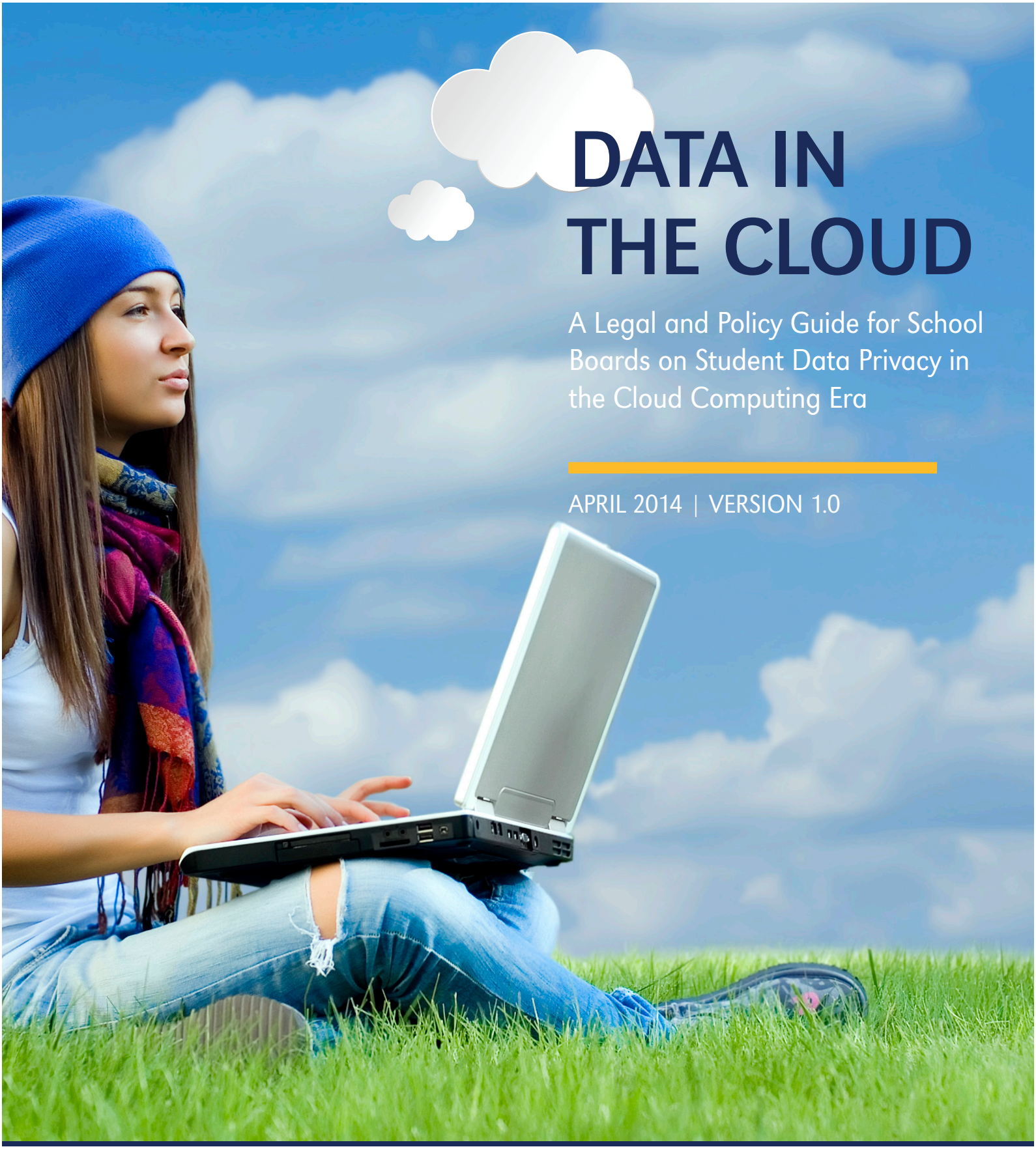

DATA IN THE CLOUD

A Legal and Policy Guide for School Boards on Student Data Privacy in the Cloud Computing Era

