



Student Privacy and Data Governance

Data Quality Network Meeting
Pennsylvania Association of Intermediate Units
1/18/2017

An Overview of the Student Privacy Landscape

Landscape of Privacy Concerns

- ▶ The “cloud”
- ▶ The scope and type of student data schools collect
 - ▶ The collection of much more sensitive data
- ▶ Who is collecting and accessing student data/education records
- ▶ Federal/State
- ▶ Third parties
- ▶ How student data is being used
- ▶ Privacy beyond data

Types of Risk

- ▶ An actual security or privacy risk
- ▶ Risk of not being in compliance
- ▶ Perception risk

Credit: Jim Siegl, Fairfax County Public Schools, Virginia

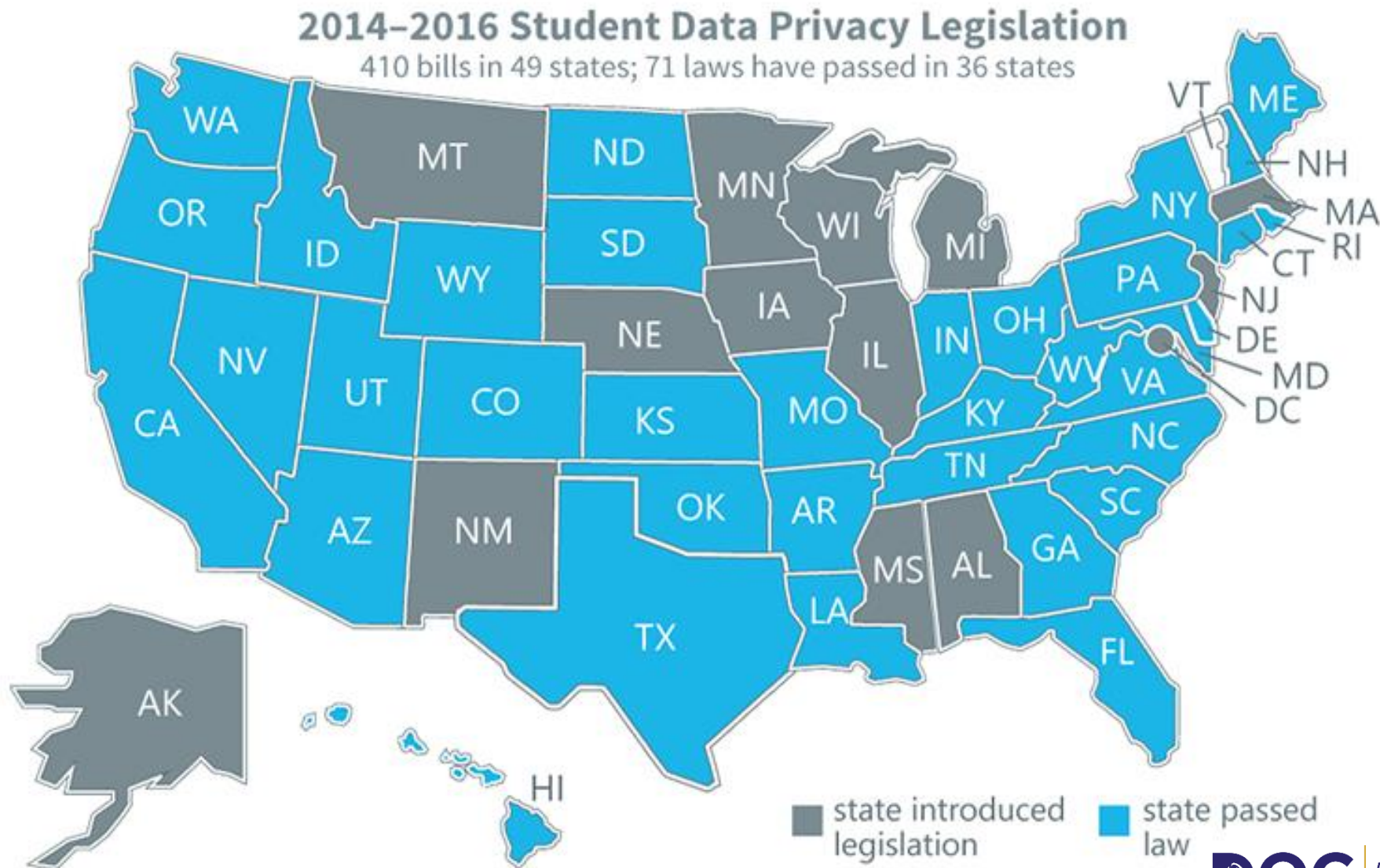
Federal Actions

- ▶ 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 may pass in 2017



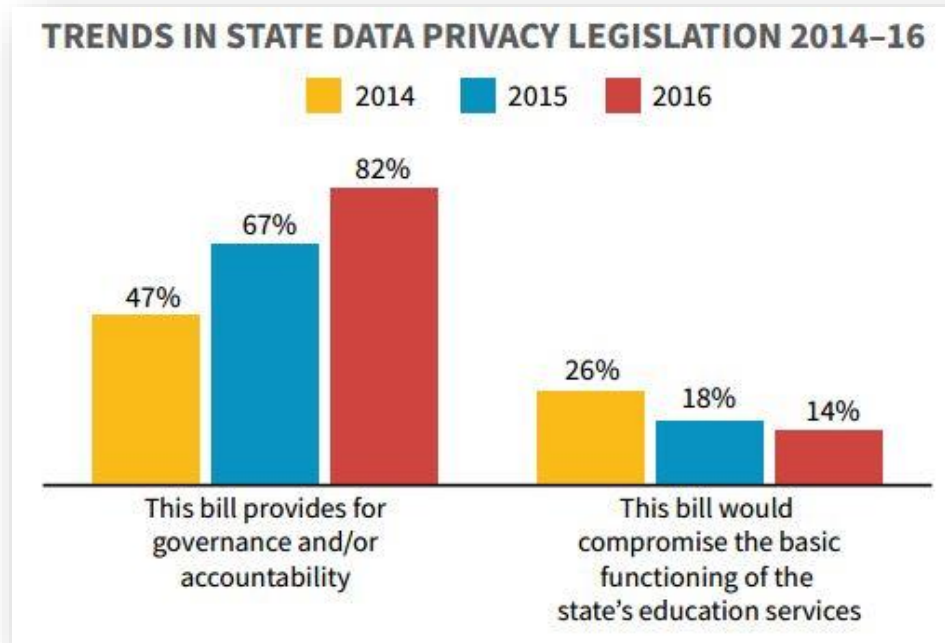
36

States Have Passed 80 Laws Since 2013



2014-2016

- ▶ **49** states and DC have introduced at least one student privacy bill
- ▶ Only **18** bills have addressed training since 2014 (out of more than 400 student privacy bills)

