This resource sponsored
by Clarity Innovations

K-12
BLUEPRINT
A planning resource for personalizing learning

Mobile Devices and Student Privacy

toolkits

“Digital footprints” are the traces of our identities that we leave behind when using social media, browsing online, or interacting with apps.

Mobile devices have granted us unparalleled freedom to access information and communicate with one another wherever we are, whenever we want. But like the popular adage goes, freedom isn’t free. The price we pay is our personal information.

This price is especially steep when it comes to children. Most students these days were born into a world of Internet technology and digital tools. So it’s understandable if they don’t always use the utmost caution when venturing online. And today’s technology, especially social media and mobile apps, makes it easier than ever to divulge personal data, location, and any number of identifying factors.

“Digital footprints” are the traces of our identities that we leave behind when using social media, browsing online, or interacting with apps. These traces have the potential to be monitored, tracked, and analyzed by most anyone with an Internet connection. Even seemingly innocuous information, such as relationship status, an impending vacation, current location, family situation, etc., could carry unforeseen consequences.

An update to COPPA (the Children’s Online Privacy Protection Act) in December 2012 (taking effect as of July 2013)[1] expanded the definition of personally identifiable information to include geo-location data, photos, videos and audio files that contain a child’s image or voice, and “persistent identifiers” (tracking cookies). The expanded protection also includes mobile apps, many of which include location tracking and the ability to post data to social media and cloud-based services.[2]

The key is that, once shared, your personal information is no longer personal. It’s no longer strictly “your” information either. This is why it’s vital to inform students to consider the potential “audience” for their images and information before posting it for all to see. Are they comfortable with the fact that everyone at their school or their family could access these images or information? Could someone possibly use this information against him or her?

It’s a bit of a cliché, but it holds true: if you wouldn’t say something or show something to someone in person, then you probably shouldn’t do it online.

Although thoroughly erasing your “footprints” is problematic and unlikely, a good start is to have students review and remove anything they don’t want posted, “untag” photos they don’t want seen, and ask anyone who has posted private information about themselves that they’d rather not have made public to remove it.

Smart phones complicate matters even further due to the fact that they can make a user locatable at all hours. This could not only affect personal safety, but sets the expectation with peers that a student is always in reach, and can prove a distraction when trying to accomplish real-world tasks. It is always safer (and more effective) to not attempt multi-tasking when on your smart phone, especially for children. If a student can’t seem to help themselves, they may be “addicted” to cellphone use and may need intervention.

Bullying is especially problematic through smart phones and mobile devices. Attacks feel more personal as many students have difficulty distinguishing between their real and online personas. Mobile attacks also make it more difficult for adults to intervene. Savvy students should keep the offending texts or pictures (though many may, quite rightly so, feel like deleting them) and consult a trusted adult. Students should also feel empowered to block bullies from sending future communications.

It’s important that your school or district teach students that they have a right to privacy, even if they don’t fully understand this right. This could mean polite refusal at having their picture or a video taken. It is commonplace to have people capture “moments” with their phones, but it is easy to forget that these potentially embarrassing or private moments could be posted or distributed in an inappropriate way that could hurt the subject. Teach students to ask permission before taking a picture or video, as it is their responsibility to ensure that an image is shared properly, and that everyone has a right to privacy regarding their own images.

[1] http://www.usatoday.com/story/cybertruth/2013/07/01/new-coppa-rules-better-protecting-children-online-take-effect-today/2479327

[2] http://www.cosn.org/sites/default/files/pdf/ETN-CloudSecurity.pdf