APRIL 2014 | VERSION 1.0

National School Boards Association

DATA IN THE CLOUD

A Legal and Policy Guide for School Boards on Student Data Privacy in the Cloud Computing Era

APRIL 2014 | VERSION 1.0

Staying competitive in today's digital world means more than merely placing a tablet in the hands of students. It means using technology in ways that are innovative in scope and reach, accessing the latest software applications, and using new electronic pathways to store and process information. It is becoming rare for a school district to house, process, and transmit the trove of educational and business records necessary to keep a school system operating effectively on servers maintained solely by a district's IT department. Today, your school district is doing much of its "computing" online. Your work has shifted to a new digital infrastructure made necessary by the ubiquity of personal devices such as tablets and cell phones. We expect to access, transmit, and store vast amounts of information instantly. This technological marvel that involves both process and substance, and hardware and software, is more than the Internet. It has come to be known simply as "the Cloud."

The Cloud's presence in both our personal and professional lives has happened so quickly and so subtly that most of us barely perceive its operation, although we feel its impact. In fact, many of the educational tools employed by your teachers and district offices operate through an Internet connection only. The advantages of Cloud-based platforms and learning tools are obvious —ease, convenience, 24/7 accessibility, less staff time maintaining on-site servers, individualized learning, and compliance with testing requirements.

But along with these benefits come serious challenges, particularly the potential for loss of privacy that accompanies the transfer of personal student information to the Cloud. Concerns about data privacy are real and must be addressed by public school districts, which reflect the values and norms of their communities.

This guide is a resource for you, a K-12 public school board member. It is designed to help you identify the crucial issues associated with student privacy when your district uses online educational services, and recommends a comprehensive approach to addressing student data privacy protection.[1]

This guide is not intended as a substitute for appropriate legal counsel. School boards will be well served by seeking the advice of a school lawyer who is a member of the NSBA Council of School Attorneys (COSA) when designing and identifying polices around the issues presented here and by Cloud computing generally.[2]

And, as always, keeping your community informed about the steps your board and administration are taking in this arena will go a long way to creating confidence in the policies you have adopted to address concerns about privacy loss.

Why the increased concern about protecting student data privacy?

➔ Simply put, we are all more aware now about the kinds of personal information being exchanged through digital devices. The news about government surveillance programs, research reports, surveys, and official guidance from the U.S. Department of Education have focused the national spotlight on data privacy, particularly privacy of student data.

With the increased public attention to this issue has come a wave of state-level proposed legislation, and federal legislation is anticipated. As a school leader, you should be able to articulate your district's commitment to protect student privacy, and its policies and practices. Teachers and administrators must understand the necessity of taking steps to ensure that cloud services deployed throughout a district's offices and classrooms comply with all applicable laws and district policies. And the school district community—including parents—should be consulted and educated about the district's use of the Cloud.

Community feedback may significantly influence the direction your school district goes with restrictions placed on student data in the Cloud. One community may influence school board policy that absolutely prohibits the disclosure and use of aggregate data by third parties for advertising and commercial purposes. Another community may be less concerned with the use of data for commercial purposes if that meant a cost savings for the district and/or a product that is easier for teachers, students, and families to use.

What online or Cloud-based tools should school boards be concerned about with respect to student data privacy?

➔ Every device and application with a connection to the Internet potentially collects student data—from the school district's email system to the video-recording app a teacher directs her students to use via digital tablet in her classroom.

