



Student Data Privacy Consortium

CONNECTING & SECURING EFFECTIVE LEARNING ECOSYSTEMS™

**The Securing Continuum: From Legislation to
Ecosystem Implementation and All Steps In-
Between.**

AGENDA

WEDNESDAY,
FEBRUARY 17, 2021

- Welcome and Introductions
- The “Top Down” View of Student Privacy Protection
- The “On The Ground” Realities on Student Privacy Protection
- Q and A
- Resources

Our Hosts

Tyler Park

Policy Counsel

Future of Privacy Forum

Fun Fact:

Jim Newton

Manager of Application Development

Beaverton School District, OR

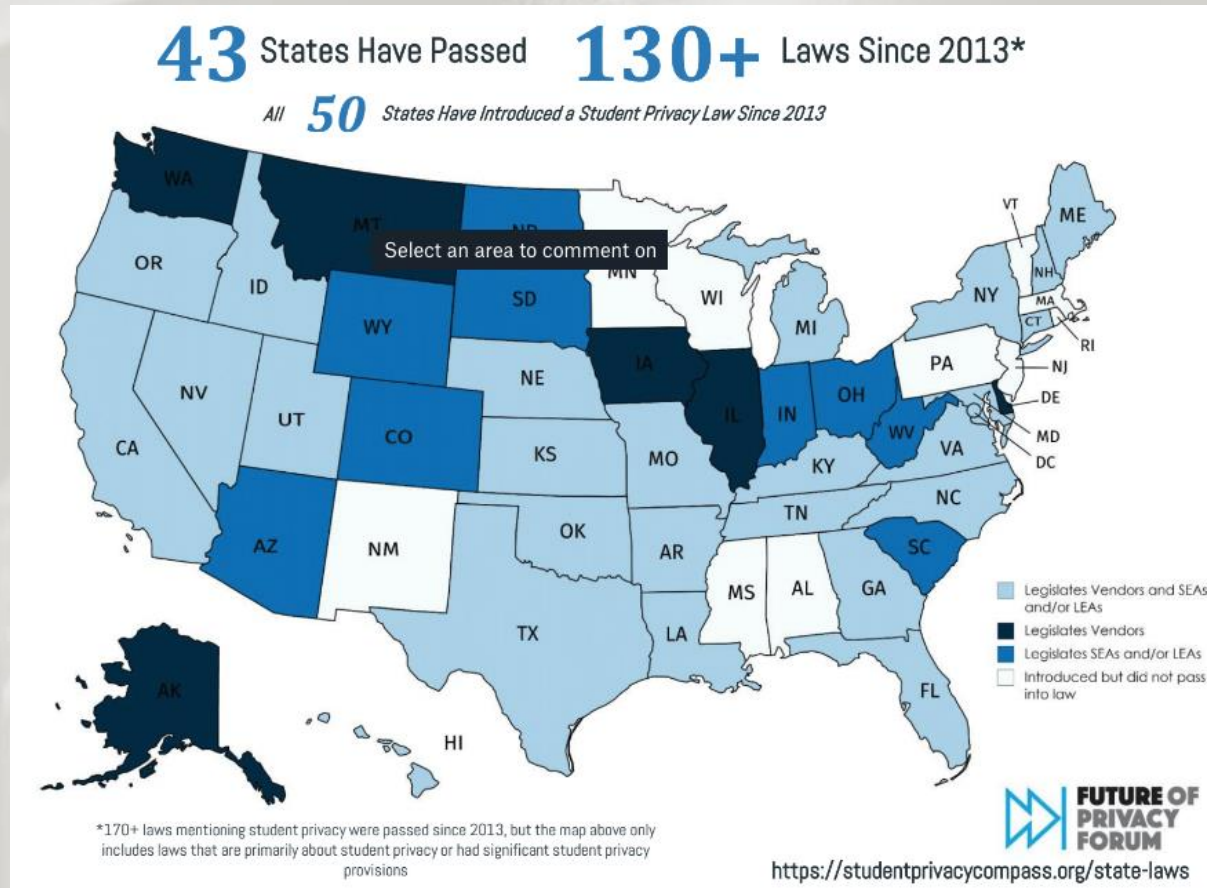
Fun Fact:

The “Top Down” View of Student Privacy Protection

Student Privacy Laws

- US Laws tend to be reactionary
- Existing Federal Laws
- State Level Rules...

