Digital Safety Tips For Parents

Published by EdTechReview | By Al Kingsley

In addition to running a global technology company, I am a father of two, and I serve on what is the equivalent of a school board in the United Kingdom, which gives me a unique insight into what parents face in raising their children to be safe and conscientious digital citizens.

Despite all this experience, I still worry that kids are safe online.

Social media, chats, and games are fun but they also have risks. Dangers like child grooming, cyberbullying, radicalization, sexting, and a digital footprint that follows a child for life mean that we cannot let our guard down when online. But, we can teach our children to stay safe when they are online.

After all, parents are ultimately the most effective advocates in helping their children navigate the internet safely.

ISTE (International Society for Technology in Education) has advice about online safety for educators. The suggestions are intended for teacher-to-student relationships but are helpful for parents, too. Here are eight important digital safety skills that don't cost anything to implement but that can dramatically minimize the risks of using technology and the Internet.

Be aware of the application footprint

Explain to your child that applications collect data and can track locations through Bluetooth and Wi-Fi. Teach your children to limit location access for applications and to disable these functions when not in use. Also, have the most updated version of an application because these have the latest protections against malware and other threats. Also, teach your child to delete applications that are no longer needed.

Teach appropriate electronic etiquette

Children should know how to conduct their online presence appropriately. Explain that your child's posts can last a lifetime having long-term implications, especially for inappropriate language and images.

Establish a safe online setting

Keep tech use in the open. Children need room to research and socialize, but they also need guardrails. Download the apps your children use to your own device so that you understand firsthand how they work. You don't need to be the expert, instead, use the opportunity to ask questions of your child. If you show genuine interest in an app, they may be more likely to share it with you.

Clarify that you won't hover when they are online but insist that social interaction occurs in an open area, not behind closed doors. If the sound of other goings-on is distracting during study time, use noise-cancelling headphones. Anything that happens on the computer or on the phone must take place in an open family space.

Monitor mindfully

It may be tempting to ban everything on the internet or lockdown apps, but inflexibility breeds angst. Digital discovery is a time for learning, so resist the temptation to block apps. Instead, allow children to practice being safe online. A monitoring program can be a practical part of the digital safety solution, but be sure to include your child in the decision-making.

If you do use monitoring software, use the activity metering. Tracking the amount of time and content of any given online experience shows patterns of behaviour. If a conversation needs to happen with a child spending too much time on a game, for example, a graphic comparing one week to another is far more helpful than your hunch about time spent.

Protect personal information

Children should be acquainted with several methods to shield data including understanding the importance of creating strong passwords with a variety of letters and characters. Devices can be further secured with unique passphrases and with touch ID. Make sure your family has a safe place to store password phrases. I recommend a password manager like Dashlane to not only secure passwords but also make them easier to share with a trusted family member.

Continually reinforce that your child never shares their school name, last name, location, age, birth date or other personal information. It is easy for children to slip up, especially when they've developed online friendships. If they cannot be mature enough to protect identifying details, they are not ready to participate unsupervised in these social platforms.

Navigating network settings

Children should have a fundamental grasp of the home network settings. They should know the boundaries for public Wi-Fi and non-secure networks. Have credible antivirus software with firewall protection on your home computers. Routinely change your router passwords and make sure to disable the household router hotspot upon setting up. Use the appropriate security protocol recommended when setting up your router and if you are unsure what WEP, WPA and an "Open Network" mean, now is the time to talk with technical support right at the beginning so that you and your family understand what the settings mean and why they are in place.

The internet is not a reality

Continually reinforce that the internet and social media do not accurately represent reality. State time and time again that people on the internet cannot be trusted regardless of how long they've been your internet "friend." While your child might be honest and polite on the web, not every person will act this way and if they do, that is not necessarily confirmation of a person's intent.

Openly discuss that addiction to social media is real and how easy it is to be enamoured with the utopia some online communities portray. Teach children how to limit screen time. Try using a simple kitchen timer for 30 minutes of concentrated study time without checking social feeds. If 30 minutes is too much, start smaller, and work your way up.

Set an example

Above all else, practice what you preach and put the same guardrails on your own behaviour. For example, if phones are off-limits during mealtime, yours should also be put away. If you routinely eat a meal in front of your computer, consider the example you're setting for your children. Be willing to talk about your own struggles and take steps to actively show your children your desire to be an accountable digital citizen.

It's a challenge all of us face, but as technology continues to shift, so will our tactics to control any adverse effects on our lives.

In this day and age, when technological advancements are gained by the second, digital skills are fundamental for success. Now more than ever before, children need to pinpoint and prepare for the possible risks, from laptops to mobile phones and tablets. And as children grow, their knowledge regarding online safety, security, and social experience also need to expand.

Keep in mind that we are not all experts just because we work in tech. Whether you code for a living or you are simply not confident on computers, we are all learning together. Likewise, keep in mind the saying "if in doubt, shout" — because no one should ever be afraid to ask for help.

About the Author

Author: Al Kingsley

Al Kingsley is the CEO of NetSupport. In his newly released book, My Secret #EdTech Diary, Kingsley shares the potential of technology to improve our schools for students and educators. The book is also a look at pre- and post-Covid EdTech, offering practical advice and insights. The book is published by John Catt Educational and is available on Amazon.