



Mar 16, 2015

Categories:
[Publications](#)

Authors:
[W. Joseph Scholler](#)

U.S. Department of Education Provides Guidance on Protecting Student Privacy While Using Apps and Online Educational Services

On February 26, 2015, the U.S. Department of Education (D.O.E.) released a [guidance](#) featuring model terms of service as well as a [training video](#) aimed at helping schools protect student privacy while using educational apps and online services. The guidance is a follow-up to the D.O.E.'s February 2014 guidance titled "[*Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*](#)." The training video provides an overview of laws governing student data and advice relating to creating policies and procedures for evaluating apps and online educational services. The 2015 guidance provides model contract terms and best practices.

Many schools have embraced the use of apps and online educational services in the classroom. Apps and online educational services are easily accessible, can be used to facilitate individualized learning, and are often inexpensive or free. However, these apps and services may collect, disclose, and use student data in ways prohibited under federal, state, and local laws including, among others, the Federal Educational Rights Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), and Children's Online Privacy Protection Act (COPPA). Since schools are ultimately responsible for ensuring compliance with these laws, they should perform due diligence to ensure that the providers' practices are consistent with the schools' legal obligations.

Unfortunately, agreements governing use of inexpensive or free apps and services are often unlike agreements that schools negotiate for more expensive paid services. While the terms in agreements for paid services are typically (but not always) negotiated by the parties and then agreed to in a signed contract, agreements accompanying apps and online educational services are more likely to be non-negotiable Terms of Service agreements

(TOS). With a TOS, a user is presented the agreement and asked to accept—for example with an “I agree” button. Because TOS are frequently presented to the user upon installation or first use, a classroom teacher (or even a student) may end up agreeing to the terms in the TOS.

To reduce the risk that a TOS with unacceptable terms will be agreed to, a school or district should have an Educational App and Online Service Review Policy (or similar policy) and procedures in place so that it can quickly review TOS associated with apps and online educational services before classroom use. The policy should be widely communicated so that educators know how to submit the applicable TOS for prompt review. Those responsible for review and approval should provide quick turn-around so that the review and approval process does not break down.

An Educational App and Online Service Review Policy should:

- Identify who within the school or district is responsible for evaluating TOS and approving apps and online educational services.
- Create an easy way for teachers to receive feedback about online apps and services that they want to use in the classroom.
- Use a process to screen out services and apps that may pose security or privacy risks.
- Require that the initial reviewer read the TOS carefully and talk to legal counsel about any concerns.
- Require that a copy of the TOS be printed for the school's records.
- Since TOS can often be unilaterally changed by the service provider, require the initial reviewer to periodically check to make sure that the TOS has not been modified in an unacceptable way.

Since the agreements accompanying inexpensive or free apps or online educational services are often non-negotiable, the 2015 guidance is designed to help schools evaluate them. To do this, the D.O.E. provides examples of model terms and best practices relating to the following:

- Data definition, collection, use, and mining.
- Data de-identification and use.
- Marketing and advertising to parents and students.
- Limiting modification to the app or online service agreement.
- Data sharing with third parties.
- Data transfer and destruction upon termination of the agreement or upon the district's request.
- Rights in school or district data that the app owner or service provider may have access to.
- Right of school or district to access all of its data held by the provider.
- Security controls.

Schools should review the 2015 guidance and video carefully and consider whether modifications to their current policies and procedures are necessary. For more information, contact [Joe Scholler](#), [Michael Nitardy](#), or any other member of Frost Brown Todd's [Privacy & Data Security Team](#) or [Government Services Practice Group](#).

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.