➔ In late 2013 and early 2014, at least three national studies and technical papers were released that addressed student data privacy. Fordham Law School's Center on Law and Information Policy released a report in December 2013 based on research regarding how K-12 public school districts address the privacy of student data when they transfer it to Cloud computing service providers. The report, "Privacy and Cloud Computing in Public Schools," received a significant amount of media attention, particularly because it identified numerous deficiencies in school district practices regarding safeguarding student privacy.[3]

In February 2014, Common Sense Media published the results of a poll it deployed to 800 registered voters nationwide. Nine out of 10 respondents were concerned about how private companies with non-educational interests are able to access and use students' personal information to market, advertise and sell products and services.[4]

And, in late February 2014, the U.S. Department of Education's Privacy Technical Assistance Center (PTAC) published much-anticipated guidance for schools entitled "Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices." It points out that the federal laws governing educational records and websites directed at children do not cover every possible use of student-related data. The department recommends that schools go beyond the "minimum" required by these laws, and "adopt a comprehensive approach to protecting student privacy when using online educational services."[5]

Perhaps the most obvious example of a Cloud-based application is Internet-accessed email. Services like Gmail, Yahoo mail, and Hotmail allow users to access and send email anytime and anywhere through an Internet connection. The applications are installed, maintained, and upgraded remotely in the Cloud by a third-party service provider.

School districts can work to protect student data privacy more directly through district-wide systems such as email and records management, where the district has some control over the terms of the contract with the provider. Districts across the country are working hard to configure their data systems to allow for the greatest efficiency while still maintaining security for student and employee privacy.

More difficult student data privacy issues arise with the universe of applications available to individual staff and students through a simple Internet connection, often to a device that can fit in a pocket. These applications create separate "doors" to district data that it may not be able to control in every case. Both types of applications—the district-wide data management systems and the myriad tools available for specific pedagogical needs—create opportunities for release of student data.

Terminology

In this guide, we use several terms interchangeably:

"Service provider" and **"provider"** refer to outside companies providing Internet-based educational services to schools, school districts, teachers, students, parents, and communities.

"Internet-based," "Cloud-based," or **"online"** used with **"educational services,"** or **"tools"** refer to the range of applications, platforms, and environments that providers make available to schools through the Internet, including services that store student data outside of the school district's control, and those accessible by an array of personal and school-owned devices.

"School(s)," "schools and districts," "school district," and **"district"** all refer to K-12 public educational agencies that may implement Internet-based educational services. Although this usually will occur at the district level, it is possible that it could occur at the school or classroom level.

What are the student data privacy risks associated with online educational services?

Once school district information is transferred or stored in the Cloud, as opposed to on an on-site server, it is housed on a system operated by others, usually on shared servers.[6] This means that the school district does not have physical control over the data, even if the contract states that the district retains "control." School networking professionals note the following potential issues that may arise:

- Data breach caused by faulty configuration, patching, and updates, or software viruses or exploits;
- Data loss by users who, knowingly or not, expose information by sharing or sending it;
- Password reuse due to lax controls (i.e., password written on a sticky note); and
- Collection and aggregation of personally identifiable data and metadata for potential use in advertising and sale to third parties.7

Data breaches tend to receive a great deal of public attention. For example, in February 2014, a University of Maryland student database was hacked. The hackers got away with names, birthdates, social security numbers, and student identification numbers of 300,000+ past and present students and faculty. This breach was widely reported in the press.[8]

But it is the final issue listed above—the ability of service providers to collect and store "profiles" of students or their families based on their use of an application—that is gathering concern. The information gleaned from such collection could be used to target advertising to students or their families. Legal standards restrict some, but not all, of this activity.

What does the law require school boards and online service providers to do to protect student data privacy?

There are numerous laws that potentially govern student data privacy. The most directly applicable to school districts and service providers are the Family Educational Rights and Privacy Act (FERPA)[9] and its sister statute, the Protection of Pupil Rights Amendment (PPRA),[10] which apply to educational institutions that receive federal financial assistance; and the Children's Online Privacy Protection Act (COPPA),[11] which applies to operators of websites and mobile apps that are directed to or known to be used by children under the age of 13.

FERPA—Requirements for School Districts

FERPA prohibits school districts from disclosing, except in limited instances, personally identifiable information (PII) contained in students' education records without the consent of the parent or eligible student. Educational records may include a range of written and electronic files. Generally, anything that is considered PII in an education record, including emails and other communications or documents created by students, teachers, and administrators, is gov-

erned by FERPA.