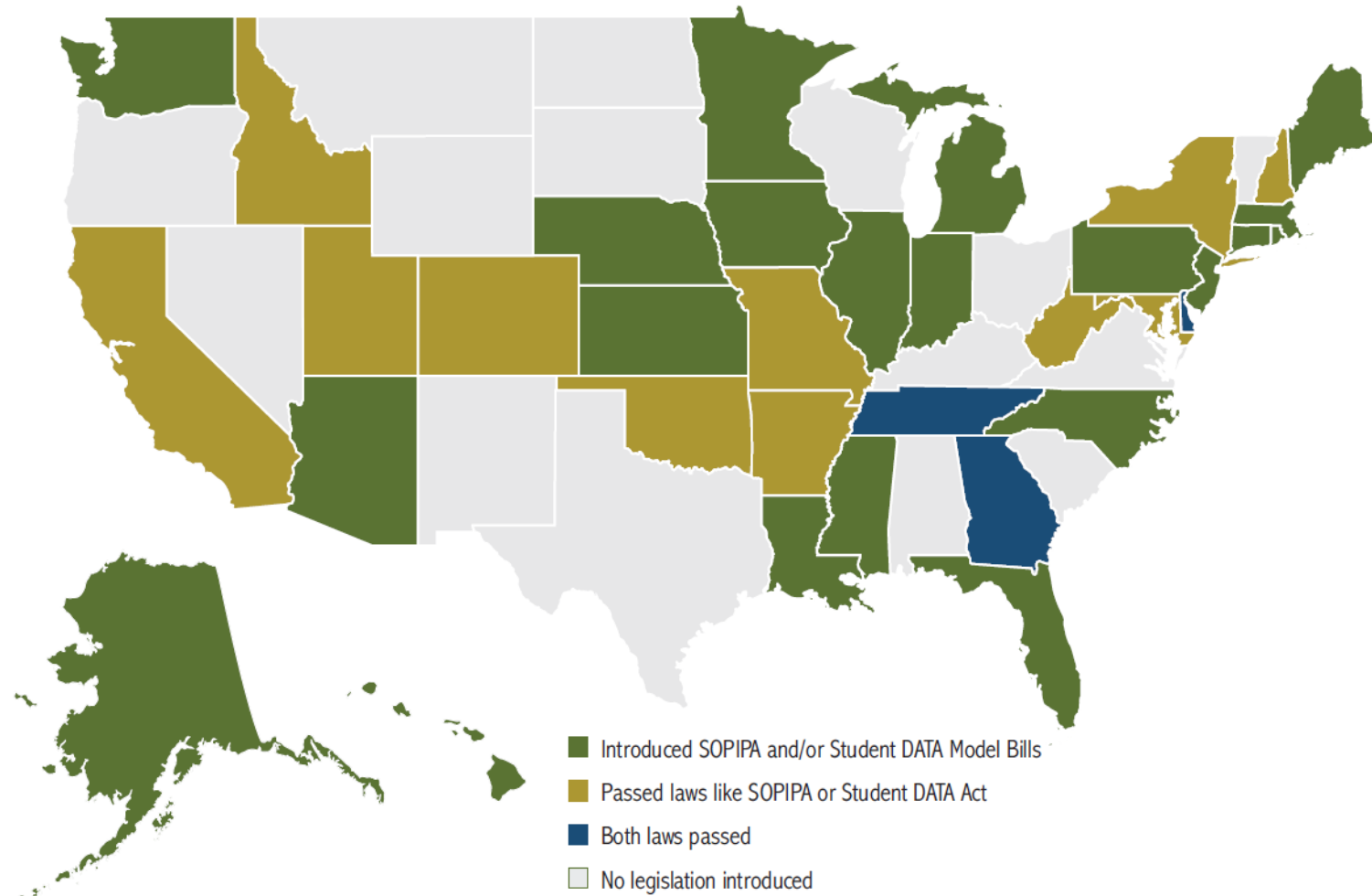


Other State Activity



- ▶ Regulations
- ▶ Executive Orders
- ▶ Resolutions
- ▶ Guidance

39 States Have Introduced One of Two Models



22 States Have Passed One of Those Two Models

Unintended Consequences

- ▶ Has been a huge problem throughout this debate
 - ▶ Louisiana
 - ▶ Oklahoma/Colorado (N-sizes)
 - ▶ Connecticut (parental notifications)
 - ▶ Kansas (research)
 - ▶ New Hampshire (video recordings)
 - ▶ Texas (video/audio recordings)
- ▶ Words matter
- ▶ Fear-based policies
 - ▶ Sen. Vitter legislation; GA Executive Order
- ▶ Privacy problems with privacy legislation
 - ▶ Sen. Markey/Hatch legislation
- ▶ The need for input

Interesting Trends

- ▶ Governance
- ▶ Disciplinary Record or Medical Record Provisions
- ▶ Opt-In or Out Requirements
- ▶ Device and social media privacy
- ▶ Audits
- ▶ Penalties (financial and criminal)
- ▶ Training

Best Practices

Best Practice “Buckets”

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

Process

- ▶ Review Your Resources
- ▶ Identify and Seek Input from Stakeholders



Best Practice “Buckets”

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

- 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

PTAC

<http://ptac.ed.gov/>



Privacy Technical Assistance Center
U.S. Department of Education



[Home](#) | [About](#) | [PTAC Toolkit](#) | [FAQs](#) | [Glossary](#) | [Contact Us](#)

SEARCH

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](#)



Parents and Students:

Learn more about the Family Policy Compliance Office (FPCO)

[Learn more](#)



Send a request to PTAC:

Send a request now to the Privacy Technical Assistance Center

[Send](#)



Email Updates:

We're looking forward to staying connected!

