# A Parent's Guide To Current Social Media Apps

July 2020

Children's
ADVOCACY & PROTECTION CENTER
OF CATAWBA COUNTY

# Currently Used Apps
# (In Alphabetical Order)

**Purpose: Amino - Communities, Chat, Forums, and Groups** is an interest-based app that lets users find people who are into the same things. Teens can join groups -- or create them -- and then post within the group, follow other users, and chat with them via text, voice, or video.

**What parents need to know:** Contact with strangers is part of the experience. While it's great for kids to be able to feel a sense of belonging and kinship with others, the mix of kids and adults blended with all varieties of chat makes it risky. Also, unless a kid is in a closed group, everything they post is public, and other users can search for them. Make sure your kid's location is not included in their profile. Mature content and bullying is common. Since each community makes its own rules, profanity, sexual references, and violent content are a part of some forums. A lot of what your kid sees, who they meet, and what people post is determined by the groups they decide to join, as some are very tame and some are definitely not for kids**. It's not made with kids in mind.** Because this app wasn't created for kids, it doesn't have the same safeguards or privacy standards as apps that are made for kids.

**Purpose: ASKfm** - This app allows users to interact in a question-and-answer format — with friends, peers, and anonymous users alike.

**What parents need to know:** The app is rated ages 13+ and is most popular in Europe but is catching on in the U.S. Some kids have used the app for hurtful cyberbullying that has been linked with suicides. British schools have sent home letters calling for students to stop using ask.fm because of its use in several cyberbullying incidents there, and its loose regulation and lack of monitoring. In response to the uproar in the U.K., the site added a button where users can report abuse, but some parents feel it's too little, too late.

**Purpose: Badoo** is also a location-based social service. It's designed to help you find people nearby who share your interests, and there's a strong smartphone app. Users can chat and share photos and videos. It's pitched as great if you're looking to hang with someone in a new city you're visiting, or connect with people at an event.

**What parents need to know:** Badoo is an adults-only app for online dating-style social networking. It includes features standard on most social media platforms have available, including live streaming. Users are able to block other users. However users can't hide their profile completely. The app identifies the location of a user by tracking his or her device's location, and then matches pictures and profiles of potentially thousands of people the user could contact within the surrounding area.

**Purpose: Bigo** is a live streaming app. It is rated for teens 17 and up. Users can vlog about their lives, live stream video game play, and host their own shows. Anyone can broadcast videos anytime and anywhere, and connect to anyone.

**What parents need to know:** This is a place where bullying, nudity, violence, and profanity is common. Primarily used by gamers, aspiring performing artists and vloggers, the app requires a minimum age of 16 for to set up an account. However, younger users can trick the AI system to get in, especially when they have a burning desire for fame and popularity. A significant risk of Bigo Live is that some user-generated content can include bad language, violence, or nudity, including sexy talk and clothing. Also, users' comments are often predatory, explicit and bullying. Sharing personal information in-app (like age, gender, and location) is not safe for younger teens. The gamification system within the app (levels and ranks, awards for signing in every day) may lead to addiction, and the constant competition to receive "beans" can distort a user's image of what talent and value mean. The app also facilitates interactions with strangers, possibly predators and stalkers.

**Purpose:** **Bumble** is a location-based social application that facilitates communication between interested users. In heterosexual matches, only female users can make the first contact with matched male users, while in same-sex matches either person can send a message first.

**What parents need to know:** Tweens and teens have been known to lie about their age and create fake accounts on apps like Bumble. The Bumble app makes it easy for predators to target victims. Connections expire every 24 hours which encourages users to check the app daily. Bumble markets itself as a place for dating, friend-finding, and career building, so the motives of the app can be confusing for younger teens. Cyberbullying, inappropriate language, and harassment are prevalent in private messages sent on the app.

**Purpose: Chat Avenue** allow users to converse in real time rather than posting through emails or forums which can result in a delayed response.

**What parents need to know:** Like its name says, the chat room website created in 2000 hosts various themed rooms like, Gay Chat, Teen Chat, Singles Chat and more. A user can create an account or start chatting as a guest with just a username.

