

TECHNOLOGY BOUNDARIES ACTION PLAN

Keeping Up with the iKids

Use the table below to write out the boundaries you want to put in place for your child's technology and internet use. Consider the seminar discussion, your personal judgment and input from family members to decide what is best for your family.

	Computer / General internet	Social media	Smartphone	Other devices (tablet, video game consoles, etc.)
When will you let them start using it?				
What time limits or other rules will you set?				
What times or places is it not OK to use it?				
What alternatives can you suggest for balance?				

Together, all the way.®



All Cigna products and services are provided exclusively by or through operating subsidiaries of Cigna Corporation.
Use and distribution limited solely to authorized personnel. 857168b 04/24 © 2024 Cigna

ONLINE SAFETY RESOURCE LIST

Keeping Up with the iKids

The websites below offer tips, information, and resources for families in the digital age. Many offer greater detail on topics discussed in this seminar.

The Digital Wellness Lab www.digitalwellnesslab.org/family-guides offers a wide range of information and tips for parents on protecting and educating children on a wide variety of media. Click on the “Resources” tab for age-specific Family Digital Wellness Guides.

Common Sense Media www.commonsensemedia.org/articles has many articles on all types of digital issues, including reviews of apps and video games, advice related to technology issues, and tools for teaching children.

ConnectSafely.org www.connectsafely.org has educational resources about evolving technology and social media. It has several “Parents’ Guides” on topics such as Snapchat, gaming, and cyberbullying.

NetFamilyNews www.netfamilynews.org offers access to a wide variety of news, studies, and commentary about children and digital concerns.

Netsmartz.org <http://netsmartz.org> has interactive and educational resources designed to teach kids and parents how to stay safe online. They have games and comics designed specifically for kids at different age levels.

StaySafeOnline.org www.staysafeonline.org/resources covers a variety of topics, from viruses to identity theft online to parenting tips for raising engaged and responsible digital citizens.

NOTE: If any of the links don’t work for you, copy and paste the URL into your browser.

Together, all the way.®



Any reference to the products, services, information or websites of any other non-Cigna affiliated entity is provided for informational purposes only and should not be construed as an endorsement by Cigna of the products, services, information, or websites of such entities, nor should such reference be construed as an endorsement by such entities of the products, services, information or websites of Cigna and/or its affiliates. Cigna neither reviews nor controls the content and accuracy of these references or websites, and therefore will not be responsible for their content and accuracy. Your access to non-Cigna web sites is at your sole risk.

All Cigna products and services are provided exclusively by or through operating subsidiaries of Cigna Corporation.
Use and distribution limited solely to authorized personnel. 857167c 04/24 © 2024 Cigna

TECHNOLOGY REFRESHER

Keeping Up with the iKids

It can be hard as a parent to stay on top of what apps and sites are popular with kids. Below is an overview of sites used by many teens and preteens, as well as some common terms and online threats. It's not exhaustive, but can give you a basic understanding of what your kids may be using or seeing online. Remember, the best resource for learning about the current technology is your kids! Ask them what they use, their favorite sites, and what their friends enjoy.

Social networking sites

Instagram: Instagram is a photo sharing app that allows users to take photos and videos on their smartphone and share them with others. Aside from its popularity among teens, the service also stands out because of the many unique "filters" that users can apply to their photos to give them a new look.

Snapchat: Remember "Mission: Impossible"? Well, Snapchat messages can be set to self-destruct 1-10 seconds after being sent. This can be a fun way for teens to share without their content being "out there" on the internet or a friend's phone. Snapchat also has a "stories" element where you can keep a running set of public snaps for 24 hours. It's important to note that while the snaps self-destruct, the app allows people to take a picture of the screen (screen shot) in order to have a saved copy.

TikTok: This mobile-based social media platform is designed for creating, sharing, and viewing short videos, often set to music or with added sound effects. Users can follow, like, and comment on other users' videos. Many "viral videos" were originally created on TikTok. Content topics vary widely, but the site is increasingly being used to promote products.

Reddit: Billing itself as the "front page of the internet," this website is more of an online forum than a social network. All content is shared by registered users. It includes photos, videos, news articles, and discussions on anything you can find on the internet (for better or worse). Content is organized into separate "subreddits." Moderators work to keep content in each subreddit appropriate to the topic. However, like the internet itself, Reddit contains items on a wide variety of different topics. Some of them may include explicit material (even on the home page) that would be inappropriate for a child.