The “Top Down” View of Student Privacy Protection



The “Top Down” View of Student Privacy Protection

- What to watch for:
 - Unintended Consequences
 - Connecticut Transparency Requirements
 - New Hampshire Video Prohibition
 - Louisiana Criminal Penalties
 - CCPA & Education
 - Mandates
 - NY Security Requirements
 - Contractual Requirements
 - Funded or Unfunded?

The “Top Down” View of Student Privacy Protection

- What comes next...
 - Policymakers’ first priority is reopening schools safely
- Other topics:
 - FERPA changes?
 - COPPA Rulemaking?
 - State Legislation Addressing:
 - Restrictions on EdTech
 - School Safety
 - Biometrics
 - COVID Data Collection
 - Children’s Privacy

The “On The Ground” Realities on Student Privacy Protection

- Beaverton - ~40k students, 54 schools, next to Portland
- Does anyone really care about privacy?
 - *As App Dev Mgr...rostering nightmare; hundreds of apps*
 - *Standardized upload process; SFTP, no custom data uploads*
 - *No app vetting process...“as you wish”...even teachers rostered!!*
- Nobody has any time for doing this correctly
- ~ 4 years ago I think it was Steve/Larry @ CoSN
 - *First learned about SDPC*
 - *CoSN Trusted Learning Environment*
- Attended first 2 SDPC conferences after CoSN

The “On The Ground” Realities on Student Privacy Protection

- Going All In
 - Getting BSD IT Management & T&L to “buy in”
 - Partnership, partnership...not just an IT thing
 - Committed to SDPC and got Oregon/Washington/ACPE to get on board
 - Two original DPA's (v1 & v2) for Oregon
 - NDPA
 - Participate on a couple national DDPC committees

The “On The Ground” Realities on Student Privacy Protection

Beaverton School District: Intranet **Department** ▼ School ▼ School School Department School



New Software Request



Beaverton School District privacy and data policies . . .

. . . ensure that the District is ethically and legally protecting student safety and student information, including student work. Protecting students from harm--identity theft, harassment, and unauthorized data collection-- are critical concerns. As an educator, it is our job to ensure our students are protected in this manner.

In today's world of advancing online resources teachers, students, and parents are benefiting from an ever increasing wealth of tools to support teaching and learning. The growth in these tools is extraordinary with great potential to improve student outcomes. Along with this explosion in growth of online learning tools, comes the inherent risks of leakage of student data and understandable concerns over student privacy.

Any online resource that students are interacting with and/or producing content on, including, but not limited to, any site requiring a student account/login, needs to be reviewed and approved.



NEW SOFTWARE REQUEST

1. See if the resource is already approved. Check the [List](#).
2. Not on the list? Complete a [Helpdesk Ticket](#).
3. You will be notified via the Helpdesk system of the status of your request. (Anticipated turn-around time is 4-6 weeks).



Have more questions? Checkout the [Data Privacy FAQs](#).

Have questions or need assistance? Contact the Helpdesk at x64300 or by [email](#).

The “On The Ground” Realities on Student Privacy Protection

Helpdesk Ticket - IT>Applications and Software>Application Request for Review

Help Request

Request Type: IT
Applications and Software
Application Request for Review

Subject:

Instructions: This ticket is for requesting an application for use by students or staff, to be reviewed by the BSD Software Review Committee. To speed up the review process, please complete this ticket with as much information as possible.

Name of Application*

Link to the Application's Product Page*

Name of Company*

Name of Company Sales Contact

Email Address of Company Sales Contact

Who will be using this Application* Staff Only

How do you plan to use this Application for Instruction?*

What Instructional Content Areas does this Application Cover? (Check all that apply)*

- ☐ Math
- ☐ Science
- ☐ Social Science
- ☐ English Language Arts
- ☐ World Language
- ☐ Health
- ☐ Physical Education
- ☐ Instructional Technology
- ☐ Computer Science
- ☐ Visual Performing Arts
- ☐ Library Media
- ☐ CTE
- ☐ Other

What Grade Levels does this Application Cover? (Check all that apply)*

- ☐ Pre-K
- ☐ K
- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5
- ☐ 6
- ☐ 7
- ☐ 8
- ☐ 9
- ☐ 10
- ☐ 11
- ☐ 12

What are the Unique Features of this Application when Compared to Other Similar Products?*