**Purpose: Discord** started as a place for gamers to chat while playing video games but has become a bigger platform where users can use text, voice-chat, and video-chat to discuss a wide variety of topics.

**What parents need to know:** There are public and private "servers" or discussion groups. Teens can join public groups, ask to join private ones, or start their own. The safest option is for them to join a private group with people they know in real life**.** Some groups are more moderated than others, some are NSFW, and some are hate-filled**.** There are plenty of groups that are meant for adults only, and some are totally tame and well moderated. If your kid is in one of the latter, the risk is much lower.

**Purpose: Grindr** is a mobile-location based dating app for men and gender non-conforming people on the LGBTQ+ spectrum, and using it is as easy as making an account and starting to chat with others on the app.

**What parents need to know:** This is a same-sex dating app that has led to a shocking number of child sexual assaults. No child **should** ever use this app. If this is on your child's phone, you need to have a conversation with your child about his sexuality and the danger of meeting up with adults for casual sex.

**Purpose: GroupMe is** an app that doesn't charge fees or have limits for direct and group messages. Users also can send photos, videos, and calendar links.

**What parents need to know:** It's for older teens. The embedded GIFs and emojis have some adult themes, such as drinking and sex. Teens are always connected. Without fees or limits, teens can share and text to their heart's content, which may mean they rarely put the phone down.

**Purpose: HOLLA** - A Live Random Video Chat is a free premium social networking app that lets users conduct live video chat sessions with random strangers.

**What parents need to know:** Users are meant to be 18 years old to use the app, but fake accounts can be created easily. While meeting strangers online might sound fun to children, parents should be aware of the risks. Trolling, racism, and bullying are sometimes evident.

**Purpose**: **Hot or Not** is a rating site that allows users to rate the attractiveness of photos submitted voluntarily by others. The site offers a matchmaking engine called 'Meet Me' and an extended profile feature called "Hotlists".

**What parents need to know:** Even though Hot or Not has made claims that underage users are separated from adults, they have no method of actually verifying the said ages of users. So it's certainly impossible to guarantee that children won't have access to adults on the app. Predators can easily make a fraud profile and sign up as a minor to acquire the privilege to get access to the age group of "protected" teen account holders. Due to this loop, teens can fall victim easily to pedophiles and predators faking to be teenagers. Once they are connected to one another, it's very easy for your child to be open to explicit content via the apps feature for private messaging. Teens as well can be matched easily on this app and start very inappropriate conversations or picture exchanges. People will be given access to prey on children knowing that they are close by, since this is a location-based application. The aim of this application is to judge superficially, the physical appearance of its members. It's more than likely that children who are a part of this app can get hurt and upset about their rating on Hot or Not and as a result suffer from extremely low self-esteem.

**Purpose: Houseparty** is a video chatting app that's pretty open. Friends can communicate with each other through live video and texts in chat groups. Two to eight people can be in a chat together at the same time. If someone who's not a direct friend joins a chat, teens get an alert in case they want to leave the chat. You can also "lock" a chat so no one else can join.

**What parents need to know:** There's no screening and the video is live, so there's nothing to keep kids from inappropriate content. Users can send links via chat and even take screenshots. There's also nothing keeping friends of friends joining groups where they may only know one person.

**Purpose: IMVU** - This is a virtual world game like SIMS. Users interact with each other as avatars. IMVU stands for Instant Messaging Virtual Universe.

**What parents need to know:** There is nudity and sexual encounters in areas that are for 18+, but there is sexual talk and behaviors in the regular area of IMVU as well. There is a Chat Now feature that randomly pairs users with other users and can lead to inappropriate pairings and interactions. All profiles are public, and there can be bullying and predators trying to get other users to share their phone numbers and to send pictures.

**Purpose: Instagram** lets users snap, edit, and share photos and 15-second videos, either publicly or within a private network of followers. It unites the most popular features of social media sites: sharing, seeing, and commenting on photos. It also lets you apply fun filters and effects to your photos, making them look high-quality and artistic.

