This resource sponsored
by Clarity Innovations

K-12 BLUEPRINT
Planning for Personalizing Learning

BYOD and COPPA

toolkits

When designing a BYOD program, consider the privacy safeguards and program regulations you will enforce in order to comply with the protections provided by COPPA.

In July 2013, the Federal Trade Commission updated the Children's Online Privacy Protection Act (COPPA) to further strengthen the protection of children's privacy and information online. The new rules were designed to give parents greater control over their family's personal information, and they have been updated to reflect recent developments in mobile apps and social networking.

A challenge for education technology leaders is to find the right balance between freedom of choice for students on their personal devices, and the legal requirement to provide adequate network filtering services and stay compliant with COPPA. When designing a BYOD program, consider the privacy safeguards and program regulations you will enforce in order to comply with the protections provided by COPPA.

How To Comply With Children's Online Privacy Protection Act

When evaluating digital content for a BYOD program, identify all websites, mobile apps, or online services that are directed towards students under age 13. In order for the content to be compliant with COPPA, it must:

- Post a clear and comprehensive online privacy policy describing their information practices for personal information collected online from children
- Provide direct notice to parents and obtain verifiable parental consent before collecting personal information online from children
- Give parents the choice of consenting to the collection of a child's information, but prohibiting disclosure of the information to third parties
- Provide parents access to their child's personal information to review and/or delete
- Give parents the opportunity to discontinue use of a child's personal information and prevent further online collection of information

- Maintain the confidentiality, security, and integrity of information collected from children
- Retain a child's personal information for only as long as is necessary to fulfill the purpose for which it was collected, then delete the information using reasonable measures to protect against its unauthorized access or use

Another consideration for BYOD programs is the security of private student information that is stored online. Protective wireless infrastructure for a BYOD program provides a segmented student network that is separate from the one used by teachers and administrators, thereby avoiding data security conflicts and protecting student information. The amended COPPA defines personal information to include:

- First and last name
- A home or other physical address including street name and name of a city or town
- Online contact information
- A screen or user name that functions as online contact information
- A telephone number
- A social security number
- A persistent identifier that can be used to recognize a user over time and across different web sites or online services
- A photograph, video, or audio file that contains a child's image or voice
- Geolocation information sufficient to identify street name and name of a city or town

BYOD programs clearly recognize that digital technologies, when used properly, can offer substantial educational benefits. These benefits, however, are not without some risks. Schools have the advantage of being able to provide an opportunity for students to learn responsible online behavior in a supervised environment that emphasizes the development of attitudes and skills that will help keep them safe outside of school.

For More Information

More information about COPPA can be found on the Federal Trade Commission* site.