Any time a school district (or even a classroom teacher) deploys new technology, your administration should consider the FERPA implications. Please consult your school attorney for assistance with examining the FERPA implications of particular technologies. Here is a short discussion of the many FERPA issues that arise in the student data context:

- Does FERPA apply at all? Under FERPA, elementary and secondary "education records" include "records, files, documents, and other materials" that: (1) "contain information directly related to a student;" and (2) "are maintained by an educational agency or institution or by a person acting for such agency or institution."[12] Many new technologies are likely to result in the storage or transmission of information that also will be considered an education record under FERPA, but a few may not. It may be prudent for your school district policy to presume that all data created by students, teachers, and staff related to students is an "education record," and to retain control over it. This presumption will help your administration direct third-party technology providers as to how they should handle the data, how they can use it, and with whom they can share it.
- Is storing student information in the cloud permitted under FERPA? Generally, yes, though the FERPA statute and regulations require schools to manage education records and student PII securely. Best practices suggested by the Department of Education and elsewhere indicate that the school or district should authorize its staff to use only those services in which the terms of service allow the school/district to retain enough control, and provide sufficient parental notice, to invoke the "school official" exception described below.
- Which parts of FERPA allow release or disclosure of some student data for use by an online educational service? There are two notable exceptions to FERPA's requirement of parental consent that may allow school staff to disclose PII in education records under certain circumstances. "Directory information" under FERPA is not an education record, but is information that historically has not been considered harmful if disclosed, such as a student name or address. Directory information may be released without parent or student consent, provided that the district has

Cloud services tend to be thought of as types of services and types of Clouds.

Services:

Software as a Service (SaaS)—Software applications formerly delivered as a service over a network are now delivered as services in the Cloud. Examples: Salesforce (CRM), Microsoft (Office 365), Google (Google Apps), Adobe (Creative Suite).

Platform as a Service (PaaS)—PaaS provides a complete development environment. The software developers can program, debug and execute their new applications through the platform. Examples: Google (App Engine); Microsoft (Windows Azure).

Infrastructure as a Service (IaaS)—IaaS is remote computing capacity, including storage, hardware, servers, and networking components that can be scaled up or down as the customer needs more capacity. Example providers: Amazon, Microsoft, Google (Compute Engine).

Clouds:

Public Cloud—A public cloud is a large data center or centers that can span multiple geographic areas running the workloads of many customers at once, managed and owned by the provider (not the school district). Example providers: Microsoft, Google (Google Apps), Apple (iCloud), Dropbox.

Private Cloud—A private Cloud is created by, located on, and/or maintained and controlled by the school district. This attempts to achieve "physical separation" of data and computing workloads, often for security purposes. Some experts would say "*private Cloud*" is somewhat of a misnomer, because physically isolated servers are really traditional data centers.

Hybrid Cloud—A hybrid Cloud is a mixture of the models described above, often including both public and private services, as well as on-site computing. A school district might elect to put different things in different places: personally identifiable employee information could reside in a private Cloud; and policies or curriculum information could reside in a public Cloud.

Community Cloud—A community Cloud, where several organizations share a private Cloud, is an attempt to combine some of the cost savings of a public cloud with some of the security benefits of a private Cloud. This approach has proven popular with the U.S. Government, which has purchased such community Cloud capacity from companies such as Amazon, Microsoft, and IBM.

Partner Cloud—In a partner Cloud, services are offered by a provider to a limited and well-defined number of parties.

Examples of Online Educational Services*

Category	Example	Consumer	District	Classroom	SaaS	PaaS	IaaS
Email Services	Outlook.com	●			●		
	Yahoo.com	●			●		
	Gmail	●			●		
Data Backup	Carbonite	●			●		
Productivity Suite	Google Apps for Education		●		●		
	Office 365 for Education		●		●		
Differentiated and Personalized Instruction	Edmentum Plato Learning		●		●		
	Compass Learning		●		●		
	Odyssey		●		●		
	Digedu		●		●		
Teacher Evaluation System	TalentEd Perform		●		●		
Student Information System	Infinite Campus		●		●		
	PowerSchool		●		●		
Career Planning Sites	Career Cruising		●		●		
	Naviance		●		●		
Ebooks	Overdrive		●		●		
Library Management Systems	Follet Destiny		●		●		
	Alexandria		●		●		
Dynamic Indicators of Basic Early Literacy Skills	Dibels		●		●		
Library Subscription Websites	CLIO		●		●		
	Gale		●		●		
	Worldbook		●		●		
	Ebsco		●		●		
	ABC		●		●		