**What parents need to know:** The app is rated 13+, but users can still find mature or inappropriate content and comments throughout the app (there is a way to flag inappropriate content for review). "Trolls" — or people making vicious, usually anonymous comments — are common. A user can change the settings to block their location or certain followers, but many users are casual about their settings, connecting with people they don't know well or at all. Teens are on the lookout for "likes, and they may measure the "success" of their photos -- even their self-worth -- by the number of likes or comments they receive. Photos and videos shared on Instagram are public unless privacy settings are adjusted. Hashtags and location information can make photos even more visible to communities beyond a teen's followers if his or her account is public. Kids can send private messages. Instagram Direct is like texting with photos or videos and you can do it with up to 15 mutual friends. These pictures don't show up on their public feeds. Although there's nothing wrong with group chats, kids may be more likely to share inappropriate stuff with their inner circles.

**Purpose: Kik** is a mobile app that people can use to text with friends at high speed and with more of a "face-to-face feel" than regular texting (users' profile pictures appear in a little bubble next to their text, and they can quickly text photos, sketches, or even pre-designed greeting cards to individuals or groups).

**What parents need to know:** The app is rated ages 17+, but there is no age verification so anyone can download it. Like some other instant messenger apps, Kik allows your teen to connect with others using just a username (rather than texting from her phone number). Stranger danger is an issue. Kik allows communication with strangers who share their Kik usernames to find people to chat with. It's loaded with covert marketing. Kik specializes in "promoted chats" -- basically, conversations between brands and users. It also offers specially designed apps (accessible only through the main app), many of which offer products for sale. Reviews in the App Store and Google Play store reveal that many people use Kik to meet strangers for sexting. The app has also been connected with cyberbullying.

**Purpose: LiveMe** - Users can stream live video of themselves to an anonymous audience of fellow users. Those users can post comments, earn currency from fans, and interact live with users without any control over who views their streams.

**What parents need to know:** Even though the app's terms and conditions prohibit sexually explicit content, hate speech, bullying, illegal activity and more, it's clear that the moderators don't manage to catch everything. Like other websites, negative and even dangerous behavior can slip under the radar and put young people in danger. Not only is LiveMe a potential hunting ground for sexual predators, the location services "…can be used to pinpoint exact locations—within 10 feet." Furthermore, many young users are careless about sharing personal information: they gladly answer requests for their addresses or their phone numbers.

**Purpose: Look** is a free video messaging app. Users can send video (of course), texts, emojis and gifs. They can also draw on and use filters on their videos.

**What parents need to know:** With Look, strangers can message kids pretty easily, and because there are no content filters, kids can come across inappropriate content. Users have reported cyberbullying activity and have found it difficult to delete their accounts.

**Purpose: MeetMe** - To allow strangers to interact and meet online. Although not marketed as a dating app, MeetMe does have a "Match" feature whereby users can "secretly admire" others, and its large user base means fast-paced communication and guaranteed attention.

**What parents need to know:** It's easy to see what makes this app so dangerous for teenagers. Despite being advertised as an easy way to make "new friends," MeetMe is regarded as a dating app. Users are encouraged and even rewarded to view profiles of the opposite sex. Although the app states that users must be at least 13, there is practically no age-verification process to keep this in check. With MeetMe Credits, users are encouraged to perform various tasks on the app. This gives the app an "arcade-like" feel; teens may forget that their actions on the app have very real, real-world consequences. They can become so caught up winning the app's games that they forget they are playing with real strangers. MeetMe possesses an "open-door" policy in regards to its user profiles. There are no privacy settings; every detail your teen adds to their personal profile will be present for anyone to see. The app encourages users to be very open and share personal details to "help" them build connections with fellow users. It's very common for sexually explicit and even pornographic material to find its way into user news feeds.

