BUILDING SAFETY IN THE DIGITAL WORLD

TIPS FOR PARENTS

Brought to you by Lauren's Kids and the Broward County Sheriff's Office

DID YOU KNOW?

- 1 in 5 children are solicited sexually through the Internet before their 18th birthday.
- Access to the Internet and digital devices should first and foremost be treated as a privilege, not as a right. Allowing a child access to the Internet without very strict oversight would be like allowing that same child to travel overseas without a parent or chaperone.
- Each Internet-capable device acts as an open door for millions of people directly into your or your child's life. Multiply that by the number of devices in a normal household and the potential for harm is staggering.
- Gaming systems, deactivated cell phones, iPods, and other such digital devices can also access the internet over WiFi. Many games, even those that cater to young children, give players access to servers where they are exposed to other players who can communicate with them through gameplay and chat features.

STEPS TO DIGITAL SAFETY

Step 1: Prior to giving any Internet-capable device to a child:

- Conduct a thorough investigation into that device's capabilities.
- Ensure you are the primary user/administrator and that at no time can a password or setting be changed or an application downloaded without your approval. Do not give your child your administrative password.
- Set up the device to only allow children access to a specific set of websites or applications. These settings vary from device to device. Ask the retailer where the device is purchased for specific information about your device.

Step 2: As the device administrator, you must be present every time an application is downloaded or a game set-up is conducted. This way, you know exactly what each application is capable of doing and can choose the most appropriate settings. Changing settings at a later time is always more difficult. Research each and every application/game prior to installing it.

Remember, just because your child's friends have an application or game does not mean it is safe.

- Some applications require location settings be turned on at all times or contact lists be shared. This allows other users, many times strangers, to know the exact location of your child or who their friends and relatives are.
- Some games allow access to PvP (player vs. player) scenarios where players can communicate with each other verbally (over headsets) or by typing messages to each other.
- Some settings, in something as innocent as the camera, can allow someone to determine the exact time and location a photo was taken after it is posted on social media.

This information may seem harmless, but it is important to realize that child predators seek out victims to groom on these platforms every single day because they allow for instant access to children and provide the ability to shield one's true identity.

Step 3: The constant monitoring of children's devices is one of the most effective ways to protect them and others. Parents usually report having no idea that their child has been involved with – or even sending photographs to – strangers online. It is natural for children to want privacy and autonomy, and to attempt to shield online activity from their parents. But if parents are diligent, they will be able to spot signs of unsafe use of the Internet before problems occur. Your child may get angry or upset about your monitoring of their devices, but remember that it is your job to keep them safe.

- Monitoring devices will not only keep them safe from unsafe adults, but will also ensure your child is not engaging in any type of cyber bullying activity or being the victim of cyber bullying themselves.
- Before you grant your child access to any Internet-capable device, create a contract with your child stating that as their parent, you will protect them.
- All of their devices will be subject to monitoring by you at any time, and if the request is refused, the device will be forfeited. If this rule is established from the beginning and reinforced throughout their childhood, it will be less likely you will receive resistance from your child since device checks will be conducted regularly.
- Create a reminder on your calendar to check your child's devices and apps on a regular basis. Children are children and they will make mistakes, especially when unsupervised – so you must remain vigilant.
- Being "friends" with your children on social media should not be considered an alternate option for checking devices. Many times, children will set up multiple accounts on the same social media platform they use to communicate with other people, or they will use settings to limit your visibility into the content they post.
- Do not share any digital or Internet-capable device's password with your child. Providing the child with the password can, depending on the vigilance of the parents in monitoring devices, allow the child to change device settings and provide the ability to download applications/programs. While it is inconvenient for the parent to constantly enter passwords for their child, it is necessary to ensure their safety.
- Consider the following when providing your WiFi password to those outside your family: Your IP address can be used by others to download illegal content over your WiFi. If an investigation is conducted, your IP address will be linked to the download.
- Use a post-it note or sticker to cover the webcam that is present on most laptops and some gaming systems when the cameras are not being used to avoid the possibility of it being covertly activated.

AS CHILDREN ENTER THE DIGITAL WORLD, PARENTS AND CAREGIVERS MUST BE VIGILANT. ULTIMATELY, YOU ARE – AND NEED TO BE – THE FRONT LINE IN THEIR DIGITAL SAFETY.