Help Me Get Apps Safely in My Digital Ecosystem? A4L/SDPC Simplifies for You!

Supporting Setting Common Privacy Expectations Between Marketplace Providers and End Users
Agenda

- Introductions
- Brief Privacy 101
- Introduction to SDPC & The IL Alliance
- What’s Next for SDPC?

Supporting Setting Common Privacy Expectations Between Marketplace Provides and End Users
“Before I write my name on the board, I’ll need to know how you’re planning to use that data.”
### Privacy 101: Student Privacy Laws

<table>
<thead>
<tr>
<th>Legislation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIPA</td>
<td>Children’s Internet Privacy Act</td>
</tr>
<tr>
<td>PPRA</td>
<td>Protection of Pupils Rights Amendment</td>
</tr>
<tr>
<td>COPPA</td>
<td>Children’s Online Privacy &amp; Protection Act</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability &amp; Accountability Act</td>
</tr>
<tr>
<td>FERPA</td>
<td>Family Educational Rights &amp; Privacy Act (1974)</td>
</tr>
<tr>
<td>STATE</td>
<td>Legislation as well as Local Statutes and Regulations</td>
</tr>
</tbody>
</table>
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.)
Student Privacy Laws

HIPAA

Health Insurance Portability & Accountability Act

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.
COPPA

Children's’ Online Privacy & Protection Act

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.

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

<table>
<thead>
<tr>
<th>Exception</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other schools to which a student is transferring;</td>
<td>1</td>
</tr>
<tr>
<td>Specified officials for audit or evaluation purposes;</td>
<td>2</td>
</tr>
<tr>
<td>Appropriate parties in connection with financial aid to a student;</td>
<td>3</td>
</tr>
<tr>
<td>Organizations conducting certain studies for or on behalf of the school;</td>
<td>4</td>
</tr>
<tr>
<td>Accrediting organizations;</td>
<td>5</td>
</tr>
<tr>
<td>To comply with a judicial order or lawfully issued subpoena;</td>
<td>6</td>
</tr>
<tr>
<td>State and local authorities, within a juvenile justice system, pursuant to</td>
<td>7</td>
</tr>
<tr>
<td>specific State law.</td>
<td></td>
</tr>
<tr>
<td>Appropriate officials in cases of health and safety emergencies;</td>
<td>8</td>
</tr>
<tr>
<td>School officials with legitimate educational interest;</td>
<td>9</td>
</tr>
</tbody>
</table>
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
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.
Student Privacy Laws

- Annually post a list of all operators of online services or applications utilized by the district.
- Annually post all data elements that the school collects, maintains, or discloses to any entity. This information must also explain how the school uses the data, and to whom and why it discloses the data.
- Post contracts for each operator within 10 days of signing.
- Annually post subcontractors for each operator.
- Post the process for how parents can exercise their rights to inspect, review and correct information maintained by the school, operator, or ISBE.
- Post data breaches within 10 days and notify parents within 30 days.
- Create a policy for who can sign contracts with operators.
- Designate a privacy officer to ensure compliance.
- Maintain reasonable security procedures and practices. Agreements with vendors in which information is shared must include a provision that the vendor maintains reasonable security procedures and practices.
- Although not required by law, school districts will also need to undertake the following to meet the above requirements:
  - Provide teachers with the list of online operators that are safe and approved for use.
  - Develop a process for keeping data inventory up-to-date.
Increased interoperability without the inclusion of privacy requirements = increased RISK
**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
What’s needed is a connected, secure, and effective learning ecosystem.
A4L and SDPC’s “New School” Role

- Increased interoperability without the inclusion of privacy requirements equals increased **RISK**.
- **BOTH** data sharing and privacy parameters must be identified and communicated.
- Learning institutions often do not have the human and/or fiscal resources to successfully address both parameters.
- A4L and SDPC is the **ONLY** community collaboration that is addressing **BOTH** interoperability and privacy.

"Leadership and learning are indispensable to each other."

- John F. Kennedy

The A4L and SDPC Communities will help schools and providers establish “connected and secure effective learning ecosystems”
SDPC Goals

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

2. 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.

3. Leverage partnership organizations working in the privacy space to have their good work utilized and no reinvention of existing work.

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. Establish a community of stakeholders who have various needs addressed through policy, technology and/or effective practice sharing around effective privacy management.
Alliances, Alliances...

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 agreement 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.
**Consortium Projects**

- 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

**Privacy By The Numbers**

- **26 State-wide Alliances**
- **34 million** Students supported by SDPC Tools
- **11350** School Districts represented
- **4** Countries Collaborating on Privacy Issues
- **76088** Signed Data Privacy Agreements
- **8533** Resources in the Database
- **59696** Signed “Piggyback” Exhibit E
Registry Workflow Support – The How!

