Student Privacy and COVID-19

Making Sure It Is Not 'Too Good To Be True…'

Access 4 Learning Community
Student Data Privacy Consortium

The COVID-19 pandemic has changed the way that we educate kids by shifting their majority 'brick and mortar' setting to an online delivery model. This shift has put huge new demands on school personnel, parents, technology providers and the learners themselves. Even before the outbreak, schools have been challenged managing hundreds of software applications in their 'bricks and mortar' digital ecosystem.

The new reality is that we are all trying to find our way – in an expedited manner – to get these and the additional proliferation of online educational tools in the hands of practitioners and their students to ensure learning continues until we come through this global challenge. A great influx of marketplace providers, and their professional organizations, have increased their communications around the value of their tools and even free or limited-time free usage of them during this crisis. While admirable, this only has added complexity to the management of these tools at the district and even school level.

While the way we are educating our youngest citizens has changed dramatically, the rules, regulations, legal accountability and expectations schools have around protecting student data privacy has not. The *Family Educational Rights and Privacy Act* (FERPA), established in 1974, is still the guiding document for schools (not vendors) in their role as data stewards. Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. FERPA does allow schools to disclose those records under certain exceptions, such as the "School Official Exception". This exception requires Data Privacy Agreements that establish control over the vendor. For marketplace providers, the *Children's' Online Privacy & Protection Act* (COPPA) imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online.

Even before this crisis, the *"what should we be doing about student privacy?"* mantra was heard coming from more and more learning institutions, parents and even the learners themselves. Numerous

organizations are collaborating to try to help school data stewards to perform their roles by providing tools, guidance and effective practice sharing around a topic they are not fully armed to address on their own due to limited legal, fiscal or human resources. What is true at present is short term "pain point" software solutions being provided now that can open up long term privacy issues including possible legal action against users.

Schools and organizations with mature models of vetting, adopting, and supporting tools with privacy in mind are finding this transition slightly less stressful. Having a full toolbox of approved applications that meet privacy requirements in the new distance learning environments, gives these schools a leg up. The majority of districts though are not in this category. Without a well-developed process of onboarding applications that many schools are struggling with, balancing distance learning needs with privacy requirements is often a task best left alone.

The **Student Data Privacy Consortium (SDPC)** is a global collaborative of schools, state and federal agencies and marketplace providers all working towards setting clear expectations between end users and vendors regarding "on the ground" student data privacy. Over 10,000 school districts and vendors representing over 7,000 school applications have collaborated to sign more than 64,000 privacy agreements clarifying each other's role in the protection of our youngest citizen's data.

The SDPC Community has some resources that can provide some quick help – here are two great ones:

- **Privacy 101 and Your Responsibility:** So, who is responsible for the what, why, and where about student data privacy? Let this walk through from the SDPC show you the how!
- **SDPC Resource Registry:** Interested in seeing where over 7,000 apps are being used, where they are being used and their signed agreements between vendors and schools? Here is the free Resource Registry helping schools manage their digital tools and set common privacy expectations with vendors.

The SDPC is also made up of numerous partner organizations that are trying to help address student privacy concerns related to the exponential growth of applications being used by learners. This is all in the attempt to not "reinvent the wheel". Here are a couple of ones to check out first:

Legal Resource Links:

Student Privacy During the COVID-19 Pandemic: The Future of Privacy Forum (FPF) and AASA: The School Superintendents Association (AASA) has released white paper offering guidance to help K-12 and higher education administrators and educators protect student privacy during the COVID-19 pandemic.

FERPA and Corona Virus Disease 2019: US Department of Education's guidance to assist school officials in protecting student privacy in the context of COVID-19 as they consider the disclosure of personally identifiable information (PII) from student education records to individuals and entities who may not already have access to that information aligned to the Family Educational Rights and Privacy Act (FERPA)

Copyright © Access 4 Learning Community

FERPA and Virtual Learning Related Resources: The US Department of Education's one-page guidance on virtual learning and federal student data privacy law.

Marketplace Providers Resources Links:

Learning Keeps Going: The COVID-19 Education Coalition is a diverse group of education organizations brought together by the ISTE/EdSurge team to curate, create and deliver high-quality tools, resources and support for educators and parents as they keep the learning going during extended school closures.

The key to address many of the concerns is *ongoing and clear communications between parents/educators and school CIO/CTOs in what applications and services are safe for learners* – and which need to become more aware of the importance of student data privacy. The SDPC is here to help. Please reach out to see how your district, state agency or provider organization can get involved and work together as a global educational technology marketplace to address these issues together.

The Student Data Privacy Consortium (SDPC) is a Special Interest Group (SIG) of the Access 4 Learning (A4L) Community. It is designed to address the day-to-day, real-world multi-faceted issues that schools, states, territories and vendors face when protecting learner information. SDPC's vision is to develop common activities, artifacts, templates, tools and effective practices that can be leveraged through a unique collaborative of end users and marketplace providers working together. For further information, visit https://privacy.A4L.org