K-12 BLUEPRINT

A planning resource for personalizing learning

Everything You Always Wanted to Know About COPPA

toolkits

COPPA (Children's Online Privacy Protection Act)

The Children's Online Privacy Protection Act (COPPA) requires that the operators of online services or websites directed to children under the age of 13 must first obtain verifiable parental consent prior to the collection, use, or disclosure of certain personal information from children. It details what a website operator must include in a privacy policy, when to seek verifiable consent from a parent or guardian, and an operator's responsibilities to protect children's privacy and safety online, including restrictions on marketing to those under 13. COPPA does not, however, apply to "school districts that contract with websites to offer online programs solely for the benefit of their students." This would include web-based testing services or learning management systems, for example.

COPPA allows, but does not require, schools to act in lieu of parents in providing consent in certain, but not all, circumstances. If the school chooses, it may act in lieu of the parent in approving the collection of personal information from students under the age of 13 when the information is only used for the benefit of the school. The school must first assess how the website or online service will collect, use, and disclose that information, and they must confirm that the data will not be used by the operator for any other commercial purpose. For example, schools may use their acceptable use policy (AUP) to inform parents of the online services that are provided to students.

Montclair Kimberley Academy, an independent pre-K–12 school in Montclair, New Jersey, provides a letter to parents describing parental consent as part of its admissions contract. It also offers a list of third-party computer applications and web-based services the school plans to use (with links to their privacy policies and terms of service) on its website: http://www.mka.org/page.cfm?p=810. The academy's Director of Technology, William Stites, provides a first-hand account of his school's handling of COPPA along with an adaptable parental consent letter: http://www.williamstites.net/2012/05/22/coppa-and-verifiable-parental-consent.

COPPA issues that schools must consider the following:

- Schools must assess the privacy policies and practices for each website and online service being considered for use in the classroom.
- Ensure that your school website(s) include a privacy policy that reflects actual practices and complies with Internet privacy laws.
- Schools are advised to keep their Acceptable Use Policy up to date when technology is added to the classroom.
- Schools are encouraged to share reporting with parents regarding their children's progress to help build support

- More and more teachers and school counselors are recording behavioral and bullying incidents onto platforms where they could be shared with the child's future schools.

- Practice transparency, with clearly written policies explaining what data are collected, how the information is used and stored, and to whom it may be disclosed.

- Engage in minimal data collection, gathering only what is reasonably required to deliver a promised product, feature, or service to a child.

The U.S. Department of Education has worked together with several education and industry groups to outline guidelines to help protect the privacy of student data. *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices* (http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20(February%202014).pdf) defines student privacy rights under both COPPA and the Family Educational Rights and Privacy Act (FERPA), and recommends that schools adhere to the following best practices:

- Be aware of which online educational services are currently being used in a district;

- Have policies and procedures to evaluate and approve proposed online educational services;

- Maintain awareness of all relevant federal, state, tribal, or local laws;

- Take extra precautions when accepting "click-wrap" licenses for consumer apps;

- When possible, use a written contract or legal agreement;

- Be transparent with parents and students; and

- Consider that parental consent may be appropriate.

COPAA Update

COPPA expanded the definition of personally identifiable information on December 2012 to include geolocation data, photos, videos and audio files that contain a child's image or voice, as well as "persistent identifiers" (tracking cookies) that could be used to build a profile over time and across different websites or online services. This applies to mobile apps and third-party website "plug-ins" as well as websites, and permits online services designed for both children and a broader audience to comply with COPPA without treating all users as children. The changes took effect July 1, 2013.

Operator Obligations

Under the revised COPPA rule, the Federal Trade Commission (FTC) has mandated that operators must not only keep data secure, but must assess the security practices of third parties with whom data is shared. COPPA requirements state the following:

"The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. 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.

In addition, the FTC has made it clear that operators must delete data 'using reasonable measure to protect against unauthorized access to, or use of, the information in connection with its deletion.'"

While COPPA doesn't prescribe specific security standards, school systems should pose key security questions when assessing an online service provider, with a service level agreement including as many of the following considerations as possible:

- What data does the provider collect?
- What, if any, data is collected by third parties?
- Are backups performed and tested regularly and stored off site?
- Are software vulnerabilities patched routinely or automatically on all servers?
- Where will the information be stored and how is data "at rest" protected? Will any data be stored outside the United States?
- Is all or some data at rest encrypted, and what encryption method is used?

Other COPPA-Related Scenarios

If a website or online service does not strictly fall under COPPA, the site or service's terms and conditions may still prevent someone under 13 from using the site. Sites such as Evernote fall under COPPA, yet the school would act as the parental agent. Khan Academy is an example of a site that doesn't fall under COPPA and allows users under 13 with parental permission or with the school acting as parental agent, while a service such as iTunes—while not falling under COPPA—only allows users under 13 if the parent creates the account.