(continued)

Examples of Online Educational Services (continued)

Category	Example	Consumer	District	Classroom	SaaS	PaaS	IaaS
Emergency Notification System	School Messenger		●		●		
Mobile Device Management (MDM) Platforms	Meraki		●		●		
	Airwatch		●		●		
Finance Systems	Infinite Visions		●		●		
	Skyward		●		●		
Content Management Systems	Edline		●		●		
	Joomla		●		●		
Professional Development Tracking Website	ProTraxx		●		●		
	Maximus Response to Intervention		●		●		
Performance Based Learning	Thinkgate		●		●		
Cloud Storage And Server Hosting Services	Amazon AWS		●				●
	Microsoft Azure		●			●	●
Learning Management Systems	Schoology		●	●	●		
	Moodle		●		●		
	Canvas		●	●	●		
	Edmodo		●	●	●		
Cloud Storage	Dropbox.com	●	●		●		
	Box.com	●	●		●		
Game Based Learning	BrainPop		●		●		
Blogging	Wordpress	●	●		●		
Supplemental Online Lessons And Instructional Modules	Skillstutor		●		●		

**Thanks to Jim Siegl, Keith Bockwoldt, and the Consortium for School Networking for assembling this information.*

designated and published in a public notice the specific types or categories of information that will be disclosed as such. Because parents must be able to opt out of disclosure of directory information, however, it is difficult for school districts to rely regularly on the "directory information" rules to transfer student information to third parties. More often, when a school district employs online educational services, it will do so under the "school official" exception, which allows a district to disclose FERPA-protected records without consent to "[a] contractor, consultant, volunteer, or other party to whom an agency or institution has outsourced institutional services or functions."[13] A district may use the so-called "school official" exception for disclosure of education records to online service providers, but the requirements of that exception must be met:

1. The designated "school official" must perform a function that the school or district would otherwise have used its own employees to perform.
2. The school district must set up reasonable methods to ensure that the service provider/school official accesses only student records in which it has a legitimate educational interest; that the service provider is under the direct control of the district with regard to the use and maintenance of the records; and that the provider uses FERPA-protected information "only for the purposes for which the disclosure was made,"[14] and refrains from disclosure to other parties without authorization.[15]

There are benefits and drawbacks for a school or district that designates all or certain providers of online educational services as "school officials" to meet the FERPA exception, which you should discuss with your school attorney.

- What can Cloud service providers do with the student data once it is in the Cloud? FERPA regulates educational agencies or institutions, not Cloud service providers. The school district is responsible for privacy and security of educational data in the Cloud. When the school official exception is in play, the provider may not use FERPA-protected information for any other purpose than that for which it was disclosed, but it is the district's responsibility to enforce that requirement.[16]
- If student information is transferred to a provider through an app or service, does FERPA require that the district give parents notice? It depends on which FERPA rule the school district is using. If the disclosure is made under the directory information concept, it must fall under one of the elements/categories of directory information that has been listed and published previously in a public notice (usually the annual FERPA notice sent home to parents). Under the school official exception, the district must specify in its annual FERPA notice the criteria for determining who constitutes a school official and what constitutes a legitimate educational interest.[17]

PPRA—More Requirements for School Districts

The PPRA requires schools and contractors to make certain instructional materials available for inspection by parents and to obtain written parental consent before requiring minor students to participate in some surveys, analyses, or evaluations that reveal information concerning certain subjects. The law also requires school districts to develop policies in consultation with parents on the collection, disclosure, or use of personal information collected from students for the purpose of marketing or selling that information, though there is an exception to this requirement for "educational products or services," including district testing.[18] School districts must give parents at least annual notice of PPRA policies, an opportunity to opt out of instructional activities related to these subjects, and notice of specific events surrounding these subjects.[19]