[Subscribe](#)



Service Offerings:

PTAC Training and Technical Assistance Services

[View more](#)



Early Childhood Data Privacy

Learn more about protecting the privacy

RECENTLY RELEASED DOCUMENTS

FUTURE OF PRIVACY FORUM

[Enrollment Data](#)

[District Privacy Programs
Service](#)

[for the FERPA's](#)

08/24/2015 - [Policies for Users of Student Data Checklist](#)



CoSN Privacy Toolkit, Training, & TLE

<https://cosn.org/>



Protecting Privacy
in Connected Learning
A CoSN Leadership Initiative

Protecting Privacy in Connected Learning Toolkit

Version 2, September 2014

Considerations When Choosing
an Online Service Provider
for your School System



**FUTURE OF
PRIVACY
FORUM**

Information on FERPA and COPPA

Information on HIPAA and PPRA

Five Steps Every District Should Take Today

- Infographic on Privacy Practices to Share with Parents/Guardians

NCES Forum Guide to Education Data Privacy

http://nces.ed.gov/pubs2016/Privacy_Guide_508_7.6.16.pdf



Best Practice “Buckets”

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

Transparency is **VITAL** to build trust

- ▶ Schools, districts, and states have not always done a good job explaining to parents the vital role data plays in education, and this lack of communication has frayed the trust between parents and students.
- ▶ 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...

School districts often use companies, which
Who can access K-12 students' personal data? No one really knows

emergencies.

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.

student IDs, can make it possible to track students' movements on and off the bus and in school. This potentially sensitive information.

MICHELLE MALKIN
Look who's data-mining your toddlers

biometric data collection.

Data analytics programs record
e key stroke, and
p ents make while
w digital materials.
T used to create

Common Core: Data Collection from Cradle to Adulthood

weaknesses that can be tailored to individualized needs.

POLITICO

Data mining your children

School MODEL VIEW CULTURE
disciplin Technology, culture and diversity media.

Grooming Students for A Lifetime of Surveillance

ence, grades, at-risk status, cal and psychological also be included.

photos, to some companies, including yearbook publishers and class-ring marketers, without written consent

HUFF POST EDUCATION

Student Privacy in Peril: Massive Data Gathering With Inadequate Privacy and Security

The New York Times

Student Data Collection Is Out of Control

grades may be based now hard a student works out.

Basic student data is sent to state education departments. Some states also gather info on pregnancy, homelessness, and bullying. Some students into the

POLITICO

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 is Transparency?

- ▶ Explaining the “why, what, who, and how” of data collection:
 - ▶ Why is data collected?
 - ▶ What data is collected?
 - ▶ Who is able to access or use my child’s data?
 - ▶ How is the data protected?



Communications Toolkit

<http://www.excelined.org/wp-content/uploads/Student-Data-Privacy-Comms-Toolkit.pdf>

APRIL 2016

STUDENT DATA PRIVACY COMMUNICATIONS TOOLKIT

- Student Data Privacy Key Messages
- Student Data Privacy Web Page Content
- Student Data Privacy Frequently Asked Questions
- Student Data Privacy Fact Sheet
- Student Data Privacy Letter to Parents/Guardians
- Student Data Privacy Talking Points
- Rapid Response Tool: Student Data Privacy Newsletter/Article
- Rapid Response Tool: Student Data Privacy Lawmaker Brief
- Rapid Response Tool: Student Data Privacy Newspaper Opinion Pieces
- Rapid Response Tool: Student Data Privacy Social Media Posts

What is Transparency?

- ▶ Make the data easy to find and understand – the “Grandma” Test



<https://www.flickr.com/photos/kimsandiego/8168063548>

It Can (and Should) Be Simple...

The screenshot shows a web browser window with the address bar displaying <https://sites.google.com/a/ccpsnet.net/anytime-anywhere-learning/privacy>. The page has a black header with the logo "Anytime, Anywhere Learning" and a search bar. Below the header is a navigation menu with links: ABOUT, I'M A STUDENT, FAQ, I'M A PARENT, CURRICULUM, and PRIVACY. The main content area features a paragraph stating: "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:". Below this text are four buttons arranged in a 2x2 grid. The top-left button is labeled "CCPS Apps & Privacy" with an icon of a box of colorful items. The top-right button is labeled "Privacy FAQs" with a circular icon containing the letters A, F, and Q. The bottom-left button is labeled "Privacy Policies & Guidelines" with a padlock icon. The bottom-right button is labeled "Ask a Question" with a question mark icon. At the bottom of the page, contact information for Chesterfield County Public Schools is provided, along with links for "Sign in", "Report Abuse", "Print Page", and "Powered By Google Sites".

