Student Data Privacy: What Are YOUR Obligations TN?

Steve Smith, CIO Cambridge Public Schools Cambridge MA
Larry Fruth II PhD, Executive Director and 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.”
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.......
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
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.

- 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 that is collected, stored, and communicated by schools or technology vendors.

- It also includes the data created or generated by the student or teacher in the use of technology (e.g. email accounts, online bulletin boards, work performed etc.).

- 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

- Children’s Internet Privacy Act
- Protection of Pupils Rights Amendment
- Children’s Online Privacy & Protection Act
- Health Insurance Portability & Accountability Act
- State Legislation
  - State Legislation
  - Local Statutes and Regulations

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.
What Are The Critical Components to Put **ME** in Charge?

➢ **Application Data Management**
  • What are some effective and proven ways to perform my data manager role?
  • What are some effective and proven ways to save us time and critical resources?

➢ **Student Data Privacy**
  • What are some effective and proven ways to perform my data stewardship privacy role?
  • What are some effective and proven ways to save us time and critical resources?
**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

**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
Its Not “One or the Other”!

No One Gets It!

Everyone Gets It!
SDPC Scope – THE HOW

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

The SDPC:

- Built upon work done in CPS
- 12+ years working with vendors
- Developed in house tools
- Awareness building
- Standardized DPAs
- Expanded across MA
Privacy – By The Numbers...
the Student Data Privacy Consortium (SDPC)

- 28 State-wide Alliances
- 32 million Students supported by Tools
- 8700+ School Districts represented
- 4 Countries Collaborating on Privacy Issues
- 11955 Signed Vendor Agreements
- 4252 Applications in Database
- 10076 Signed “Piggyback” Exhibit E

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

‘Tactical’ Privacy Information – contract to implementation

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 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 TETA was formed in 1993 by educators who saw a need for a focus on educational technology. Our purposes include: to share and exchange ideas, materials, and procedures; to promote the effective use of information, communication, and technology; to encourage the appropriate use of technology for the improvement of educational management; to promote professional standards in the field of educational technology; and to communicate current research relating to educational technology.
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.
1. Check the Resource Registry – No Password Needed!

2. Check the TN Alliance Site

3. Request – Or Push Your Tech Support – To Get an Account and Join Free!

4. Explore the Resource Registry Tools and Import Your List of Apps (PDF)

5. The Alliance will begin convening to discuss a statewide agreement or working to adopt the *National Data Privacy Clause Set* under development.
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)
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
Resources

Student Data Privacy Consortium (SDPC) Application / Resource Registry

TRAINING: District Admins
February 25, 2019

Student Data Privacy Consortium

Student Data Privacy Consortium

Tactical Privacy for the Front Lines

https://privacy.A4L.org

Over the past 2 years there have been more than 100 student data privacy legislative efforts crafted in more than 95 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 those “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 forums (green or forming...
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.
Find Out More

- Steve Smith
  ssmith@cpsd.us
- Larry Fruth II, PhD
  lfruth@a4l.org

https://privacy.a4l.org