This resource sponsored
by Clarity Innovations

K-12 BLUEPRINT

A planning resource for personalizing learning

The Call for Response

toolkits

Student Privacy and Digital Compliance Strategies

Clive Humby, the Sheffield mathematician who helped multinational grocery retailer Tesco with its Clubcard system, famously referred to data as "the new oil" in 2006. And judging from the geyser of opportunity that data has given countless technology firms, his assertion rings true.

Yet with any type of oil—even the data kind—comes the sobering reality of possible oil spills and costly cleanup. And in no industry are these potential data spills as controversial as in education. In June 2014, the personal information of roughly 47,000 Florida State University student teachers in training was accidentally leaked during a data transfer[1]. In February 2014, the information of 146,000 Indiana University students and graduates may have been exposed after a data breach[2]. And in 2012 alone, more than 12% of all data breaches were in the education sector[3].

And while student privacy and digital compliance in education involves a learning curve, it's in the interest of educators, policymakers, the private sector, and parents to put the right policies and practices in motion as quickly as possible.

One particularly urgent aspect of student privacy is in the swift and thorough response to these "data spills" and other "data incidents."

A data incident is, basically, any school-related issue that comes up involving the use of digital technology. This issue could involve students, faculty, or both—either at school or off campus. Intervention and response is required if an incident adversely affects a student's safety and emotional well being, or if it interferes with their ability to achieve their academic best. Any behavior that strays outside of your school's Responsible Use Policy (RUP) if likely to classify as a data incident.

Some data incidents may require outside resources, such as lawyers or counselors, or—if involving unlawful behavior—police intervention, while others will be quickly resolved without the need for outside help.

Having a committee of multiple stakeholders well trained in handling data incidents can not only help increase the speed and success of response, but also eliminate many incidents before they ever happen. This committee should be abreast of privacy policies and protocols while monitoring ongoing compliance.

With privacy, a proactive offense is better than defense. A systematic approach to privacy that includes comprehensive policies, appropriate security protocols, safeguards, proper data deletion and disposal, oversight, and plans for how lost or stolen devices are dealt with will help schools prevent harmful and costly privacy issues. Contracting a third party to assess your school's privacy policies—locating risks and gaps, updating based on new technologies and laws, etc.—can help make your data privacy and security policies as strong as possible. This is especially useful as new technology, resources, and services are brought into the classroom.

All staff and faculty should be trained on privacy and data security so that your school can ensure compliance with policies. They should all take responsibility for security and be aware of best practices for dealing with passwords, data disposal, privacy violations and legal repercussions, policies around confiscation of electronic devices as well as malware, phishing, and other online threats. They should also be aware of how digital tools (such as apps and websites brought into the curriculum) could pose risks to data security and privacy. Third-party services should be carefully vetted based on your school's particular data privacy policies and obligations.

iKeepsafe's *Data Privacy and Schools: Outlining the Conversation*[4] poses important questions that school educators and administrators should ask themselves regarding their data privacy solutions, including the following:

- How can schools be equipped to assess privacy policies and practices of vendors that might house and have access to student data?
- How can stakeholders handle data around behavioral incidents, and should they treat that differently than academic or attendance data?
- How can schools assess the privacy policies and practices for each website and online service being considered for use in the classroom?

1 http://educationnewyork.com/files/educationbreaches2013.pdf

2 http://www.csmonitor.com/USA/Education/2014/0226/Data-breach-at-Indiana-University-Are-colleges-being-targeted

3 https://www.riskbasedsecurity.com/reports/2012-DataBreachQuickView.pdf

4 http://storage.googleapis.com/ikeepsafe/Data_Privacy_And_Schools.pdf