<https://sites.google.com/a/ccpsnet.net/anytime-anywhere-learning/privacy>

Anytime, Anywhere Learning

[ABOUT](#) [I'M A STUDENT](#) [FAQ](#) [I'M A PARENT](#) [CURRICULUM](#) [PRIVACY](#)

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) 748-1405

[Sign in](#) | [Report Abuse](#) | [Print Page](#) | Powered By [Google Sites](#)

Leading Districts: Denver Public Schools

<https://academictechnologymenu.dpsk12.org/studentdataprivacy.aspx>



The screenshot shows the Denver Public Schools Academic Technology Menu. The header includes the Denver Public Schools logo with the tagline "Discover a World of Opportunity™" and a search bar. The main navigation bar has links: "Browse the Menu", "Search the Menu", "Submit a Tool for Evaluation", "Evaluation Process", and "Student Data Privacy Info". The "Student Data Privacy" section is active, featuring a header image of a child and three tabs: "REQUIRED VIDEO", "USING TECHNOLOGY & DATA", and "LEGAL". The "USING TECHNOLOGY & DATA" tab is selected, displaying a list of steps for using software that includes student data. The "LEGAL" tab is also visible, showing links to FERPA-approved app lists, board policy, and records release information. The "Forms" section on the right lists various consent templates and translated versions of the parental consent form.

DENVER PUBLIC SCHOOLS
Discover a World of Opportunity™

Academic Technology Menu

Browse the Menu Search the Menu Submit a Tool for Evaluation Evaluation Process Student Data Privacy Info

Student Data Privacy

REQUIRED VIDEO USING TECHNOLOGY & DATA LEGAL

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.
 - Forms are found on the right side of this page.
 - You have to do this each year for each tool.
 - You can send consent forms for one school year.
 - If you can't get consent, you can't put student data in the application.
 - Data can also be anonymized.
 - Examples that wherever you are putting a student's name, you instead put in anonymous information. So instead of a student's first name, you would put "Blue" and instead of the last name, you would put "Bonnet" or "Bunny" or "Suede Shoes".
 - This could be unwieldy for you as a teacher to keep track of which student is "Blue Bonnet" and which is "Red Rover".

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]
- Translated versions of the Parental Consent form are available on the internal Multicultural Portal (DPS Login required)



Wisconsin's Amazing Webpage

<https://dpi.wi.gov/wise/data-privacy>



Best Practice “Buckets”

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

Vendor Monitoring

- ▶ Limit data use for non-educational purposes
- ▶ Contract provisions for data use/storage

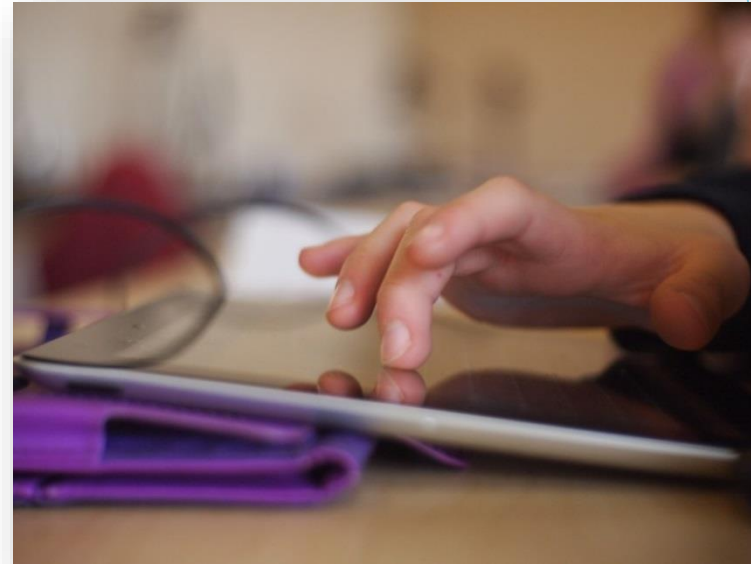


Photo Credit: Flickr user Brad Flickinger

PTAC

http://ptac.ed.gov/sites/default/files/TOS_Guidance_Mar2016.pdf



Privacy Technical Assistance Center

(855) 249-3072 ♦ privacyTA@ed.gov ♦ ptac.ed.gov



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>.



**FUTURE OF
PRIVACY
FORUM**

this document and suggestions for future technical assistance resources relating to comments and suggestions can be sent to PrivacyTA@ed.gov.

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!

http://ptac.ed.gov/sites/default/files/TOS_Guidance_Mar2016.pdf


LATEST NEWS

Student Privacy Pledge Reaches Milestone of 300 Signatories

common sense education™ Privacy Policy Annotator Browser

Reviews & Ratings Digital Citizenship Teaching Strategies Professional Development Privacy Initiative Blog

Enter name of the app you wish to search for.