The PPRA exception for "educational products or services" often swallows

up much of the rule in the school setting.[20] You should regularly consult with your school attorney, however, regarding application of this statute to student data collections.[21]

COPPA—Requirements for Website and Online Service (Including Mobile App) Operators

COPPA imposes certain requirements on website (and mobile app) operators "to place parents in control over what information is collected from their young children online."[22] The Federal Trade Commission (FTC) enforces COPPA, and it has issued rules and guidance that apply to operators that collect, use, or disclose personal information from children, and those with actual knowledge that they are collecting, using, or disclosing personal information from children under the age of 13. Personal information includes: geolocation data, photos, videos, and audio files that contain a child's image or voice, and "persistent identifiers" (tracking cookies). COPPA requires that such operators obtain parental consent before undertaking such activities.

When a school contracts with a Cloud vendor to provide online services to students, it may provide consent under COPPA on behalf of the parents under certain circumstances, but school personnel need to understand fully the purpose for which any personal information about students is collected and how it is used or shared by the operator.[23] The FTC has stated that there is a difference between collection, use, or sharing of a child's personal information "for the use and benefit of the school," and collection, use, or sharing for "other commercial purpose."[24] An operator will need to obtain actual parental consent (not school district consent) when it "intends to use or disclose children's personal information for its own commercial purposes in addition to the provision of services to the school."[25]

Beyond the law to best practices: What should my school board be doing to address student data privacy in the context of online educational services?

As a school board member, you can be a key component of your school district's move toward a comprehensive student privacy protection program. We encourage school districts to review and, if necessary, reformulate policies (working with your state school boards association, school attorney, and technology staff) after engaging your community. Here are some specific steps you can take:

- Identify an individual district-wide Chief Privacy Officer (CPO), or a group of individuals with district-wide responsibility for privacy.
- Conduct a district-wide privacy assessment and online services audit, preferably by an independent third party. By determining what services are currently in use, and to what extent student data is used and protected within those services, your district will have the basis for determining what policy or practice changes are necessary.
- Establish a safety committee or data governance team that includes the school or district's Chief Privacy Officer. This team engages with the school community regarding proposed and existing use of Internet-based educational services that may use student information, recommends policies and best practices, and serves as the liaison between the school district and the community on privacy issues. This team also could serve as the review board to approve adoption of specific apps and services.
- Regularly review and update relevant district policies and incident response plans, in consultation with your state school boards association and school attorney. Consider including the following in your district's policy:
    1. Clear guidelines or procedures for evaluation and adoption of Cloud services, which include requiring a written contract; and
    2. Statements regarding whether or when the district may allow the use of student data for service-provider uses outside of the contracted service.
- Consistently, clearly, and regularly communicate with students, parents, and the community about privacy rights and district policies and practices with respect to student data privacy. Include in an annual notice to parents the types of information transferred to Cloud service providers.
- Adopt consistent and clear contracting practices that appropriately address student data and discourage acceptance of take-it-or-leave-it terms. Contracts with service providers should include terms that enable the district to control student data. Your school attorney should have access to detailed contract recommendations at *www.nsba.org/COSA*.
- Train staff. To be sure of consistent implementation of your school district's policies and procedures regarding student privacy, extensive staff training may be necessary. Individual classroom teachers should not make unilateral decisions regarding implementation of online services. School district staff need to be informed not only of the basic legal requirements and the specific policies and procedures that must be followed in your district, but also of privacy "norms" that fuel public sentiment and understanding of what privacy means.

It is very important that school districts carefully examine operator data collection, use, and sharing policies prior to deploying those services, or agreeing to act as an agent or intermediary for parental consent.[26] When a school or district acts as an agent of the parent(s) to provide consent for the collection of student personally identifiable information, it must notify the parents—usually through an acceptable use policy or consent form. COPPA does not apply to websites contracting with school districts for the sole benefit of the school's use of their students' data (for example, Gradebook).

