This resource sponsored
by Clarity Innovations

K-12 BLUEPRINT

A planning resource for personalizing learning

Student Privacy Considerations for Parents

toolkits

Parents should not only be involved with their child's home technology use, but also be familiar with the data privacy policies and practices of their child's school.

Parents want the best for their children. And efficiently employed technology in the classroom can build the crucial 21st century skills that students need to flourish, both academically and in life.

But parents also, quite understandably, worry about the possible implications that online services, digital tools, and social media have on their children's privacy. This is why parents should not only be involved with their child's home technology use, but also be familiar with the data privacy policies and practices of their child's school.

A school privacy policy should maintain the security, integrity and confidentiality of student data while notifying parents and students of how this data is collected, used and disclosed. These policies should also include a comprehensive and actionable incident response plan to mitigate any potential damage caused by a privacy breach.

In general, schools should, according to the U.S. Department of Education's *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices* guidelines:

- Be transparent with parents and students regarding privacy policies;
- Consider that parental consent may be appropriate; and
- Communicate consistently, clearly, and regularly with students, parents, and the community about privacy issues[1].

The Family Educational Rights and Privacy Act (FERPA) provides parents with a set of rights and expectation regarding the privacy of their children's data. According to FERPA, schools must give parents certain access to their children's education records. Having an understanding of FERPA regulations—along with other pertinent legislative guidelines such as CIPA (Children's Internet Protection Act) and COPPA (Children's Online Privacy Protection Act)—can help parents make better sense of their children's privacy rights.

If your child's school is disclosing education records containing personal student data for students under the age of 13, they must obtain written and signed consent before sharing the education record with any third-party provider (unless it is only collecting it on behalf of the school and will only use the information to provide services to the school). Schools should also, ideally, issue letters to parents describing parental consent expectations and post a list of third-party computer applications and web-based services the school plans to use on their school web pages, with links to their privacy policies and terms of service.

Types of student information typically captured by school systems include the following:

- Search engine history and Internet usage
- Learning management system logins and session duration
- Blog and forum comment history
- Emails sent and received
- Social media profiles and usage
- Digital textbook progress
- Videos watched
- Exercises completed

Lastly, if parents encounter an incident with their children, there should be a clear way of reporting these to either a school e-safety coordinator or school front office/ designated faculty member.

On the home front, parents would be well advised to frequent the social networks that their children use to better understand the types of interactions and situations they face, being sure to give them their "space." Ideally, this will help spur thoughtful conversations about the dangers of sharing information, such as addresses, and potentially embarrassing photographs, plus what it means to be a respectful digital citizen.

1 http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20(February%202014).pdf