Student Privacy: National Trends and Best Practices

9/8/2016

NASBE
National Association of State Boards of Education
State Boards of Education Have At Least Some Authority Over Education Data Privacy
Take a minute to discuss with your neighbor...

• What are you worried about regarding data privacy in Connecticut?
• What might data do for Connecticut that you are excited about?
Why is Data Important?
How Data Is Being Used To Help Kids Succeed

➢ Provides additional support for children, teachers, and administrators
➢ The only way to personalize education
➢ Gives parents (and students) a window on how their child is doing in school
➢ The engine behind every successful school

Credit: The Data Quality Campaign
Landscape of Privacy Concerns

- The scope and type of student data schools collect
- Who is collecting and accessing student data/education records
- Common Core and Assessment Consortia
- Use of data collected by third parties
- The “cloud”

Credit: The Data Quality Campaign
Hypothetical

A parent in your school district has requested access to their child’s record. What do you do? What data is part of the student record? Can you charge the parent for the time or copy costs? What if the parent says something is wrong in the record?
An Overview of the Student Privacy Landscape
FERPA

- Primary student privacy law for years
- Passed in 1974 in response to abuses, and periodically updated (primarily through regulations)
- More of a parental rights statute than a privacy-focused statute
FERPA

- Right to *annual notification* of FERPA policy
- Right of *access* to own education records
- Right to seek *amendment/correction* of own education records
- Right to *confidentiality* of personally identifiable information in own education records
- Right to *file a complaint* with FPCO for alleged violations
FERPA

- Exceptions for Disclosure
  - Directory information
  - School Official
  - Studies
  - Audit or Evaluation
- Penalty: Loss of all federal funding
Federal Actions

- In January 2015, President Obama offered a multi-pronged strategy to protect student data privacy.
- There were several still-pending student data privacy bills introduced in Congress in 2015, and a FERPA re-write will likely pass in 2017.
States Have Passed 70 Laws Since 2013

NASBE
National Association of State Boards of Education

www.nasbe.org
2016 State Legislative Activity

116 + 73 bills related to student data privacy in 39 states.

22 laws passed in 15 states.

NASBE | National Association of State Boards of Education

www.nasbe.org
Other State Activity

- Regulations
- Executive Orders
- Resolutions
- Guidance
39 States Have Introduced One of Two Models

22 States Have Passed One of Those Two Models

Updated 9/6/2016

- Introduced SOPIPA and/or Student DATA Model Bills
- Passed laws like SOPIPA or Student DATA Act
- Both laws passed
- No legislation introduced

NASBE | National Association of State Boards of Education

www.nasbe.org
Unintended Consequences

- Has been a huge problem throughout this debate
  - Louisiana
  - Oklahoma
  - Kansas
  - New Hampshire
- Words matter
- Fear-based policies
- Privacy problems with privacy legislation
- The need for input
Interesting Trends

- Governance
  - Longitudinal Data Boards
- Disciplinary Record or Medical Record Provisions
- Opt-In or Out Requirements
- Device and social media privacy
- Penalties (financial and criminal)
- Audits
Missouri Audit Criteria

- Data Governance
- Security Controls
- User Accounts
- Incident Response & Continuity Planning
- Security Awareness Program
- Vendor Monitoring
Training is Essential

- Anyone who handles data should know how to protect those data.
- Provisions for training appear in only a couple of the more than 400 bills introduced.

Human error is a factor in 95% of data security incidents.

NASBE
National Association of State Boards of Education
www.nasbe.org
Types of Risk

- An actual security or privacy risk
- Risk of not being in compliance
- Perception risk
So What Do Administrators and Teachers Need To Know?
Hypothetical

A parent in your school district was looking on their school’s website for information about how the school handles students with allergy medication. The parent finds that the school has accidentally posted on their school's webpage a list of all students with allergies and the medications they take.
Administrators Need To Know...

- How To...
  - Create a culture of privacy
  - Ensure transparency
  - Provide oversight
Administrators Need To Know...

- Depends on the district or school:
  - What supports are available?
  - How many vendors do they contract with?
  - How many ed tech products are they using?