Achieve3000 Literacy Solutions

AUDIENCE
Parents, Teachers, Students

GOOD TO KNOW
Used with Under 13

PRIVACY POLICY
Policy length: 5,600 words
No. of policies: 2
Time to read: 46 minutes



Actively Learn


AUDIENCE
Parents, Teachers, Students

GOOD TO KNOW
Vendor requires parental consent managed by School, Used with Under 13

PRIVACY POLICY
Policy length: 5,283 words
No. of policies: 2
Time to read: 42 minutes

SAFETY PRIVACY SECURITY COMPLIANCE


FUTURE OF PRIVACY FORUM



FERPA Certified

Gives confidence to educators and parents that student data is safe with your product, and provides simple answers about your product data practices through the product profile.


LEARN MORE



COPPA Safe Harbor

Assures parents and teachers that your product is compliant with COPPA. As an FTC Safe Harbor, iKeepSafe can protect your company against FTC fines and legal action.

LEARN MORE



California Student Privacy Certified

Provides a comprehensive certification of compliance to the most rigorous state privacy laws and requirements, including SOPIPA, California Education Codes (Contracts with Technology Providers, Student Information from Social Media), Colorado HB 1423, and others.

LEARN MORE

Student Data Privacy Consortium

<https://secure2.cpsd.us/mspa/>



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](#)



SEARCH the
Database 



**FUTURE OF
PRIVACY
FORUM**

Are your students safe online? [Join us!](#)

Questions? Concerns? [Email us](#)

[Admin](#)

Student Data Privacy Consortium

<https://secure2.cpsd.us/mspa/>



[Massachusetts Student Privacy Alliance](#) > [Search](#) > Application Profile

[New Search](#) | [About MSPA](#) | [Participating Districts](#) | [District Login Page](#)

Download Student Data Privacy Agreement

Version 3: [pdf](#)

Version 2a (includes Terms of Service): [pdf](#)

Version 1: [pdf](#)

Application Profile

BrainPOP

Company Name: BrainPOP | Contact: Shiri Levi | Email: shiril@brainpop.com | [Website](#)

District Information

Don't see your District's Information here? [Request a District Account >>](#)

Status Key

Active: Contract is signed and app is in use.

Pending: Contract acquisition process has begun. App is not in use.

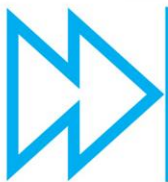
Declined: Vendor was unable to sign the contract and the app is not in use.

Show entries

Search:

District Name	Agreement Status	Agreement Type	Date Approved	Data
Pending Contract	Agreement V2 (Includes Terms of Service)			Coming Soon
ve	Agreement V2a (Includes Terms of Service)	1969-12-31		Coming Soon

Previous Next



**FUTURE OF
PRIVACY
FORUM**

Questions? Concerns? [Email us](#)

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

Best Practice “Buckets”

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

Training is Essential

- ▶ Anyone who handles data should know how to protect those data.
- ▶ Provisions for training appear in only 18 of the more than 400 bills introduced since 2014.

Human
error is a
factor in

95%



of data
security
incidents

Types of Risk

- ▶ An actual security or privacy risk
- ▶ Risk of not being in compliance
- ▶ Perception risk

Credit: Jim Siegl, Fairfax County Public Schools, Virginia

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

When Should Training Occur?

Wisconsin Student Privacy Training Module

<https://dpi.wi.gov/wise/data-privacy/training>

Menu

▼ Protecting PII

Introduction

Definitions of PII

Non-Sensitive and Sensitive PII

Context of PII

Laws That Protect PII


Workplace PII

Actions To Protect PII

Data Privacy Policies


More Resources

Protecting PII for School Districts

 WISCONSIN DEPARTMENT OF
PUBLIC INSTRUCTION

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.

