This resource sponsored
by Clarity Innovations

K-12 BLUEPRINT

A planning resource for personalizing learning

Don't Have Your Head "Up in the Clouds" with Metadata

toolkits

Metadata can both help a student to achieve his or her academic goals, or be used to identify that student for as long as that information is available.

In the past, "education data" meant a student's name, grade, address, and attendance record. But with today's digital learning tools, education data is much, much more: a morass of "metadata" gleaned each time a student interacts with these tools and learning services.

According to the U.S. Department of Education, metadata is the contextual or transactional data collected by many online educational services as part of their operations[1]. This information can both help a student to achieve his or her academic goals, or be used to identify that student for as long as that information is available.

While removing data or "de-identifying" data once it is no longer being used is one way schools and districts can help protect student privacy but, according to U.S. Department of Education Chief Privacy Officer Kathleen Styles, "re-identification risk is a very real risk. You can't just take off somebody's name and say that the record is anonymized. With the amount of information that's available online, it's increasingly easy to re-identify individuals"[2].

Data privacy is further complicated when, through a variety of popular educational services, this data resides not on school servers but instead in the cloud.

"We've had a very rapid adoption of cloud storage and online services," says Bob Moore, the founder and chief consultant of RJM Strategies, LLC. "Districts have much more responsibility in managing these issues than they often realize"[3].

A December 2013 report by the Fordham Law School Center on Law and Information Policy[4] found that while "95 percent of districts rely on cloud services for a diverse range of functions," fewer than 7 percent of those studied prohibit service providers from selling or marketing student data.

This means that, in this world of phishing scams and social hacking, school districts must be vigilant of both their in-house student data and data stored in the cloud, due to third-party providers. Schools need to be confident that vendors have only necessary information and written confirmation that student data will not be sold.

In April 2014, the National School Boards Association released a legal and policy guide for school boards called "Data in the Cloud"[5] which recommends that school districts:

- Identify an individual district-wide chief privacy officer;
- Conduct a privacy assessment and online-services audit, preferably by an independent third party;
- Establish a data-safety committee or data-governance team;
- Review and update district privacy policies regularly;
- Adopt consistent and clear contracting practices that address student data appropriately, and discourage take-it-or-leave-it terms; and
- Train staff members about data-privacy issues and tactics for protecting data.

Other questions to ask before signing a cloud services agreement include the following:

- Are all passwords and backups encrypted?
- Can content be shared with another party without written consent from the school district?
- Will all content, including backups, be deleted upon termination of the contract?

1 http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20(February%202014).pdf

2 http://www.educause.edu/ero/article/privacy-and-security-initiatives-and-recommendations-us-department-education

3 http://blogs.edweek.org/edweek/DigitalEducation/2014/03/post_7.html

4 http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip

5 https://cdn-files.nsba.org/s3fs-public/Data_In_The_Cloud_Guide_NSBA_COSA_02-09-15.pdf?RQkKRotGvL6gD6tmH_jHZTHelMfxdlUA