- Basic internet and computer safety information

- Basics of laws

- The dangers of unintentional student data disclosure

- Contract and app issues
Administrators Need Resources and Training On...

- Data Governance and Security
- Transparency
- Vendor Monitoring
- Training Teachers and Other Staff
Administrators Need Resources and Training On...

- Data Governance and Security
- Transparency
- Vendor Monitoring
- Training Teachers and Other Staff
Process

• Review Your Resources
• Identify and Seek Input from Stakeholders
Data Governance
Governance as Foundation

• Processes and systems governing data quality, collection, management, and protection

• Formal policies defining:
  – Roles and responsibilities
    • Data access, disclosure, and use
  – Data management and monitoring
  – How data are collected, accessed, and used
Nothing to Hide

- Strong regulations
- Procedures for compliance
- Training available to all stakeholders
- Strategy to respond to incidents
- Personal investment
- Respect for stakeholders
Select the Person(s) in Charge

• Who will answer people’s questions?
• Who creates policy and guidance?
• Who enforces the policies?
PTAC

Student Privacy 101: FERPA for Parents and Students

Ever have questions about your rights regarding education records? This short video highlights the key points of the Family Educational Rights and Privacy Act (FERPA).

View More

Recently Released Documents
- 05/10/2016 - OCR response to Louisiana on Enrollment Data and Disclosure Avoidance
- 08/20/2015 - Checklist for Developing School District Privacy Programs
- 08/25/2015 - Responsibilities of Third-Party Service Providers under FERPA
- 08/24/2015 - Contractor Responsibilities under the FERPA's Audit or Evaluation Exception

Parent and Students:
Learn more about the Family Policy Compliance Office (FPCO)

Send a Request to PTAC:
Send a request now to the Privacy Technical Assistance Center

Email Updates:
We're looking forward to staying connected!

Service Offerings:
PTAC Training and Technical Assistance Services

Early Childhood Data Privacy

http://ptac.ed.gov/
CoSN Privacy Toolkit, Training, and TLE

Protecting Privacy in Connected Learning Toolkit

Version 2, September 2014

Considerations When Choosing an Online Service Provider for your School System

Includes key information on FERPA and COPPA plus:
- New sections on HIPAA and PPRA
- Ten Steps Every District Should Take Today
- Infographic on Privacy Practices to Share with Parents/Guardians

https://www.cosn.org
NCES Forum Guide to Education Data Privacy

Administrators Need Resources and Training On...

- Data Governance and Security
- Transparency
- Vendor Monitoring
- Training Teachers and Other Staff
Data Wall Hypothetical

You are a new principal in a new school and a parent emails you to complain that on a recent parent’s night they the teacher projected an app that showed a “wall” of the performance of all the students in the class.

What are Data Walls?

• A visual, interactive representation of data that displays results over a period of time to provide an “at a glance” look at the school’s data as a whole, for specific classrooms, and individual students.
The Importance of Transparency

- Vital to build trust
- If LEAs and SEAs do not take the lead in being transparent, legislatures will pass laws requiring transparency – often in ways that may be burdensome (and not particularly useful to parents)
- In the absence of being transparent...

Schools, districts, and states have not always done a good job explaining to parents the vital role data play in education, and this lack of communication has frayed the trust between parents and schools.
School districts often sell student data to companies, which can access K-12 students’ personal data. Who can access K-12 students’ personal data? No one really knows.

The New York Times

With Tech Taking Over in Schools, Worries Rise

Teachers use behavior management systems to dole out positive and negative feedback in real time. Each child’s status may be visible to the class. Behavior data can be used to create reports for administrators.

Common Core: Data Collection from Cradle to Adulthood

Data analytics programs record every keystroke, and parents make while using digital materials. This is used to create weaknesses that can be tailored to individualized needs.

POLITICO

Data mining your children

Grooming Students for a Lifetime of Surveillance

The New York Times

Student Data Collection Is Out of Control

Student data is sent to state education departments. Some states also gather info on pregnancy, homelessness, and bullying. Some companies track students into the Big Brother: Meet the Parents

School-issued devices like laptops contain location-tracking technology that may monitor activity on password-protected sites, including webmail and social media.
What Do We Mean By Transparency?

