



Supporting Student Data Privacy: *A Ten Step Approach to Success*

Bill Fritz, Learn21

<http://bit.ly/SDPC2023-Chicago>



Today's Goals

Learn About

Our journey with student data privacy work

How Ohio got started

Processes developed that have led to our success

Lessons we have learned

Partnerships we have developed

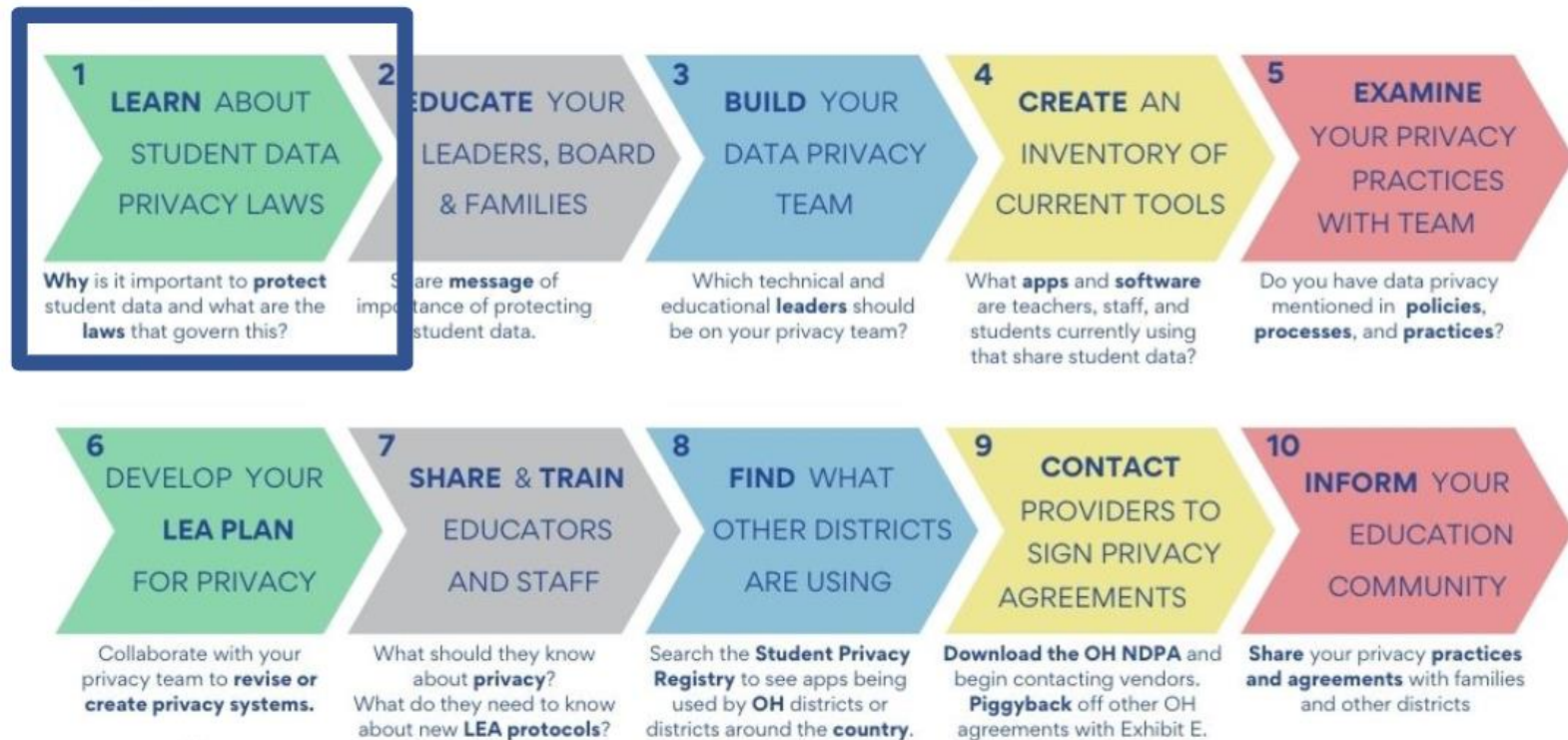
How we have messaged our work, wins and losses and plans for the future

