PRIVACY, SECURITY, AND INTEROPERABILITY CONVENING

DECEMBER 6TH 2018 • NEW YORK, NY

READ-OUTS

Major takeaways, lessons, and insights from the day

Olga Garcia-Kaplan - NJ Parent, FERPA | SHERPA Blogger

Interoperability can be an intimidating word. It certainly is if one doesn't work in technology and it most certainly is if one is a parent of children whose data is captured in their schools.

Interoperability is the ability of different technology systems and software to communicate and exchange data in a controlled environment and use the information that has been exchanged. Privacy and security concerns are front and center when discussing student data, and Project Unicorn's convening aimed at tackling the challenges posed by capturing student data and using that data through different systems to benefit all students in a secure and private environment.

The day was packed with panels that covered a wide range of topics addressing the edtech field, vendor and district stories, federal and state laws, and public and parent perspectives. I am encouraged by how the conversation has matured in the past few years. There are still challenges when it comes to student data, but the conversation was centered on how to properly secure and maintain student data privacy. How do we leverage data to serve all students, but also how do we ensure that information is protected as it moves through different systems? We have moved from looking at collecting all the data we can to thinking about only collecting what is necessary to serve that student.

We get smarter when we listen to a diverse group of people who agree and disagree with us. The day was filled with differing viewpoints, however, everyone was focused on ensuring the security and privacy of student data. The conversation has evolved and we are facing a number of challenges in maintaining student data privacy. I walked away with an understanding that the ultimate goal of interoperability is to maximize the student data we have and use it to the greater benefit of both an individual and a group of students. What can interoperability solve? It can help students become better learners - but we still need to look at how can interoperability benefit all students. We need to give students the ability to utilize their information to their advantage as they map their educational journeys. And let's not forget that at the end of all this work, there is a student. That is what matters most.

Sara Kloek - Director of Education Policy, SIIA

The gathering hosted by Project Unicorn and Future of Privacy Forum highlighted many important topics but my biggest takeaway from the event is that there isn't a quick and easy "fix". Districts and vendors, as well as parents, students, and other stakeholders, will need to be partners to identify approaches that work. There isn't just one approach and there isn't just one fix. Identifying best practices and practicing radical transparency will be key to finding success in improving student learning.

Susan Bearden - Chief Innovation Officer, CoSN

Keeping Education Data Secure in an Interoperable World [Privacy, Security, and Interoperability Convening], an event hosted by Project Unicorn and the Future of Privacy Forum, brought together a diverse group of education stakeholders to discuss the intersection of student data privacy and edtech interoperability.

As panelists Bill Fitzgerald and Michael Hawes both noted during their respective panels, privacy and edtech use are often viewed as binary, black and white choices. You can use technology, but not have data privacy, goes the narrative. IT systems are either 100% safe, or riddled with risk. The reality of edtech, interoperability, and student data privacy, however, is far more nuanced.

Much of IT management is about managing risks and benefits. A heavy-handed approach to web filtering might block objectionable content, but prevent access to educationally valuable websites. Active Directory policies that force teacher machines to lock automatically after 10 minutes of inactivity are more secure, but potentially interfere with classroom instruction. An updated firewall appliance might better protect a network against threats, but at significant financial cost. In every case, IT leaders must do a cost and risk/benefit analysis to determine the best solution for a given environment. Often, the risks posed by a particular solution can be addressed and/or mitigated. A robust digital citizenship education program will help protect students from online dangers; cybersecurity training and awareness can reduce the risks posed by extending the time before a computer locks. The key to successful education IT management is to thoughtfully mitigate risks while maximizing benefits and evaluating cost.

As with anything else, edtech interoperability presents many benefits, reduces some risks, and may introduce others. Educational and cost benefits aside, interoperability has the potential to lower the risk of user error, which is a significant cause of data breaches and erodes data integrity. When data is stored in multiple systems that require different usernames and passwords, users are more likely to store login credentials insecurely - the "passwords written on sticky notes" syndrome. In addition, the manual import and export of user data into .csv files or excel spreadsheets increases the likelihood of confidential student data being sent via email or stored in insecure locations. However, if an interoperable system is compromised or if user access is not carefully controlled, more data can potentially be exposed in a single breach.

The key to leveraging the benefits of edtech interoperability is, like in other areas of education IT, is to identify the risks and implement strategies to mitigate them. Careful evaluation of edtech vendor privacy policies and thoughtful district-vendor contracts that specify data storage security requirements can help protect the privacy of student data. Robust data management policies and procedures - including regular user audits - can reduce the risk of unauthorized access to interoperable systems. Quality user training can reduce the risk of data breaches caused by human error. A thoughtful, carefully considered approach to cybersecurity and student data privacy can help school systems maximize the benefits of interoperability while minimizing the potential risks of digital data systems.

Risk mitigation is a strategy we implement on a daily basis, even if we don't realize it. We may not consciously consider the risks that come with driving on a daily basis, but wear seatbelts and drive cars with airbags to mitigate the risk of a car accident. We cross busy streets, but use the crosswalk and look both ways before we start walking. Thoughtful risk mitigations strategies can change the conversation from "either/or" to "and," enabling educators to leverage the benefits of edtech interoperability while also protecting student privacy.