- Explain the “who, what, where, why, and when” of data collection
- Make the data easy to find and understand – the “Grandma” Test
Communications Toolkit

APRIL 2016
STUDENT DATA PRIVACY COMMUNICATIONS TOOLKIT

What Do We Mean By Transparency?

- Explain the “who, what, where, why, and when” of data collection
- Make the data easy to find and understand – the “Grandma” Test
It Can (and Should) Be Simple...

Chesterfield County Public Schools is serious about the privacy of student data and wants to make efforts to preserve student privacy as transparent as possible. To learn more, click these icons:

- CCPS Apps & Privacy
- Privacy FAQs
- Privacy Policies & Guidelines
- Ask a Question

Chesterfield County Public Schools
P.O. Box 10, Chesterfield, VA 23832
(804) 748-1403

Sign in | Report Abuse | Print Page | Powered by Google Sites
Leading Districts: Denver Public Schools

Student Data Privacy

1. Before you use any software that includes any student data, go and check the district Academic Technology Menu or the list of FERPA-approved apps. It's easy to search the district academic technology menu and find the website, app, or software you plan to use.
2. When you find the tool you want to use, check its FERPA status. If it's listed as "approved" that means that student data can be shared with the company that runs the tool and you are clear to use it.
3. If the tool is listed as "Parent Consent Required," you'll need to get parent permission. If you don't find the website or app you are looking for on the menu, you'll also have to get parent consent.
   - Active parent consent means that the parent or guardian of every student would sign a permission form for their data to be in that website, app, or software.
   - These forms are found on the right side of this page.
4. You can send parent consent forms home for each online tool, or you can use the form that lets you list multiple tools. You can do this classroom by classroom or for your whole school.
   - These forms are found on the right side of this page.
   - You have to do this each year for each tool.
   - Store the consent forms for one school year.
   - If you don't get consent, you can't put student data in the application.
5. Student data can also be anonymized.

Links
- FERPA-Approved App List
- Board Policy JRA/JRC Student Records/Release of Information on Students

Forms
- Parental Consent template for using multiple tools [docx]
- Parental Consent template for using multiple tools (Spanish) [docx]
- Parental Consent template for unsupported apps [pdf]
- Parental Consent template for unsupported apps [docx]

Wisconsin’s Amazing Webpage

Student Data Privacy Main Menu

About Student Data Privacy

Using student data for district, school, and classroom improvement planning can be very helpful when it is used correctly and with the necessary security and privacy practices in place. Although data can be used to facilitate change and improvement, there is a need to balance the usefulness of this data with the privacy of the students who the data is about. Use the following links to become more familiar with Student Data Privacy.
Administrators Need Resources and Training On...

- Data Governance and Security
- Transparency
- Vendor Monitoring
- Training Teachers and Other Staff
Hypothetical: Step 1

You “Google” your child’s name online and find links to an online math app used by teachers in your child’s school. In addition you find student work and the grades of many students exposed.
Hypothetical: Step 2

Further investigation of the app reveals that the company’s privacy policy & terms of service clearly state the company owns the data and they can do whatever they want with it.
Hypothetical: Step 3

You learn that your school district has no process in place to vet online applications or any sort of professional development for staff around student data privacy.
Vendor Monitoring

- Limit data use for non-educational purposes
- Contract provisions for data use/storage
Protecting Student Privacy While Using Online Educational Services: Model Terms of Service

About PTAC
The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a “one-stop” 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. PTAC provides timely information and updated guidance through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of student data systems. More PTAC information is available at http://ptac.ed.gov.

PTAC welcomes input on this document and suggestions for future technical assistance resources relating to student privacy. Comments and suggestions can be sent to PrivacyTA@ed.gov.

Purpose of this Guidance
In February 2014, PTAC issued guidance titled Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices. This Model Terms of Service document is intended to further assist
Badges and Seals and Pledges, Oh My!

Clever’s new badges help K-2 students access apps on its education platform.