10 concrete steps that can be replicated in their state

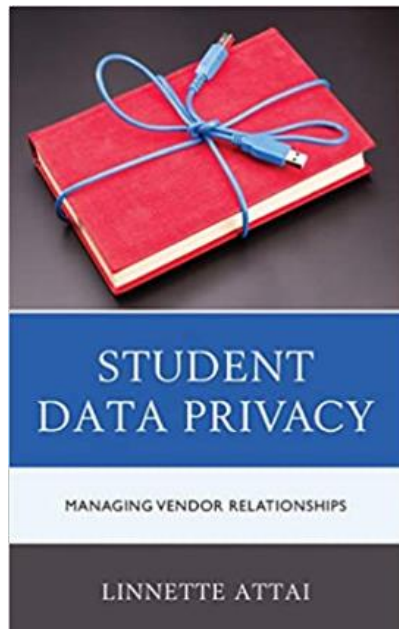
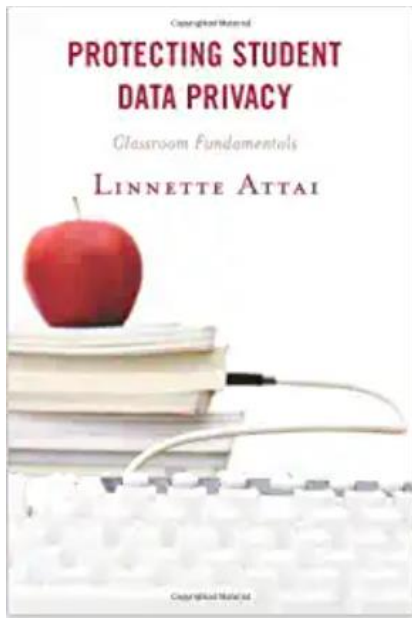
Ten Step Approach



Ten Step Approach



Ten Step Approach



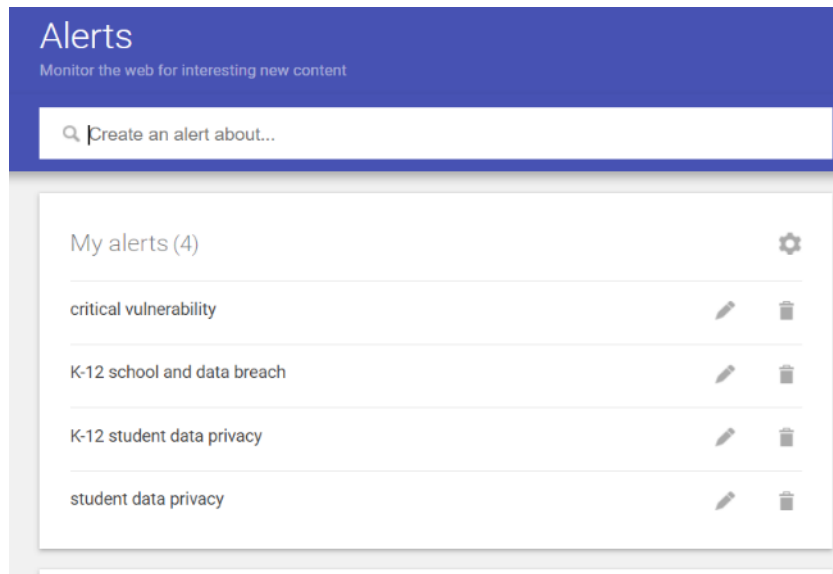
- FERPA - US Department of Education
- COPPA - Federal Trade Commission
- CIPA - Federal Communications Commission
- PPRA - US Department of Education
- HIPPA - Center for Disease Control

Ten Step Approach

2 EDUCATE YOUR
LEADERS, BOARD
& FAMILIES

[Why is important to
protect student data?](#)

- Setup a Google Alert -
<http://alerts.google.com/>
- Today's Examples
 - [Fairfax County
Schools](#)



Ten Step Approach

2 EDUCATE YOUR
LEADERS, BOARD
& FAMILIES

Why is important to
protect student data?

