This resource sponsored
by Clarity Innovations

K-12 BLUEPRINT

A planning resource for personalizing learning

Privacy in the Age of No Privacy

toolkits

The education sector has never been more vigilant regarding the practice of student data privacy.

It's a double-edged sword: The No Child Left Behind Act of 2001 required teachers to better utilize student data in order to create more targeted lessons with the intent of improving academic performance. But to accomplish this amidst dwindling education budgets meant reaching out to education technology companies to store, handle, and protect an ever-growing collection of sensitive student data to enable personalized learning. Even Facebook CEO Mark Zuckerberg declared that privacy was no longer the social norm back in 2010[1]. While this is true in some respect (never have we been more willing as a society to blithely trade privacy for convenience), the education sector has never been more vigilant regarding the practice of student data privacy.

And the stakes are high: *The Wall Street* Journal reported that for nine out of 20 websites that collected sensitive data, including medical, personal relationship, or children's data, potentially identifying information was shared.[2]

Of particular concern is the issue of data theft. A child's Social Security number is a boon for identity thieves, so much so that children are 35 times more likely to fall victim to ID theft than adults.[3]

An Education on Security in Schools

According to Jim Shelton, acting deputy secretary of the U.S. Department of Education, privacy begins with outlining the rights and protections every child should have, and supporting that with a comprehensive, evolving regulatory framework.

"But there is a huge variance in how districts are protecting themselves and their students, which is in some ways completely understandable given the differences in their size and capacity, so that means we need federal and state regulatory frameworks that help close those gaps while also maintaining a healthy environment for new more effective solutions. This challenge is not unique, but it is pressing because our children's safety is at stake. That said, we also don't want unwarranted panic to result in bad legislation or regulation that robs us of the opportunity for the potentially fantastic advancements ed-tech holds.

Let me add that in addition to our responsibility to create a robust regulatory framework to protect students, two other things are critical: (1) the ed-tech industry needs to adopt some ethical standards with regard to the uses of student data and student privacy; and (2) we need to educate students and families to understand their rights and how to protect them. These two groups will always be on the front line of whatever is new in the data space and their choices will always be most determinative of how safe our children actually are online—even in school"[4].

How to Protect Your Students

The integrity of your school's student data begins with a simple/not-so-simple question: what are your school's particular security needs? Gauging your school's overall technology and privacy needs is a formidable task, but a crucial one. What are your data security procedures? Do you utilize the services of vendors? If so, how do you assess their data collection and security practices? Internet security and online privacy for students requires digital literacy, a thorough knowledge of what technology is capable of (and, perhaps more importantly, *not* capable of), smart filtering, as well as the support and supervision of teachers and parents.

Some schools—due to size, expertise, or unique resources—choose to handle security themselves. This is fine if you *truly* have both the ability and the capacity to implement appropriate security protocols yourself. In addition to ensuring your school's needs and abilities, you must also make certain that your provider has appropriate security protocols in place. After all, the protection of invaluable student data is at stake.

Your school system must filter Internet access both on school grounds, but also when/if school-owned devices are taken home so that, by routing through the school's filter, inappropriate sites continue to be blocked wherever students use the devices. A school's Internet access provider can also lock screens or send students if inappropriate online behavior is detected.

In February 2014, the Software & Information Industry Association released five "best practices" for the handling of private student data:

- **Educational Purpose**: School service providers collect, use, or share student personally identifiable information (or PII) only for educational and related purposes
  for which they were engaged or directed by the educational institution, in accordance with applicable state and federal laws.

- **Transparency**: School service providers disclose in contracts and/or privacy policies what types of student PII are collected directly from students, and for what purposes this information is used or shared with third parties.

- **Authorization**: School service providers collect, use, or share student PII only in accordance with the provisions of their privacy policies and contracts with the educational institutions they serve, or with the consent of students or parents as authorized by law, or as otherwise directed by the educational institution or required by law.

- **Security**: School service providers have in place security policies and procedures reasonably designed to protect PII against risks such as unauthorized access or use, or unintended or inappropriate destruction, modification, or disclosure.

- **Data Breach Notification**: School service providers have in place reasonable policies and procedures in the case of actual data breaches, including procedures to both notify educational institutions, and as appropriate, to coordinate with educational institutions to support their notification of affected individuals, students, and families when there is a substantial risk of harm from the breach or a legal duty to provide notification[5].

Dealing with Outside Providers

The complexity of school data collection and the protection of student information is daunting. Luckily, there are a host of competent providers who can handle the many issues accompanying data aggregation and security. But which vendor is right for your school's needs?

First, you must establish your school's security standards for any provider who would store, process, transmit, or otherwise deal with your students' education records or PII. Online-service providers must reasonably maintain the security and confidentiality of a child's personal information, protecting against risks such as unauthorized access or use, or unintended or inappropriate destruction, modification, or disclosure. In case of data breaches, these providers must have policies and procedures that notify schools and support a school's notification of affected students.

Some questions to ask potential providers include:

- What data will be collected and how (and where) will it be stored?
- Does a third party collect any data?
- Are backups performed and tested regularly and stored off site?
- Are software vulnerabilities patched routinely or automatically on all servers?
- Will any data be stored outside the United States?
- Is all or some data at rest encrypted (e.g., just passwords, passwords and sensitive data, all data) and what encryption method is used?
- Who has access to information stored or processed by the provider?
- Does the provider subcontract any functions, such as analytics?
- What is the provider's policy for deleting collected information?

1 http://www.theguardian.com/technology/2010/jan/11/facebook-privacy

2 http://online.wsj.com/news/articles/SB10001424127887324784404578143144132736214

3 http://content.usatoday.com/communities/technologylive/post/2012/05/service-to-protect-kids-from-id-theft-launches/1

4 http://www.forbes.com/sites/jordanshapiro/2014/03/10/edtech-student-privacy-too-much-testing-qa-with-the-department-of-education

5 http://blogs.edweek.org/edweek/marketplacek12/2014/02/industry_group_issues_best_practices_on_privacy_for_ed-tech_companies.html