KEN YEUNG  APRIL 19, 2016 6:00 AM
TAGS: CLEVER, CLEVER BADGES, CLEVER NEWS, EDTECH, EDUCATION

IKEEPSAFE BLOG

NEW BADGES TO IDENTIFY EDTECH PRODUCTS THAT PROTECT PRIVACY
January 13, 2015 | 0 Comments | Share

200 Companies Serving Students and Schools have now Signed the Student Privacy Pledge

LATEST NEWS

New Tool Helps Schools Manage Digital Policies and Practices

A new tool from Internet Keep Safe Coalition (iKeepSafe) in partnership with edtech innovator BrightBytes will help schools and districts best manage their current digital policies and procedures.

Called the Digital Privacy, Safety & Security module, the new tool helps users “access research-based content and exemplars from across the country to help fulfill their privacy and safety responsibilities. Through the new module, iKeepSafe and BrightBytes...
Common Sense Media Privacy Policy Browser

Actively Learn

AUDIENCE
Parents, Teachers, Students

GOOD TO KNOW
Vendor requires Parental Consent managed by School, Used with Under 13

PRIVACY POLICY
Policy length: 5,158 words
No. of policies: 2
Time to read: 42 minutes

SAFETY
PRIVACY
SECURITY
COMPLIANCE

What's This?
What's This?
What's This?
What's This?

Read the full evaluation

Class Dojo

AUDIENCE
Parents, Teachers, Students, Other (Staff etc.)

GOOD TO KNOW
Vendor has Parental Consent verification process, Used with Under 13

PRIVACY POLICY
Policy length: 16,023 words
No. of policies: 2
Time to read: 129 minutes

SAFETY
PRIVACY
SECURITY
COMPLIANCE

What's This?
What's This?
What's This?
What's This?

Read the full evaluation

Code.org

Desmos

https://privacy.graphite.org/
Student Data Privacy Consortium

Massachusetts Student Privacy Alliance

About MSPA
Search the Database
View Participating Districts
Download Student Data Privacy Agreement
V3 V2a (Includes Terms of Service) | V1
Learn more about the Agreement Types
District Login Page

Are your students safe online? Join us!

https://secure2.cpsd.us/mspa/
Massachusetts Student Privacy Alliance

STUDENT DATA PRIVACY SPECIAL TERMS AND CONDITIONS

This Student Data Privacy Special Terms and Conditions dated [date] (hereinafter “Agreement”) is by and between [Enter School Name] (“ABR”) and [Contractor], a contractor performing institutional services and functions that will require student data to perform those services and functions.

1. Contractor and ABR have contracted for the Contractor to provide [Services], which are institutional services and functions, to ABR. In the course of performing the Services, Contractor will obtain confidential student records and/or confidential student record information that contain personally identifiable student records, data and/or personally identifiable information and other non-public information, including but not limited to student data, meta data and user content (“Data Files”). ABR and Contractor acknowledge and agree that this Agreement is for the purpose of sharing Data Files between the parties in a manner consistent with the Family Education Records Privacy Act of 1974 (“FERPA”) and Massachusetts student record regulations, 603 C.M.R. 23.00 (“State Regulations”). The Data Files will be used by the Contractor and its employees to populate student data only for the purpose of delivering these Services. Contractor further acknowledges and agrees that all copies of such Data Files, including any modifications or additions to Data Files or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Data Files. The ability to access or maintain Data Files and/or any portion thereof under this Agreement shall not under any circumstance transfer from Contractor to any other party.

2. Contractor acknowledges and agrees that it is providing institutional services or functions for ABR and that it is under direct control of ABR with respect to the use and maintenance of Data Files in connection with these Services. Contractor additionally acknowledges and agrees that at no point in time is the Contractor the owner of the Data Files. Ownership rights are maintained by ABR and ABR reserves the right to request the prompt return of any portion of the Data Files and/or all Data Files at any time for any reason whatsoever. Contractor further acknowledges and agrees that it shall adhere to the requirements set forth in both federal and state law regarding the use and re-disclosure of the Data Files or any portion thereof, including without limitation, any student data, meta data, user content or other non-

https://secure2.cpsd.us/mspa/
Student Data Privacy Consortium

Privacy Contract Framework
The first project of the group was to leverage the great work done by the Massachusetts Student Privacy Alliance (MSPA) and their work around a “common contract” for usage across 40 districts. The clear expectation by establishing the contract and the partnership has benefited districts and even the vendors working with them. This project looks to exponentially leverage and expand upon this work.