- **Develop your professional network**
- **Get involved in the work - committee volunteer**
- **Attend webinars, conferences**
- **Share with colleagues**

Ten Step Approach

2 EDUCATE YOUR
LEADERS, BOARD
& FAMILIES

[Why is important to
protect student data?](#)

- **WEBPAGE** - US DoE - Protecting Student Privacy
- **COURSE** - FERPA 101 by US DoE
- **COURSE** - FERPA 201 BY US DoE
- **WEBPAGE** - FAQs on PII by US DoE
- **VIDEO** - History of FERPA
- **VIDEO** - Staff Responsibilities Under FERPA
 - Note - this resource references Post K-12
- **VIDEO** - The ABCs of Student Directory Information

Ten Step Approach

2 EDUCATE YOUR
LEADERS, BOARD
& FAMILIES

Why is important to
protect student data?

- You Are Always Communicating and Marketing
- Be Ready to Share with Leaders
 - Offer relevant facts
- Be Listening for Opportunities to Share
 - Board of Education Updates
 - Weekly/Quarterly Emails/Newsletters
 - PTO sessions
 - Administrator Meetings
- Ask Essential Questions

Ten Step Approach

3

BUILD YOUR PRIVACY TEAM

Which technical, business, and educational **leaders** should be on your privacy team?

- Email to ALL STAFF and/or DIRECT REQUEST FOR INDIVIDUALS to be on the team
- Google Form requesting volunteers

Ten Step Approach

4 CREATE AN
INVENTORY OF
CURRENT TOOLS

What **apps** and **software**
are teachers, staff, and
students currently using?

- Database of Resources
 - Digital Resources Spreadsheet Template
 - Sample of Live Record
- Work with curriculum department to obtain adopted (purchased) resources
- Request information from staff
 - Google Form requesting what teachers are using
 - Email to principals and/or department/grade level leaders requesting information and purchased resources
- Application/website usage monitoring software

5
**EXAMINE YOUR
PRIVACY PRACTICES
WITH TEAM**

Where are there gaps in
your policies, processes,
and practices?

Discussions with Administration Team and School Board

- Examine Board Policy and work with Board to ensure appropriate policies are represented
 - NEOLA
 - OSBA
- Discuss processes with administration team
- Work towards CoSN's TLE Seal

6
DEVELOP YOUR
LEA PLAN
FOR PRIVACY

Collaborate with your
privacy team to **revise or**
create privacy systems

Privacy System - Not Just A Flowchart

- LEA privacy plan is more than a template of a workflow
- INITIALLY
 - Resource approval process is a good start (especially if pursuing TLE)
 - Where many are at the moment (next slide)
- LONG TERM
 - It is building an entire program and culture on technology governance

Ten Step Approach

6 DEVELOP YOUR LEA PLAN FOR PRIVACY

Collaborate with your privacy team to **revise or create privacy systems**



7
SHARE & TRAIN
EDUCATORS
AND STAFF

What should they know
about **privacy**?
What do they need to know
about new **LEA protocols**?

Suggestions & Sample Trainings

- Emails (sample on next slide)
- Videos/Screencasts
 - Quicktime Player
 - Screencastify
 - Loom
- Sessions at PD Day or delayed starts
- Website
 - Highland Local Schools Technology Governance Guidelines

Ten Step Approach

7
SHARE & TRAIN
EDUCATORS
AND STAFF

What should they know
about **privacy**?
What do they need to know
about new **LEA protocols**?

SUBJECT: DCS Digital Resource Approval Process

Over the last 18 months, many staff members have utilized new digital resources with their students in order to teach in remote and blended learning environments. As we come out of the pandemic and are trying to wrap our arms around all of the resources teachers have found, we have discovered several websites, companies, and educational entities that have data privacy policies that do not meet appropriate standards and can put our students' and teachers' personal identifiable information at risk.

Right now, we are not going to pull the plug on all of these existing resources. Any new digital resource moving forward that teachers or principals wish to use in our district that requires the creation of student accounts will need to go through the DCS Digital Resource Approval Process. This process will allow us to look closely at the data privacy policies of the companies providing those resources so that we can ensure our student and teacher data is not being used for other purposes. Most "free" resources that companies make available are not truly free. There are various ways the company makes money off of the "free" educational sites they provide educators. We are instituting this guideline to protect both you, as the teacher, and your students so that personal identifiable information is not put at risk.