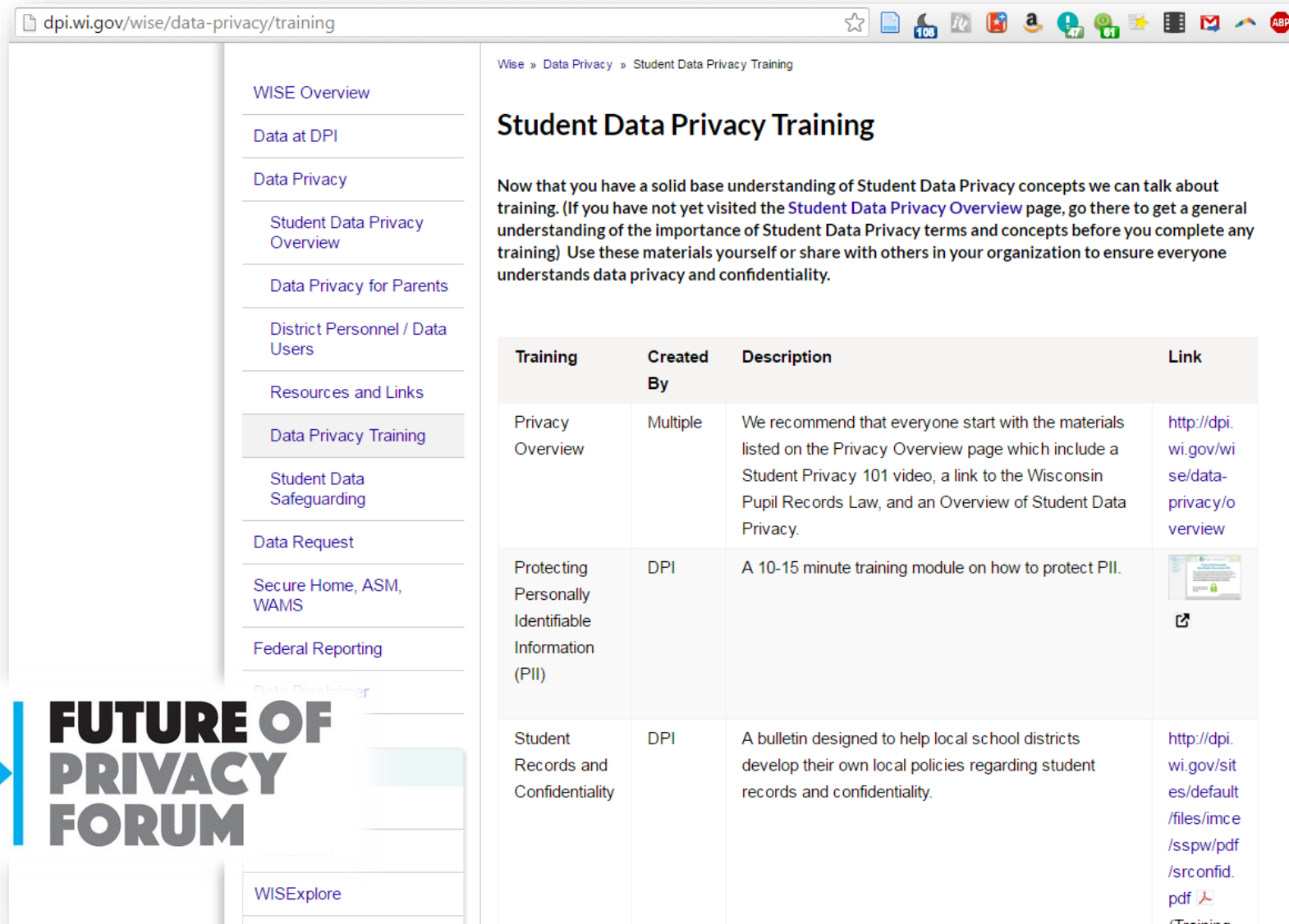
Wisconsin Department of Public Instruction
Protecting Personally Identifiable Information (PII)

NEXT >


 **FUTURE OF
PRIVACY
FORUM**

Wisconsin Student Privacy Training Module

<https://dpi.wi.gov/wise/data-privacy/training>



The screenshot displays the Wisconsin Student Privacy Training Module website. The browser address bar shows the URL dpi.wi.gov/wise/data-privacy/training. The page has a sidebar on the left with the following navigation links: WISE Overview, Data at DPI, Data Privacy, Student Data Privacy Overview, Data Privacy for Parents, District Personnel / Data Users, Resources and Links, Data Privacy Training (highlighted), Student Data Safeguarding, Data Request, Secure Home, ASM, WAMS, Federal Reporting, and Data Disclosure. The main content area is titled "Student Data Privacy Training" and includes an introductory paragraph: "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." Below this is a table with the following data:

Training	Created By	Description	Link
Privacy Overview	Multiple	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.	http://dpi.wi.gov/wise/data-privacy/overview
Protecting Personally Identifiable Information (PII)	DPI	A 10-15 minute training module on how to protect PII.	 Link
Student Records and Confidentiality	DPI	A bulletin designed to help local school districts develop their own local policies regarding student records and confidentiality.	http://dpi.wi.gov/sites/default/files/imce/sspw/pdf/srconfid.pdf

At the bottom of the sidebar, there are links for "Data Disclosure" and "WISE Explore".