The Privacy Contract Framework resources and tools can all be found in the SDPC App.

Track one is designed for schools, districts or regional organizations/associations or state agencies that do not yet have a model/template contract designed specifically for their jurisdiction. Organizations entering into the project via track one will utilize SDPC products and resources to assist with the development of a model/template contract. These resources will include model contract clauses, appropriate federal and state laws, examples of other jurisdiction’s model contracts as well as interaction with the community members to develop a new model contract. Get Started >>

Track two is designed for schools, districts or regional organizations/associations or state agencies that do have a model/template contract designed specifically for their jurisdiction and are ready to create a jurisdictional specific alliance for the purpose of utilizing shared model contracts. Organizations entering into the project via track two will utilize SDPC products and services to create and implement a specific jurisdictional alliance. These resources will include an online tool for the management of the contracting process by all alliance members, including inventoring applications, tracking contract status, posting contracts, and creating transparency with all stakeholders. Get Started >>

https://secure2.cpsd.us/a4l/index2.php/
Other Factors to Consider

• Click-Wrap Agreements
• Defining Who Can “Sign” Contracts
• Sub-Contractors
• Requiring Certain Training
• Having a “standard” set of contract requirements might backfire
Administrators Need Resources and Training On...

- Data Governance and Security
- Transparency
- Vendor Monitoring
- Training Teachers and Other Staff
What Do Teachers Need To Know?

- Basic internet and computer safety procedures
- How to use data to help students
- The dangers of unintentional student data disclosure
- How to use apps safely
Wisconsin Student Privacy Training Webpage

Student Data Privacy Training

Now that you have a solid base understanding of Student Data Privacy concepts we can talk about training. (If you have not yet visited the Student Data Privacy Overview page, go there to get a general understanding of the importance of Student Data Privacy terms and concepts before you complete any training.) Use these materials yourself or share with others in your organization to ensure everyone understands data privacy and confidentiality.

<table>
<thead>
<tr>
<th>Training</th>
<th>Created By</th>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Overview</td>
<td>Multiple</td>
<td>We recommend that everyone start with the materials listed on the Privacy Overview page which include a Student Privacy 101 video, a link to the Wisconsin Pupil Records Law, and an Overview of Student Data Privacy.</td>
<td><a href="http://dpi.wi.gov/wise/data-privacy/overview">http://dpi.wi.gov/wise/data-privacy/overview</a></td>
</tr>
<tr>
<td>Protecting Personally Identifiable Information (PII)</td>
<td>DPI</td>
<td>A 10-15 minute training module on how to protect PII.</td>
<td><img src="image" alt="Icon" /></td>
</tr>
<tr>
<td>Student Records and Confidentiality</td>
<td>DPI</td>
<td>A bulletin designed to help local school districts develop their own local policies regarding student records and confidentiality.</td>
<td><a href="http://dpi.wi.gov/sites/default/files/mentor/sspm/pdf/mentorconfidential.pdf">http://dpi.wi.gov/sites/default/files/mentor/sspm/pdf/mentorconfidential.pdf</a></td>
</tr>
</tbody>
</table>

Protecting Personally Identifiable Information (PII)

When you possess an individual's personal information, it is your responsibility to protect the individual's privacy. Ethically, employees are obligated to be vigilant about protecting other individuals' personally identifiable information so they will not create any undue harm to the individual or to the organization. Treat others’ personally identifiable information (PII) as if it is your own.

This training should take about 10-15 minutes to complete.
Wisconsin Student Privacy Training Module

Actions To Protect PII

Click on each picture to learn how to protect SII in different situations.

- In your office
- On electronic devices
- Traveling
- Sharing with others
- Working remotely

https://dpi.wi.gov/wise/data-privacy/training
Ask Before You App

Video Tool: Keeping an Eye on Privacy

Integrating educational apps and tools safely, responsibly, and effectively can be a challenge. This short video provides guidelines for today’s education professionals. It is a handy reference for classroom teachers and as a training tool for professional development.

http://www.f3law.com/resources.php?id=155&rs_id=69
New Educator’s Guide to Student Privacy

Technology tools and apps are making it possible for educators and students to collaborate, create, and share ideas more easily than ever. When schools use technology, students’ data—including some personal information—is collected both by educators and often the companies that provide apps and online services. Educators use some of this data to inform their instructional practice and get to know their students better. It is just as essential for educators to protect their students as it is to help them learn.