What Devices do you intend to use this Application with? (Check all that Apply)*

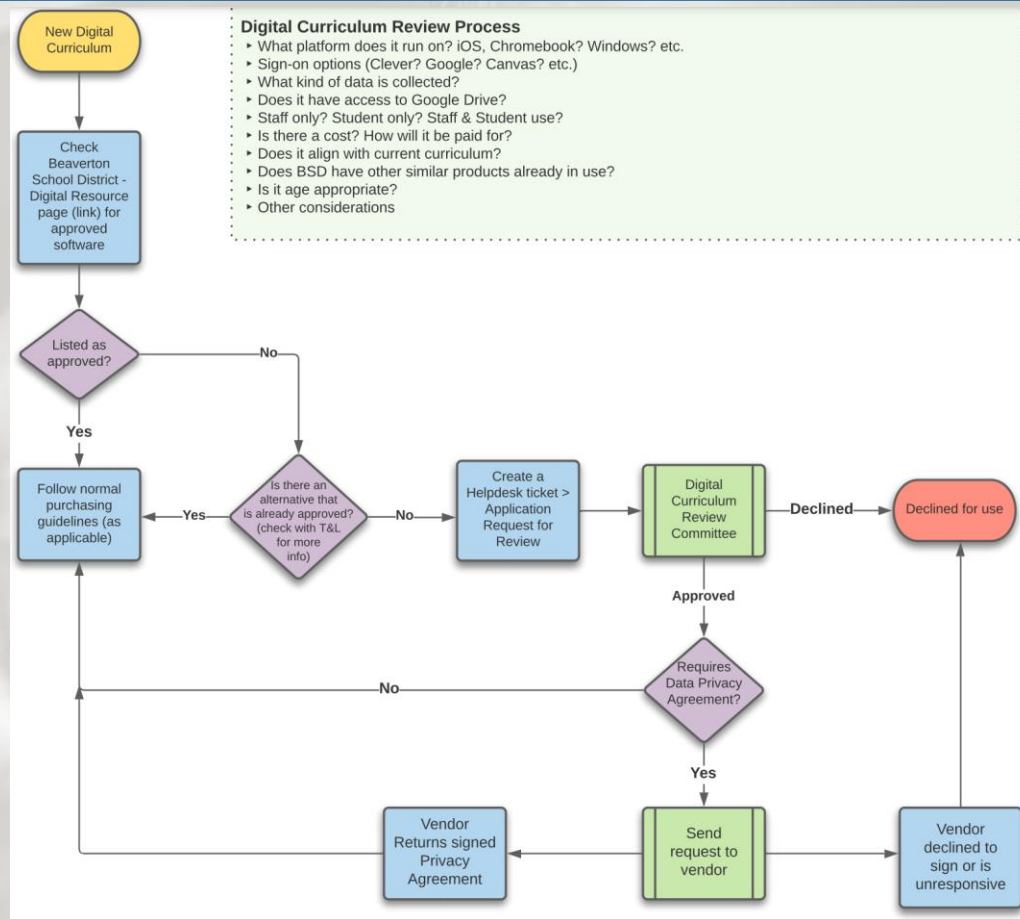
- ☐ Chromebook
- ☐ iOS
- ☐ Mac
- ☐ Windows

How will this Application be Paid for?* It is Free

Any additional information that the Software Review Committee should be aware of?

Attachments [Add File](#)

The “On The Ground” Realities on Student Privacy Protection



The “On The Ground” Realities on Student Privacy Protection



Student Data Privacy FAQ



What is the approval process? Check it out.

What constitutes student data? 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.

What are some of the potential consequences of not being aware of student privacy protections when using a digital tool? Use of a digital tool that has not been vetted presents the opportunity for student level data to be inappropriately exposed, shared, or in some cases sold.

Why can't I just make fake names for student accounts? A made up username or ID is simply another student identifier. It does not change the fact that the online digital tool may be collecting student level data and work that needs to be protected.

If a website or app doesn't ask for a student's name, can I use it? All applications should be properly vetted to ensure any student level data collected is properly protected.

Many online applications say "Sign In with Google." Aren't those OK to use since our students have CPS Google accounts? No, these applications also need to be vetted. Using a BSD Google Login does not ensure that the data remains in the BSD Google Domain.

How can we get more companies on board? In other words, what can teachers do to explain the importance of this and why companies should care? Refer the companies to the [Student Data Privacy Consortium](#), who's goal is to engage vendors on this topic.

Why do we need to get approval to use some resources? In order to ensure all student level data is properly protected all online applications need to be properly vetted by the IT department. In addition, Teaching and Learning checks to make sure the software/app is in alignment with current curriculum.

What kinds of resources do I need to get approval for? Any resource that a student interacts with needs to be approved. Ideally, we desire a seamless student experience with products that are integrated into the systems we use such as Clever, Google, etc. We want to activate single sign on authentication whenever possible.