We will start taking a closer look at the digital resources that are currently being used across the district later this school year so that by the beginning of the 2022-23 school year every resource will be evaluated using the (LINK TO EVALUATION RUBRIC)

8

FIND WHAT
OTHER DISTRICTS
ARE USING

Search the **Student Privacy
Registry** to see apps being
used by **OH** districts or
districts around the **country**.

Ways To See What Others Are Using

- Use SDPC Registry as a “feel good/bad guide”
 - <https://sdpc.a4l.org/>
- Collaborate with other district during area tech meetings
- Joining CoSN TLE committee
 - [Ohio CoSN TLE Committee Focus Areas for ‘23-’24](#)
- Be active in state listservs
 - How to join Tech Leader Listserve ([groups.io](#)): send a blank email to ohio12edtech+subscribe@groups.io

8

FIND WHAT
OTHER DISTRICTS
ARE USING

Search the **Student Privacy
Registry** to see apps being
used by **OH** districts or
districts around the **country**.

Ways To See What Others Are Using

- Use SDPC Registry as a “feel good/bad guide”
 - <https://sdpc.a4l.org/>
- Collaborate with other district during area tech meetings
- Joining CoSN TLE committee
 - [Ohio CoSN TLE Committee Focus Areas for ‘23-’24](#)
- Be active in state listservs

Suggestions & Sample Communications Template Letter To Vendor

9 CONTACT
PROVIDERS TO
SIGN PRIVACY
AGREEMENTS

Download the NDPA for each vendor. **Piggyback** off other district agreements with and Exhibit E addendum.

Subject: Ohio Data Privacy Agreement

Vendor Contact,

Our district is working in collaboration with the Learn21 Ohio Alliance of SDPC (Student Data Privacy Consortium) - <https://privacy.a4l.org/> Our goal is to implement a common Ohio DPA (data privacy agreement-see attached) for all Ohio districts and those vendors that provide solutions to Ohio schools.

Attached you will find the Ohio DPA that our district would like you to review, sign and return. The Ohio DPA is adopted from the National DPA developed in conjunction with SDPC and 31 states alliances. (OPTIONAL) I have also attached a copy of the DPA that you signed for _____ school district, for your reference.

Your platform easily allows for the collaboration and creation of digital assets, which bridges the gap between learning and technology. Please partner with me and other districts in the state of Ohio by signing the attached Ohio Data Privacy Agreement and Exhibit E addendum (which provides efficiency for your other Ohio schools). By doing so, you will join the ever growing list of vendors, not just in Ohio, but nationwide, that are working together to keep our student data safe.

In addition, if your organization is not an SDPC Member/Partner, I encourage you to be part of the work by joining SDPC - <https://privacy.a4l.org/members-partners/>

Looking forward to partnering with you,

Suggestions & Sample Communications Working With Challenging Vendors

9 CONTACT
PROVIDERS TO
SIGN PRIVACY
AGREEMENTS

Download the NDPA for each vendor. Piggyback off other district agreements with and Exhibit E addendum.

- Could you add a description of your product and all the resources that this DPA will cover in Exhibit A?
- I have a question about one of the data elements that you have selected, can you tell me more about this. What do you mean by other? Can we talk more about this? (Exhibit B)
- I see you didn't check the box for Exhibit E. Does this mean you only would like to go into agreement with my district?
- Do you follow a cybersecurity framework? (Exhibit F)
- I don't agree with the changes you have made to the DPA, can we schedule a meeting to discuss this? (Exhibit H)



Messages to Families and Community Regarding Data Privacy Practices and Approved Resources

- Data Privacy Practices
 - District Website
 - Link to Sample Letters to Families
- Communicating Approved Resources
 - District Website
 - Application/website usage monitoring software public facing site
 - SDPC public facing page



Bill Fritz, Learn21

wfritz@learn21.org

Twitter - @williamdfritz



<http://bit.ly/SDPC2023-Chicago>

