal obligations</td>
</tr>
<tr>
<td>Technical obligations</td>
</tr>
<tr>
<td>Data access</td>
</tr>
<tr>
<td>Condition list</td>
</tr>
<tr>
<td>Data controller obligations</td>
</tr>
<tr>
<td>Data processor obligations</td>
</tr>
<tr>
<td>Subject specific obligations</td>
</tr>
<tr>
<td>Data deletion obligations</td>
</tr>
<tr>
<td>Data sub-processor details</td>
</tr>
</tbody>
</table>

Automate Contract Clause Expectations Exchange and Vendor Verification

*The “POD”*  
(Privacy Obligation Document)
Global Education Privacy Standard

POD Creation from Resource Registry

Are your students safe online? Join us!
Automation & Enforcement

Leverage SDPC

GEPS
PODS
Integration

Security Requirements

Enforcement & Automation
MA Data Hub Services

MA Data Hub

District Hub
- IAM - SSO
- GEPS - Enforce & PODS
- Mash-ups
- Validations
- Transformations
- ODS

State Hub
- State Identify Portal
- State Reporting
  - Reports
  - Dashboards
- Generate
  - EDFacts
  - Dashboards
  - CEDS

Services:
- SIF2/3/Unity App (SIS?)
- OneRoster App (LMS?)
- Proprietary API App (Clever?)
- Legacy CSV App
- Delegated Administration
- GEPS Contract & POD Management
- Operational Dashboard

Copyright © Cedarlabs, LLC 2019 — All Rights Reserved
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

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!

Here is the data we will give you and details on how we want it treated

Here is how we have treated the data and details on how we can prove it to you

Increased interoperability without the inclusion of privacy requirements = increased RISK. Both data sharing and privacy parameters must be identified and communicated.
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 schools' 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 (yellow) groups.