Visioning Session; Connected & Secured Effective Learning Ecosystems
Introductions

**Steve Smith**  
CIO Cambridge Public Schools & Co-Founder  
Student Data Privacy Consortium

**Ben Silberglitt**  
Founder and Chief Strategy Officer  
Cedar Labs, LLC
Introductions

WHO is in the Audience?
Why are we talking about this?

Rapid explosion of unmanaged or vetted educational technology tools causes both inefficiencies in management as well as increased risk to students by using un-vetted applications. At the same time, caregiver and student concerns about privacy are continuing to increase.
What does it mean to you to have a “connected and secure” learning ecosystem?

What do you do in your current role, to securely connect data across systems?

What are yours or your constituents’ biggest obstacles to establishing and maintaining a connected and secure learning ecosystem?

Let’s talk!
Connected & Secure Effective Learning Ecosystem: Key Components

- Application vetting
- Centralized data interoperability
- Data privacy enforcement
- Professional development
The explosion of online learning and technology in K12 has increased the risk to student's privacy. The expansion of the use of K12 apps, along with limited resources of school districts, exponentially increases the potential of the gathering and misuse of student level data.
EDTech in Schools

• **Explosion** of technology in schools
• Most districts have some sort of 1:1 program
• Chromebooks now in 70% of U.S. schools
• 2018 EdTech market in the U.S worth over **$8.38B**
• The average U.S. school employs **400 to 1000** online tools/apps (whether then know it or not)
InBloom = Privacy Explosion in USA
40 States Have Passed 125 Laws Since 2013

*Courtesy Future of Privacy Forum*
Application Vetting

- In order to solidify the culture shift in a district there must be an effective application vetting process.

- Vetting may take into consideration at least 3 aspects;
  - Curricular alignment
  - Technical support or data integration needs
  - Privacy

- Privacy vetting
  - Years ago meant reading TOS & PP
  - Now the market has shifted towards standard Data Privacy Agreements
Centralized Data Interoperability

Problem Statement

If you want to protect & connect your data, you need to know where it is.
Centralized Data Interoperability

How can we make sure each system only gets the data it needs, when it needs it, transported securely, in the format it requires?

What are the barriers to centralized data interoperability, for districts / vendors / states?
A New Approach

The MA DataHub:
Real-time statewide data integration and privacy management for SEAs and Districts
Data Privacy Enforcement

Problem Statement

Increased interoperability without privacy controls results in increased risk to students’ privacy.
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

- You pick the technical security standard

Privacy Obligation Document (POD)

- Obligation 1 XML
- Obligation 2 XML

Technical

Vendor (Data Processor)

The legalese from the DPA

The technical obligation from the legalese

A machine-readable document for detailed obligations
Unity Enabling Privacy Expectations

Automate Contract Clause Expectations Exchange and Vendor Verification

The “POD” (Privacy Object Document)
Data Privacy Enforcement

Discussion

How might the POD be valuable to you as a district / vendor / state?

What role do they play in protecting education data in the future?

What barriers are there to POD adoption?
What's needed is a connected, secure, and effective learning ecosystem.
Even with the best designed technical solutions to automate and secure digital platforms, if users are not properly informed there are always shortcuts. Teachers are ethically obligated to follow and model good digital citizenship practices and behaviors with their students. This includes thinking carefully about the digital products and processes that are incorporated in any project or lesson design.
Professional Development

Discussion

How are you addressing Professional Development in your systems?

How could SDPC assist you?
Professional Development

Strategies for changing the culture in a district

- Privacy Embedded in PD
- Privacy awareness supported at the classroom level
- Tools to enable staff to select from a list of approved apps and then request a new app
- Quick turn around for approval process
- Assuring staff that they do not want to take on burden of vetting apps for privacy “We have your back”
Introducing.....
Global Education Security Standard

The goal of this new working group would be to identify and document a security framework that could become the **Global Education Security Standard (GESS)**.

Participants
Vendors and Education Agencies representing

1. Establish an international working group consisting of education technology professionals and vendors with expertise in security, privacy and safety matters.
2. Leverage existing member work such as **AU’s ST4S Framework**
3. Invite external (non-SDPC) security experts to participate in the working group.
4. Identify and select a relevant security framework that is globally recognised and is suitable for K-12 education needs (eg NIST Cybersecurity Framework - [https://www.nist.gov/cyberframework](https://www.nist.gov/cyberframework)).
5. Work through the selected framework to determine which aspects would be suitable for an education technology vendor supplying products to schools, school districts, state and federal authorities.