Request

Approval

Agreement
Manage Apps

Transparency

Digital Resource Request Form | Step 1

<table>
<thead>
<tr>
<th>Workflow Step</th>
<th>Order</th>
<th>Workflow Step</th>
<th>Order</th>
<th>Make Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Pursue</td>
<td>1</td>
<td>Did Not Pursue</td>
<td>1</td>
<td>Order: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Progress Email:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This email is to let you know that your Online Resource Request has not be</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ened reviewed.</td>
</tr>
<tr>
<td>Educationally Aligned</td>
<td>2</td>
<td>Educationally Aligned</td>
<td>2</td>
<td>Order: 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Progress Email:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This email is to let you know that your Online Resource Request has been</td>
</tr>
<tr>
<td>With Legal Dept</td>
<td>3</td>
<td>With Legal Dept</td>
<td>3</td>
<td>Order: 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Progress Email:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This email is to let you know that your Online Resource Request has no be</td>
</tr>
</tbody>
</table>

Agreement

<table>
<thead>
<tr>
<th>ABC-User</th>
<th>Agree</th>
<th>Approved</th>
<th>Agreement Date</th>
<th>Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>08/02/2019</td>
<td>08/03/2021</td>
<td></td>
</tr>
</tbody>
</table>

Agreement

<table>
<thead>
<tr>
<th>ABC-Go</th>
<th>Agree</th>
<th>Approved</th>
<th>Agreement Date</th>
<th>Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>08/03/2019</td>
<td>08/04/2021</td>
<td></td>
</tr>
</tbody>
</table>
Further increase consistency across Alliance DPAs
Standardize the DPA Format so it looks the same across Alliances
Ease logistics of implementing
Identify common legal requirements across jurisdictions
Provide mechanism to add other jurisdiction specific requirements
Standardize terminology & definitions across jurisdictions
Greater impact on, and buy in, from the vendors = Adoption
# Making Agreements “Simple”

<table>
<thead>
<tr>
<th>NDPA Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section</td>
<td>Cover Page</td>
</tr>
<tr>
<td>Section</td>
<td>Page 2 - Options</td>
</tr>
<tr>
<td>Section</td>
<td>Page 3 - Signatories</td>
</tr>
<tr>
<td>Section</td>
<td>Standard Clauses</td>
</tr>
<tr>
<td>Section</td>
<td>- Exhibits</td>
</tr>
<tr>
<td></td>
<td>- A = Descriptions of Services</td>
</tr>
<tr>
<td></td>
<td>- B = Schedule of Data</td>
</tr>
<tr>
<td></td>
<td>- C = Definitions</td>
</tr>
<tr>
<td></td>
<td>- D = Directive for Disposition of Data</td>
</tr>
<tr>
<td></td>
<td>- E = General Offer of Terms</td>
</tr>
<tr>
<td></td>
<td>- F = Data Security Requirements</td>
</tr>
<tr>
<td></td>
<td>- G = Supplemental State Terms</td>
</tr>
<tr>
<td></td>
<td>- H = Additional Terms or Modifications</td>
</tr>
</tbody>
</table>

The Provider and LEA hereby agree to enter into the following Data Processing Agreement (the “Agreement”) and is entered into by and between:

[School District Name], located at [Street, City, State] (the “Local Education Agency” or “LEA”) and [Provider Name], located at [Street, City, State] (the “Provider”).

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“COPPA”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. Special Provisions. Check if Required

   - If checked, the Supplemental State Terms and attached hereto as Exhibit “G” are hereby incorporated by reference into this DPA in their entirety.
   - If checked, LEA and Provider agree to the additional terms or modifications set forth in Exhibit “H” (Optional).
   - If checked, the Provider has signed Exhibit “E” to the Standard Clauses, otherwise known as General Offer of Privacy Terms.
National Research Data Privacy Agreement

- Leverages National Data Privacy Agreement (NDPA) template but for Researchers
- Developed with Foundations, Universities, Researchers, State and Local Ed Agencies
Resources!

February 12-13, 2020
OETC Conference

Teachers - A Student Privacy 'Cheat Sheet' Session
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; and The Where: Resources

Student Data Privacy: What are YOUR obligations?
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; and The Where: Resources

Student Data Privacy Consortium
'Tactical' Privacy for the Front Lines
https://privacy44k.org

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 school's 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" or "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 "small" or "forming"
The "POD" (Privacy Obligation Document)

- Header
- POD - Technical applicability
- Contract
- Legal obligations
- Technical obligations
- Data access
- Subject specific obligations
- Condition list
- Data deletion obligations
- Data controller obligations
- Data processor obligations
- Data sub-processor details

School / Department of Education
(Data Controller)

Written Contract
Clause 1
Clause 2

Contract Obligations Pool

Contract Obligations
Obligation 1
Obligation 2

Legal / Policy

NIST/ISO/IEEE
"Other" standards

You pick the technical security standard

SDPC Set
Set 2

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

A machine-readable document for detailed obligations

Technical

Vendor (Data Processor)

Automate Contract Clause Expectations Exchange and Vendor Verification

The legalese from the DPA

The technical obligation from the legalese
What’s Coming From the SDPC?

- SDPC successes has detoured legislative activity on privacy requirements
- The NDPA left security choice up to providers - “pick the one you used……”
- Choices out there are “round peg in square hole” for K12 technologies
- Also the AU SDPC Community has a national project coming to the states - Safer Technology 4 Schools (ST4S) - vetting applications for privacy and security
- The SDPC Management Board just approved a new Project Team - Global Education Security Standard - tapping into existing Standards Orgs
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.
It’s Not “One or the Other”!

“Connecting and Securing Effective Learning Ecosystems”®

No One Gets It!

Everyone Gets It!
Find Out More

- Steve Smith
  ssmith@cpsd.us
- Chris Wherley
  cwherley@ltcillinois.org

https://www.A4L.org
https://privacy.A4L.org