K-12
BLUEPRINT
A planning resource for personalizing learning

Give Your Third-Party Vendors the Third Degree

toolkits

Contracts with third-party vendors should specify exactly what data will be collected, who has access to that data, what that data will be used for, and how (and when) that data will be deleted.

Third-party vendors provide a number of powerful services that can empower both students and teachers to take full advantage of 21st Century learning. But with that opportunity comes the very real possibility that student data can be compromised or used for unintended purposes. This is why contracts with third-party vendors should specify exactly what data will be collected, who has access to that data, what that data will be used for, and how (and when) that data will be deleted.

To address some of the security concerns brought about by contracting with third-party vendors, the Software & Information Industry Association has created the Best *Practices for the Safeguarding of Student Information Privacy and Security for Providers of School Services* resource, which includes a number of best practice guidelines including the following:

"***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 personally identifiable information 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 personal student information 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."*[1]

According to FERPA (the Family Educational Rights and Privacy Act), only a student's PII is protected. But in 2009, the definition of "school official" was expanded to include service providers, so that if there is a legitimate educational interest to grant a student's PII, prior written consent is not required.[2]

Meanwhile, under the revised COPPA rule, operators must both keep data secure while assessing the security practices of third parties with whom that data is shared: "The operator must also take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security, and integrity of such information, and who provide assurances that they will maintain the information in such a manner."[3]

This puts a lot of pressure on district leaders. This is why educating students and staff in acceptable and responsible use of technology and services is so vital, as well as establishing transparency with parents regarding how their child's privacy is being secured by posting online the services used by the district, the types of data uploaded to them, and the privacy protections for that data.

Also be sure that contracts with vendors prohibit or limit the selling or marketing student information without parental consent and require district notification if data is breached.

[1] http://archive.siia.net/index.php?option=com_content&view=article&id=1682:siia-announces-industry-best-practices-to-safeguard-student-information-privacy-and-data-security-and-advance-the-effective-use-of-technology-in-education&catid=62:press-room-overvi

[2] http://blog.varonis.com/passing-grade-edtech-needs-privacy-solution

[3] http://www.ecfr.gov/cgi-bin/text-idx?SID=9fd598ec532cda9673a45941a7f53135&node=20130117y1.14