Do FERPA, PPRA, and COPPA cover all student data privacy issues?

➔ No. The laws provide a basic framework, but not a complete regulatory scheme for addressing student data privacy issues. As noted by the Department of Education, simply because an online educational service collects or maintains student information does not mean that such information is protected by FERPA or PPRA. FERPA may not require parental notice or consent for every release of student information. For example, metadata, such as the amount of time a student takes to perform a particular task, how many attempts he or she made, or how long the student's mouse hovered over an item, could be disclosed consistent with FERPA if they are stripped of all direct and indirect student identifiers.

Some state legislatures have imposed new data protection requirements, and other states and Congress may do so in the near future. With an incomplete and evolving legal landscape and public opinion leaning in the direction of additional protections for student data, your school board should consider going beyond the current legal requirements and adopting a "comprehensive approach to protecting student privacy."[27]

Given all of these concerns regarding student data privacy, should school districts stop using online tools and services?

➔ No. The purpose of this guide is to point out issues that need to be addressed when your school district transfers student data to the Cloud, not to discourage your school district from innovating. School districts can protect student privacy appropriately while still taking advantage of modern technology, including using data to improve school performance and student learning.

Where do I go to explore the issue of protecting student data privacy in more detail?

➔ As student data privacy rules and norms continue to evolve, NSBA and its member state school boards associations will continue to update resources that will be useful to you. Please regularly check *www.nsba.org* and your state school boards association website. If your school attorney is a member of NSBA's Council of School Attorneys, he or she will have access to updates and resources on the quickly-evolving legal standards at *www.nsba.org/COSA*.

Resources

Center on Law and Information Policy at Fordham Law School, "Privacy and Cloud Computing in Public Schools" (report issued December 12, 2013), *available at* http://law.fordham.edu/center-on-law-and-information-policy/30198.htm.

Consortium for School Networking (CoSN), "Security and Privacy of Cloud Computing," available at http://www.cosn.org/about/news/cosn-issues-new-report-%E2%80%98security-and-privacy-cloud-computing%E2%80%99.

iKeepSafe, "Digital Compliance and Student Privacy: A Roadmap for Schools," *available at* http://storage.googleapis.com/digital_compliance/DigitalComplianceStudentPrivacy.pdf.

Safegov, "5 Things School Officials Must Know About Privacy" (video for school officials), *available at* http://edu.safegov.org/school-officials/.

U.S. Department of Education Privacy Technical Assistance Center, "Frequently Asked Questions: Cloud Computing" (June 2012), *available at* http://ptac.ed.gov/sites/default/files/cloud-computing.pdf.

U.S. Department of Education Privacy Technical Assistance Center, "Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices" (February 25, 2014), *available at* http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29.pdf.

Letter from Secretary of Education Arne Duncan to Senator Edward J. Markey (January 13, 2014), *available at* http://ptac.ed.gov/sites/default/files/2014-01-10_Education_Privacy.pdf.

End Notes

1 Numerous collateral issues are not addressed in detail here—employee privacy, online communication and social media, incident response protocols, security measures such as encryption, school websites, search and seizure (as well as surveillance) of student-owned or -used devices, and the specifics of education and training for school officials, educators, and the community, to name just a few. As your district expands its use of Internet-based tools, awareness of the need for privacy protections increases, and as Congress and state legislatures pass related legislation, your policies and practices will need to remain up-to-date. Please check frequently with NSBA, your state school boards association, and your school attorney for updates to this and state-level guidance documents.

2 The National School Boards Association's Council of School Attorneys (COSA) is the professional network of school lawyers representing K-12 public schools. To find a COSA lawyer, or to learn more about COSA, go to: www.nsba.org/COSA.