YouTube: YouTube is the most popular video sharing site. People can upload their own videos, generally less than 10 minutes long, onto YouTube. Top channels include official music videos, original comedy, and videos of people playing, reviewing, and/or reacting to video games (like Minecraft). When someone refers to a "viral video," it is almost always a video on YouTube that has been seen and shared thousands of times in a short period.

Facebook is still the world's most popular social networking site. On Facebook, you can add "friends" and then see their updates. Status updates, pictures, videos, links to websites that your friends share all appear in your "news feed." You can comment on or "like" almost anything that your friends share. Organizations, from businesses to music groups, can start "pages" which people can "like." Updates from the organization can be seen in one's news feed.

X formerly Twitter: On X, people post updates or share links using up to 280 characters per entry. Anyone on the platform can "follow" anyone else, depending on the user's privacy settings, meaning they can subscribe to anyone's updates. The posts shared by individuals, groups, and organizations have been called "tweets," but the name is evolving. It's common for people to follow celebrities, bands, or news networks.

Forms of interpersonal communication online

Posting/commenting. Most social media websites focus on posts. You can post your personal status, post a note on your friend's page, or post links or pictures. Once posted, your friends, friends of friends, or anyone can view what you've posted, depending on your privacy settings. They can also comment on your posts, creating a sub-post that is also viewable by anyone who can read the original post.

Chat/Instant Messaging, like email, is an exchange of electronic messages online. However, both sender and receiver must be online at the same time to be involved. With the rise of always-online smartphones, messaging apps are often used as a way to stay connected either in addition to (or instead of) texting.

Video chat is speaking with someone else through a computer using a webcam so that both people can see each other. It is available through a few different platforms, including FaceTime, Google+ and Skype. It requires both a webcam and a microphone so that you can see each other and speak.

TIP: Technology evolves quickly. It may be helpful to focus on key features when researching a new social networking site, app, or gaming environment.

- › Is it anonymous or partially so?
- › Do messages or videos disappear after being sent?
- › Can you monitor usage easily?
- › How easy it is to delete items?
- › How much privacy will your child have; do you have control over the privacy settings?

Threats on the internet

Keep in mind that kids can access the internet in a variety of ways. When reviewing safety, consider gaming systems, e-readers and smartwatches, in addition to phones, tablets and computers.

Viruses are files that you download to your computer, usually from an email or a website. They are harmful and can cause your computer to slow down, freeze, or crash. Keeping your computer's security software up to date and not clicking on strange links (even if they are sent from people you know) are the best ways to avoid getting viruses.

Keyloggers are a type of virus that can infect a computer or mobile device. They are usually created and distributed with criminal intent and will monitor keystrokes and relay information back to the hacker. These can put passwords for email, banking information, credit card information, and/or online shopping accounts (Amazon, etc.) at risk. Like any other virus, they can be avoided and treated with careful computer use and antivirus protection. Banking activity that you didn't do or a hacked email account could be signs that a keylogger has infected a device.

Adware/Spyware refers to files that are downloaded to your computer without your knowledge, usually from websites. They don't usually do damage like viruses but can still slow down your computer. These files track your internet browsing habits for the sake of advertising to you. There are free programs that you can download that will find and eliminate spyware from your computer.

Spam or junk email is email received from people you don't know. It's often filled with poor grammar or is in another language. It is sent to many people at the same time. It can include ads, often for medications or explicit material, malware (links to viruses or other files meant to harm your computer), and phishing or other scams.

Phishing is a scam which is used to obtain personal information such as usernames, passwords, bank accounts, social security numbers, etc. by posing as a trusted person or organization. This can often be done using emails sent from fake email addresses that are made to look like real people, but sometimes the same tactic is used with websites. As a general rule, do not give out personal information on the web.

Any reference to the products, services, information or websites of any other non-Cigna affiliated entity is provided for informational purposes only and should not be construed as an endorsement by Cigna of the products, services, information, or websites of such entities, nor should such reference be construed as an endorsement by such entities of the products, services, information or websites of Cigna and/or its affiliates. Cigna neither reviews nor controls the content and accuracy of these references or websites, and therefore will not be responsible for their content and accuracy. Your access to non-Cigna web sites is at your sole risk.

All Cigna products and services are provided exclusively by or through operating subsidiaries of Cigna Corporation.

Use and distribution limited solely to authorized personnel. 857166c 04/24 © 2024 Cigna

