Hogan Lovells

MEMORANDUM

Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

TO School District Clients and Friends

FROM Maree Sneed
Bret Cohen

DATE March 2, 2015

SUBJECT ***Department of Education Issues "Model Terms of Service" and Other Guidance on Student Privacy Compliance***

On February 26, the U.S. Department of Education issued guidance aimed at assisting schools and school districts when considering whether the use of online educational services and mobile applications complies with student privacy laws. The guidance consisted of two main components. First, the Department published a document entitled *Protecting Student Privacy While Using Online Educational Services: Model Terms of Service*, which evaluates common privacy-related provisions in online Terms of Service and analyzes how they comply with student privacy requirements. Second, the Department produced a user-friendly, 10-minute training video directed to K-12 administrators, teachers, and staff about schools' privacy obligations when using online educational services and applications. Finally, the guidance encourages school administrators to check the Student Privacy Pledge when considering whether to use online educational services in the classroom.

This follows Department of Education guidance issued almost exactly a year ago, which we summarized in a detailed Client Alert at the time, about the privacy obligations of schools and school districts when considering online service providers and applications. That guidance commented that schools should review online educational service providers' online Terms of Service (TOS) prior to sharing student data with online services to determine whether the TOS are consistent with privacy requirements under laws like the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and the Protection of Pupil Rights Amendment (PPRA).

Model Terms of Service

The "Model Terms of Service" issued by the Department built on that previous advice. Despite the title, the Model Terms are not a template that the Department expects schools to insist that their online educational services and applications adopt when providing services to the school. Instead, the document contains a checklist of the types of privacy-related provisions that commonly appear in online services' TOS, such as provisions related to marketing and advertising, modifications to the TOS, data use, data sharing, security controls, and data de-identification. For each type of provision, the document provides sample TOS provisions under the headings "GOOD! This is a Best Practice" and "WARNING! Provisions That Cannot or Should Not Be Included in TOS," and explains why those provisions either represent a best practice or are problematic when considered in light of schools' privacy obligations.

For example, the guidance includes the following with respect to TOS provisions on data sharing:

	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
8	Data Sharing	"Data cannot be shared with any additional parties without prior written consent of the User except as required by law." *Or* "The [School/District] understands that Provider will rely on one or more subcontractors to perform services under this Agreement. Provider agrees to share the names of these subcontractors with User upon request. All subcontractors and successor entities of Provider will be subject to the terms of this Agreement."	"Provider may share information with one or more subcontractors without notice to User." *Or* "Where feasible, Provider will require third-party vendors to comply with these Terms of Service."	While it is perfectly acceptable for providers to use subcontractors, schools/districts should be made aware of these arrangements and subcontractors should be bound by the limitations in the TOS.

This recommendation helps schools and districts comply with their obligations under FERPA and other laws to take steps to make sure that third-party service providers use student information only for the purposes outlined or anticipated by the school.

Training Video

In addition to the TOS guidance, the Department's training video provides an overview of the obligations of schools and districts when using educational services. The video notes:

> "Technology in classrooms can improve education by expanding our knowledge, communication, and productivity. But as we enjoy these new tools, we must be mindful of the risks they bring, and follow best practices to secure and protect students' private information."

It summarizes FERPA's requirement to obtain consent when disclosing student information to an online educational service or application, including common exceptions like the "directory information" exception—which permits certain disclosures of non-harmful student information of the kind that commonly appears in directories, with a parent opt-out—and the "school official" exception—which permits the disclosure of student information to a service provider that performs an institutional service or function that is under the direct control of the school. The video notes that school administrators, teachers, and staff also must keep in mind their obligations under COPPA, the PPRA, and state and local student privacy laws. And it piggybacks on the guidance included in the Model Terms by providing the following example:

> "Meet Ms. Jones, a high school teacher. She just found a great new app to help kids with math through games. Her students love to play games, and the app is free. . . . Some apps require the acceptance of Terms of Service. These can be long, boring, and full of complicated legal language. Ms. Jones needs to fully understand what she is agreeing to in the Terms of Service. We may not think of clicking an "Accept" button as the same thing as signing a written contract, but they can be legally binding agreements. For these reasons, and more, Ms. Jones should talk to the appropriate individuals about the school's policies and procedures before signing up for the app. Administrators should review the app and the Terms of Service to make sure it won't adversely affect student privacy or the security of the school's systems. If your school or school district doesn't already have a process for reviewing and approving apps and online services for classroom use, you should create one."

Student Privacy Pledge

In addition to the Model Terms and the video, the press release announcing the guidance states that school officials can check to see if a potential online educational service has signed the Student Privacy Pledge. The Pledge, issued by the Future of Privacy Forum and The Software & Information Industry Association, contains a list of 12 commitments by which signatories agree to treat student information when providing online educational services to K-12

schools. The Department of Education adds its endorsement of the Pledge to that of President Obama, who supported it in a White House press release and speech last month.

Implications for Schools, School Districts, and Service Providers

By releasing this guidance, the Department of Education is continuing its push for covered schools, school districts, and universities to increase their awareness of their student privacy compliance obligations as online educational services proliferate in the classroom. But the guidance and applicable federal laws are just the tip of the iceberg. Student privacy has become the topic du jour in state legislatures around the country, with over 100 state bills introduced and over 10 laws passed in 2014 touching on student privacy, including California's trailblazing Student Online Personal Information Protection Act, which has become the model for draft federal legislation as part of the President's 2015 legislative platform.

For these reasons, it's becoming crucial for companies offering online services and apps to schools to reconsider their offerings and their TOS in light of student privacy requirements. As we recommended a year ago after the Department of Education issued its previous guidance, online educational services may be able to gain a competitive advantage by taking the initiative to incorporate student privacy requirements and best practices into their existing TOS and contract templates for educational institutions. In particular, online educational services and applications can review their existing TOS against the Department's Model Terms (and the Pledge). If they align, it can serve to demonstrate an organizational commitment to student privacy.

The increased interest in student privacy also is apparent from the schedule for the upcoming SXSWedu conference in Austin, TX, with no fewer than nine panels addressing privacy over the course of three and a half days the second week in March. Hogan Lovells will be on one of those panels, *Student Data: When Innovation Meets Privacy Law*, along with representatives from school administration and industry to discuss how we can create innovative, workable, and secure solutions for student data and digital learning initiatives. With the many layers of laws, guidelines, and best practices out there, we will discuss how educators and EdTech can work together to get innovation into the classroom in a safe and responsible way, all while respecting student privacy and complying with all applicable laws.

* * *

We hope this information is useful to you. If you have questions about Student Privacy please contact Maree Sneed at 202-637-6416 or maree.sneed@hoganlovells.com or Bret Cohen at 202-637-8867 or bret.cohen@hoganlovells.com.