Troxell

Troxell Communicator

Protecting Student Data in an Increasingly Digitized World

You can debate the merits of technology usage in the classroom all you want, but the reality is that it's here to stay. Today's educators are seeking out digital tools and continue to create innovative lesson plans that involve new gadgets like virtual reality and wearables for students and new tools like advanced analytics for teachers. These approaches have great educational merit, allowing students to better engage with subject matter and become more in-tune to technologies they'll eventually see in the workplace.

It's not just changing for students, though—as an educator, you have additional responsibilities as your classroom becomes more plugged in. Besides teaching your students to be good digital citizens—an absolute necessity, especially in the age of increased cyberbullying—you must also consider the data your students are generating and how to best protect it. **After all, data collection in schools could be a double-edged sword and could put students at risk for breaches if not handled properly. Here's what you can do about that.**

Student Data Protection Best Practices

Schools now have the ability to collect data from students including personal information, educational information, and health information. While this information has been helpful to educators and administrators, it can also put students at risk for security breaches. Here are some best practices for you to use as you work to protect your students' data:

Be transparent in what types of data are being collected. Make sure families of students have access to any type of data you're collecting. Not only that, but full transparency means sharing with them how the data about their child(ren) will be used and precisely who else has access to it. McKinsey & Company recently reported on President Obama's Student Digital Privacy Act, aimed at addressing concerns about student data being sold to third parties.

Ensure programs being used aren't profiling from student data collection. Sometimes, there's so much data generated and collected by users and programs that it's hard to keep track. If your school is starting from scratch, consider generating a 'data calendar' or hiring out a thorough audit to ensure programs aren't profiling from the data being collected.

Establish security protocols and make sure all administrators and fellow educators understand it. As a teacher, this might not be your job—but it *is* your job to say something if it's not getting taken care of by a chief technology officer, system administrator, or even a team of different stakeholders. (Note that Harvard Graduate School of Education reported that several entities—the U.S. Department of Education, New York State, and Denver Public Schools all created a "chief privacy officer" position.) Security protocols should make sense, and you should be able to implement the techniques easily.

Encrypt devices being used in classrooms. Many schools protect exterior data transmission via a commonly used firewall, but data stored on computers can fall by the wayside. This is where encryption comes in. All data—even 'data at rest,' according to EdSurge—should be secured. You should enlist the help of the system administrator (or chief privacy officer, as mentioned above) to approach encryption.

Educate students on cybercrime and how to safely interact with technology. You spend a great deal of time teaching students how to use technology, but you should also teach them how NOT to use it when it comes to giving out personal information. Educate your students about the risk of cybercrime and encourage them to avoid sharing personal data—even when logging in to common sites—without the permission of an adult. For older students, instruct them to actually review privacy policies, not just click 'accept.'

What's Next?

As an educator, you have the unique opportunity to help shape your students' relationships with technology. By opening their young eyes to the digital world early, you can enrich their educational experience and help them better connect with coursework. It's imperative, though, that you take steps to protect their data in this digital world. By exhibiting data transparency, establishing security protocol, encrypting devices, and educating students on cybercrime, you can do just that.