This guide is meant to help teachers utilize technology in the classroom while protecting their students’ privacy.

Privacy Courses for Teachers

IKEEPSAFE PRIVACY COURSES FOR K12 TEACHERS AND ADMINISTRATORS

Protecting Student Privacy and Advancing Learning

Student data privacy concerns can create hurdles to expanding access to edtech and digital innovations. Addressing those concerns, and helping parents and others understand how student personal information is used — and protected — is essential. K12 educators have a unique role in managing edtech, student data, and privacy, and in building parent confidence in digital learning.

The iKeepSafe Privacy Courses for educators focus on three objectives:

- Communicate the importance of balancing innovations in learning with privacy and security responsibilities.
- Explain the importance of teaching all students and staff about student data privacy and security.
- Describe why everything and everyone who connects to the school network must comply with privacy and security requirements.

As an educator and an edtech leader, you probably know some of this information already. These materials are designed to help you talk with parents about edtech and students’ personal information — and to help colleagues address issues they may face when expanding technology in their classrooms.

Find iKeepSafe’s Privacy Courses:

http://ikeepersafe.org/privacyeducation/
Learning Through Teaching

Safety, Privacy, and Digital Citizenship
High School Curriculum

Learning Through Teaching

About

What is the DLRP?
The Digital Literacy Resource Platform (DLRP) is an evolving collection of tools that you can use to learn more about online safety, privacy, information quality, creativity, and copyright. These tools aim to empower you with knowledge about connected learning environments and other parts of the digital world so you can make the online choices that are right for you. If you are responsible for educating others, these tools will also support you as you teach, parent, or fill other valuable guidance roles. Our goal is to support the co-creation of trustworthy and supportive digital spaces for all of us.

The DLRP is designed and maintained by the Berkman Center for Internet & Society at Harvard University, with support from the MacArthur Foundation’s Digital Media Literacy Trust Challenge Competition.

Who can use the DLRP?
Anyone! There is something here for everyone, with a focus on resources for educators, librarians, school administrators, parents, and youth. Even if a resource is labeled for a different audience, go ahead and try it out! The digital world is dynamic, and these tools are designed to be as well. If something looks interesting, check it out!

What tools are available?
A lot! The DLRP hosts tools that explore four main areas of digital life: privacy, safety, information quality, and creative expression. Within each area, tools address a range of issues, using different formats to do so. For instance, if you want to learn more about the primary federal laws that govern whether and how schools can share students’ private data, you could check out our Guide to the Family Educational Rights and Privacy Act (FERPA) and the Children’s Online Privacy Protection Act (COPPA) that explains these laws in a user-friendly, Q&A format. And if you want to learn more about how to address cyber-bullying, you could take a look at our video on a “tale of tolerance.” If you’re a 6th grade educator looking for a lesson on password management, check out our middle-school privacy curriculum. Lots of good stuff!

What can I use this for?

http://dlrp.berkman.harvard.edu/About
Privacy Education

Volunteer Privacy Educators Program

Fordham CLIP’s Volunteer Privacy Educators Program is a first-of-its-kind privacy education program aimed at engaging middle school students in discussions about privacy and its relevance in their lives. CLIP created a series of lesson plans and visual aids to be used by instructors in middle school classrooms to teach students about what privacy is, how it may be relevant to young people’s lives, and how the technologies they regularly use impact their privacy. Specific topics include:

- Managing an Online Reputation
- Understanding How Technologies Work
- Dealing with Social Media
- Maintaining Secure Passwords

The Volunteer Privacy Educators Program is supported by a grant from the Digital Trust Foundation.

https://www.fordham.edu/info/24071/privacy_education/
NASBE Data Privacy Resources
What other resources do you feel you need?
QUESTIONS OR WANT MORE INFO?

Amelia Vance
Director of Education Data & Technology
Amelia.Vance@nasbe.org
@ameliaivance

http://tinyurl.com/nasbesdpresources