Ask Before You App

http://www.f3law.com/resources.php?id=155&rs_id=69

Ask Before You App

Video Tool: Keeping an Eye on Privacy

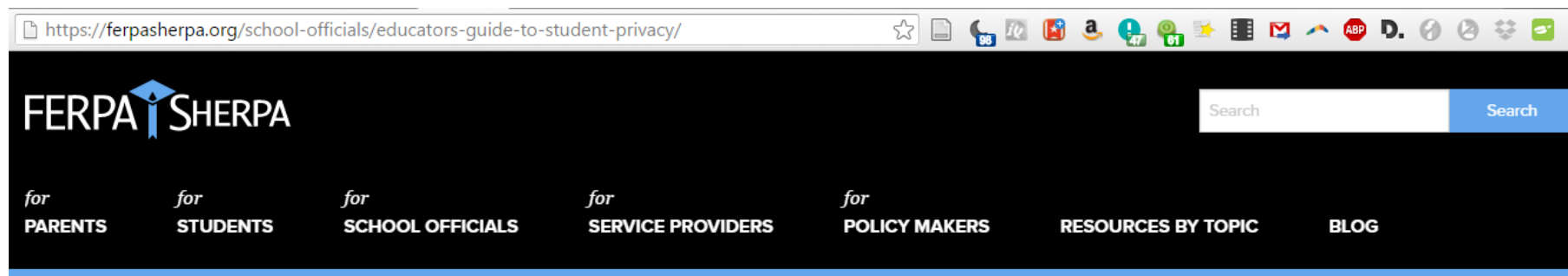
Integrating educational apps and tools safely, responsibly, and effectively can be a challenge. This short video provides guidelines for today's education professionals. It is a handy reference for classroom teachers and as a training tool for professional development.



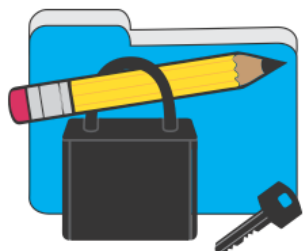
**FUTURE OF
PRIVACY
FORUM**

Educator's Guide to Student Privacy

https://ferpasherpa.org/wp-content/uploads/2016/05/EduGuide_DataPrivacy_516.pdf



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.



Why should classroom teachers care about student data privacy?

This project is brought to you by:



ConnectSafely
Smart Socializing Starts Here™

Privacy Courses for Teachers

<http://ikeepsafe.org/privacyeducation>

iKEEPSAFE

PRIVACY

BEaPRO™

PARENTS

EDUCATORS

COMMUNITIES

YOUTH

PREVENT & DETECT

ABOUT US

PARTNERSHIPS

VIDEOS

SUPPORT US

Generation Safe | BLOG |   

 SUBSCRIBE IN A READER | SHARE | 

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 students about edtech and students' personal information – and to help educators address issues they may face when expanding technology in classrooms.

Find iKeepSafe's Privacy Courses:

- Privacy Certification Course: Teachers and Employees
- Privacy Certification Course: Administrators
- Privacy Certification Course: School Board Members



Privacy Overview for K12...

Find iKeepSafe Privacy Approved Products



TOP 10 STUDENT PRIVACY TIPS FOR EDUCATORS

 bigbytes.org/privacy |  ikeepsafe.org



Learning Through Teaching

<http://blogs.harvard.edu/youthandmediaalpha/files/2016/03/DLT-Curriculum-Introductory-Materials.pdf>



Berkman

The Berkman Center for Internet & Society
at Harvard University

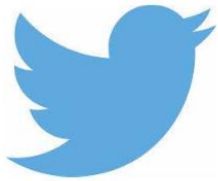
Safety, Privacy, and Digital Citizenship

High School Curriculum



**FUTURE OF
PRIVACY
FORUM**

Questions?



- ❖ www.fpf.org
- ❖ facebook.com/futureofprivacy
- ❖ [@futureofprivacy](https://twitter.com/futureofprivacy)