Internet Safety Tips for Parents

1. **Establish an ongoing dialogue and keep lines of communication open:** Spend time online alongside your children and create an atmosphere of trust. Encourage your children to make good choices.

2. **Supervise the use of all Internet-enabled devices:** Keep your child's computer/laptop in an open area of your home. Monitor other points of Internet access including your child's cell phone, portable music device, smart TV, and gaming devices.

3. **Know your child's online activities and friends:** Be familiar with each of your children's passwords, screen names, and all account information, and have them provide the identities of every person on their buddy list or anyone they have "friended" on social networking or gaming sites.

   a. Caution your children to only communicate online with people they know in-person and who have been approved by you. Remind your children that the people they meet online may not be who they say they are.

4. **Regularly check the online communities your children use, such as social networking and gaming sites, to see what information they are posting:** Make sure you, as the parent, are added to your child's "Friend list," because if their profiles are set to private (as they should be!) you will not be able to view any of their information. If you are unsure whether your child has a profile, conduct a simple online search through the site or by typing their name into a search engine (e.g., Google).

   a. Be aware of not only what your children are posting, but what other kids are posting about your children. Before allowing children to use social media sites, familiarize yourself with the content on the site and thoroughly review the safety practices and privacy tools available through that social networking site.

   b. Popular social media sites include Facebook, Twitter, LinkedIn, Pinterest, Tumblr, Instagram, and Zoom among many others. Many such sites have a minimum age limit of 13 years old but do not have age-verification technology to keep younger children from lying about their age.

5. **Supervise the photos and videos your kid's post and send online and through their mobile device:** Photos and videos can be uploaded instantly to sites like YouTube, Facebook, and many others from any platform with Internet access including your child's cell phone, webcam, and gaming device. These images may make your child vulnerable to online predators, cyberbullies, and strangers, or lead to damaged reputations.

   a. Check with your child's school to ensure that any projects, art, or photos placed on the school website are only accessible by password (or through the school's intranet) and do not contain any personally identifiable information. Younger children should not post, text or send photos or videos.

6. **Monitor the use of webcams and mobile video devices:** Most computers, cell phones, and other mobile devices now come with a built-in webcam and video devices, but videos and webcams should only be used under closer parental supervision, particularly with kids younger than grades K-8.

   a. Videos should be only sent to trusted friends and family. Be especially careful allowing kids to use webcams in private areas. Monitoring technology is particularly useful in establishing accountability with your child regarding the use of video technology.

7. **Teach your children how to protect personal information posted online and to follow the same rules with respect to the personal information of others:** Remind your children to think before they post – there are no takebacks online. Nothing is truly private on the Internet; any and all information sent or posted online is public or can be made public.

   Caution your children about posting:

   - PERSONAL OR CONTACT INFORMATION: Your child's full name, address, phone number, passwords, and financial information should only be provided on a secure site under parental supervision.

   - INTIMATE PERSONAL INFORMATION: Private, personal, and sensitive information (such as a teen's journal) should not be posted and should only be shared in private e-mails with a trusted, personal friend.

   - REPUTATION-DAMAGING INFORMATION OR IMAGES: Inappropriate pictures (i.e.., content that is explicit, suggestive, illegal, etc.), should never be posted or sent.1

   - EVENT INFORMATION: Teach children to use caution when posting information about parties, events, or activities where someone could track them down

8. **Be sure your children use privacy settings:** Privacy settings limit who can view your teen's profiles. On most social networking and gaming websites, your teen can change his or her privacy setting by clicking on "account settings."

   a. Ask your teens to show you the account settings or, if you have access to your teen's account, you can check their settings for yourself. Remember that no one can detect a

disguised predator, and even using these settings does not always achieve true privacy; all your child's friends have access to and could distribute any material included on their profile.

9. **Instruct your children never to meet face-to-face with someone they only know online or through their mobile device:** Online and mobile 'friends' may not be who they say they are. Children should be advised to come to you if anyone makes them feel scared, uncomfortable, confused, asks for any personal or personally identifiable information, or suggests meeting them.

10. **Establish an agreement with your children about Internet use at home and outside of the home:** Remind them that rules for good behavior don't change just because they're on a computer.

Taken from www.internetsafety101.org & credited to Enough Is Enough® (EIE).