How do I know if a resource has already be approved to be used? All Approved resources can be found [here](#).

Are there any other schools/districts using an approval process? Yes, this process is being replicated in over 25 states and thousands of school districts.

The “On The Ground” Realities on Student Privacy Protection

Am I able to use the application while waiting for approval? No.

What do I do if a resource I requested declines to sign our privacy agreement? Teaching and Learning will help you seek out an alternative application that meets your needs and adequately protects student data privacy.

Why does it take so long to get a data breach agreement signed sometimes? There are many reasons that might drag out the process. These may include;

- The Vendor business model - especially for free applications - leverages the re-use of student level data for profit.
- Vendor has no legal resources to review document
- Vendor refuses to consider separate agreement
- The resource has flaws that expose student level data

What if I've already been using the resource with students and didn't know it wasn't approved? Contact Teaching and Learning and they will assist.

What if I've paid for the resource? Same process applies for teacher paid resources, District paid, or free resources.

If a student wants to use an unapproved resource for an individual project (when students are allowed to choose how they present their work, for instance), and the parent approves, is that okay? In other words, if I'm not requiring or encouraging the resource's use, can a student choose to use it on school equipment? Not without written parental consent.

Legal - What laws dictate how schools and teachers handle student data?

- [FERPA – The Family Educational Rights and Privacy Act](#)

FERPA requires that schools have written permission from the parent or guardian in order to release any information from a student's education record. So the most important thing is that, with some very specific exceptions, you shouldn't be sharing student information with apps and websites without parent permission.

- [COPPA – The Children's Online Privacy Protection Act](#)

COPPA puts special restrictions on software companies about the information they can collect about students under 13. So, students under 13 can't make their own accounts, teachers have to make the accounts for them. In making the accounts, teachers need to be aware of their responsibility under FERPA.

- [CIPA – The Children's Internet Protection Act](#)

Teachers don't need to help comply with CIPA, but it's useful to know that it is in place. CIPA requires districts to put measures in place to filter Internet access and other measures to protect students.

- [PPRA – Protection of Pupil Rights Amendment](#)

PPRA governs the administration to students of any survey, analysis, or evaluation that concerns one or more of eight designated protected areas.

- [SDTSA – Colorado Student Data Transparency and Security Act \(HB 16-1423\)](#)

SDTSA puts additional restrictions on how school districts can share student data with third party service providers. The three primary focus areas of the law are:

1. Data Use Obligations and Restrictions
2. Data Transparency
3. Data Security & Destruction



Q and A Time

"On the Ground" Reality Checks?

Resources

- [Tyler Park](#)

<https://studentprivacycompass.org/>

<https://studentprivacycompass.org/state-laws>



- [Jim Newton](#)

<https://www.beaverton.k12.or.us/departments/information-technology/digital-resources>



Don't miss...

REGISTER:

<https://bit.ly/3oJmd4P>

FEBRUARY 24, 2021

Connecting and Securing in the Real World: The MA Data Hub Solution

This pilot project was designed to leverage the MA Department of Elementary and Secondary Education's (DESE) state data collection & Cedar Labs' "hub and spoke" architecture to branch a state reporting data connection and create an easy-to-manage data integration platform for school districts. MA DESE, and Cambridge Public Schools are leveraging the existing state data connection to branch the flow of data not just for state reporting, but to also provide additional value add services such as standards agnostic rostering and privacy enforcement.

Don't miss...

REGISTER:

<http://bit.ly/3pLLi4L>

FEBRUARY 23, 2021

All the talk now is about 'Unity'... is it time to do something about Data Privacy and Data Interoperability 'Unity'?

The Student Data Privacy Consortium (SDPC) has been moving the needle on setting privacy expectations between School Districts, States and marketplace providers. The strength of the collective power of the Community and the best practice leadership shown in protecting student data through Data Privacy Agreements (DPAs) is the reason for this success.

It's a GREAT first step but collectively we could do more in protecting your local learning ecosystem:

- *How are your vendors implementing the privacy requirements?*
- *How do you convey legal requirements to the vendors' technical teams?*
- *How does increased data interoperability without embedded privacy created increased risk?*
- *Is there a way I can address and enforce privacy requirements through openly developed technical standards?*



Student Data Privacy Consortium

Thank you for attending!

Presentations slides and follow-up
information will be sent to you
shortly...

For more information:

<https://www.A4L.org>

<https://privacy.A4L.org>