3 Center on Law and Information Policy, Fordham Law School, Privacy and Cloud Computing in Public Schools (Dec. 12, 2013), *available at* http://law.fordham.edu/center-on-law-and-information-policy/30198.htm. *See* Natasha Singer, Schools Use Web Tools, and Data is Seen at Risk, N.Y. Times, Dec. 13, 2013, *available at* http://www.nytimes.com/2013/12/13/education/schools-use-web-tools-and-data-is-seen-at-risk.html?ref=natashasinger.

4 "Student Privacy Survey," Common Sense Media (Jan. 2014), *available at* http://cdn2-d7.ec.commonsensemedia.org/sites/default/files/uploads/about_us/student_privacy_survey.pdf. Over half did not know anything, or not very much, about how their schools currently collect, use, store, and destroy student data. A significant percentage (anywhere from 70-91 percent) would support regulation of the use of student data, including requiring schools to notify parents before sharing students' personal data with private companies, tightening security standards to protect student data stored in the cloud, making it illegal for schools and tech companies to sell students' personal information to advertisers, restricting companies from using students' online habits and searches on school computers to target online ads to them, and restricting large, for-profit companies from using student email, online searches, and Web history to build a profile of personal data and demographics over time.

5 U.S. Dep't of Educ. Privacy Technical Assistance Ctr., *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices* (Feb. 25, 2014), *available at* http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29.pdf.

6 The Consortium for School Networking (CoSN) has published a guide for school officials entitled "Security and Privacy of Cloud Computing," *available at* http://www.cosn.org/about/news/cosn-issues-new-report-%E2%80%98security-and-privacy-cloud-computing%E2%80%99.

7 CoSN Guide, at 2.

8 Patrick Svitek & Nick Anderson, *U.Md. Computer Security Attack Exposes 300,000 Records*, Wash. Post, Feb. 19, 2014, *available at* http://www.washingtonpost.com/local/college-park-shady-grove-campuses-affected-by-university-of-maryland-security-breach/2014/02/.

9 20 U.S.C. § 1232g; *see also* 34 C.F.R. 99.1-99.35 (Department regulations implementing FERPA).

10 20 U.S.C. § 1232h.

11 15 U.S.C. § 6501 *et seq.*

12 20 U.S.C. § 1232g(a)(4)(A).

13 34 C.F.R. § 99.31(a)(1)(i).

14 34 C.F.R. § 99.33(a); *see also* 2014 ED Guidance, at 3-4.

15 The 2014 ED Guidance suggests that schools and districts "usually" will be able to establish direct control for purposes of the school official exception through a contract with the provider. Similarly, a Terms of Service agreement may provide sufficient terms to legally bind the provider that are consistent with the direct control requirements. 2014 ED Guidance, supra note 7, at 4.

16 2014 ED Guidance, at 5; *see also* 34 C.F.R. § 99.33 (use and re-disclosure requirements).

17 34 C.F.R. § 99.7(a)(3)(iii).

18 20 U.S.C. § 1232h(c)(1)(E), -(c)(4).

19 20 U.S.C. § 1232h(c)(2).

20 20 U.S.C. § 1232h(c)(4).

21 The Department's 2014 ED Guidance contemplates application of PPRA to a situation in which a school district provides FERPA- protected data to an online service provider to open accounts for students, after which there are subsequent data-gathering interactions between the provider and the student. 2014 ED Guidance, at 6.

22 Fed. Trade Comm'n, "Complying with COPPA: Frequently Asked Questions," *available at* http://business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions.

23 COPPA FAQ.

24 COPPA FAQ, at M.1.

25 COPPA FAQ, at M.2.

26 The FTC directs school districts to ask specific questions of operators before determining whether to serve as an intermediary for parental consent. For example: Does the operator use or share the information for commercial purposes not related to the provision of the online services requested by the school? Does it use the students' personal information in connection with online behavioral advertising, or building user profiles for commercial purposes not related to the provision of the online service?

27 *See* 2014 ED Guidance, at 5.

1680 Duke Street Alexanria, Virginia 22314-3493
Phone: 703.838.6722 Fax: 703.683.7590
www.nsba.org