**Purpose:** The **Monkey** app is a video chat app that randomly matches people with other users on the platform for a brief 15-second video call. The platform uses their Snapchat usernames and mobile numbers to connect to the service and run matches while also allowing users extra time to continue a connection. Group video chats are also available in the app to allow multiple users to chat at the same time. Additionally, one can also post a “moment” which can be seen by their followers.

**What parents need to know:** The Monkey app aims to cater to the kids. However, the app does not come with any kind of age verification. And while many believe that an app that caters to teens should have some kind of age verification method in place to be able to offer a safer environment for the kids, Monkey app doesn’t provide any of it. The app claims that it offers 24/7 content moderation to protect its users; however, it does not provide any real privacy. This is because kids who use the application are asked to share a number of personal details, including their name, profile picture, date of birth, user-contributed content such as the images, texts, videos, and screenshots that have been shared with other users. In addition, they are also asked to share automatic information, which is their browser, I.P. address. All such details and data have been covered in the App’s Privacy Statement with different levels of protection.

**Purpose: Omegle** is a free online chat website that allows users to socialize with others without the need to register. The service randomly pairs users in one-on-one chat sessions where they chat anonymously using the names "You" and "Stranger" or "Stranger 1" and "Stranger 2" in the case of Spy mode.

**What parents need to know:** Without an effective age gate, underage users can use the site by pretending to be adults. Though it’s said that all the content on the site is unregistered, all chats are stored in a server. If someone shares any personal information (phone number, address, email), their data is stored. Everything that the users disclose about themselves is archived on the website's servers for about four months. Age, sex and location - these are valuable filters on Omegle. Unfortunately, this information can also be used by adults with malicious intentions to identify potential targets. It is filled with people searching for sexual chat. Conversations with strangers can be monitored or unmonitored, depending on the user's preference. But while ‘unmonitored’ might seem the obvious way to go, note that users are warned by Omegle of a greater possibility they will find themselves at the receiving end of explicit and inappropriate content when initiating an unmonitored conversation. Omegle added a dangerous feature that allows an user to capture a screenshot of the conversation. Users can even enter into what is known as 'Spy Mode' in Omegle. In ‘Spy Mode’, they can ask a question to two people engaged in a chat conversation and also view their conversation. Alternatively, the 'Spy Mode' feature also allows a user to discuss with another person a question posed by a stranger.

**Purpose: Paltalk** is a proprietary video group chat service that enables users to communicate via video, internet chat and voice. It offers chat rooms and the ability for users to create their own public virtual chat room.

**What parents need to know:** The platform requires users to be at least 13 years old with parent's permission. Parents and Guardians assume all liability.

**Purpose: Periscope** enables you to “go live” via your mobile device anytime and anywhere.
The app enables you to become your own “on the go” broadcasting station, streaming video and audio to any viewers who join your broadcast.

**What parents need to know:** There are definite safety concerns when it comes to Periscope, including cyberbullying, sexual harassment, and potential access to your child's location. Since Periscope isn't monitored, its users are often free to behave however they choose.

**Purpose: SKOUT** is a location-based dating app and website. SKOUT was one of the first dating and mobile people discovery applications to emphasize generalized user location.

**What parents need to know:** Skout is supposed to prohibit people under 17 from sharing private photos. However, police say kids can easily create an account with a different age. Skout is a flirting app used to meet and chat with new people. Based on the age entered at registration, teens and adults are assigned to different groups, but ages aren't verified. Once teens turn 18, they're automatically moved into the adult group, but it's easy to enter a false birthday at registration and pose as either an adult or a teen. In 2012, the teen app was briefly suspended to tighten safety protocols. As a result, a teen's exact location isn't revealed, only a general region, and posts are now more closely monitored. Also, teens can't send pictures in private messages. They can earn points for using the app and responding to ads. Then they can redeem points to reveal the profiles of users who've "checked" them out or to access users in other geographic areas. Posts include plenty of profanity and suggestive pictures.

**Purpose: Snapchat** is an app that allows users to send photos and videos that disappear after they're received. It's rated ages 12+. The filters and special effects allow users to alter pictures.

**What parents need to know:** Some kids are using the app to send racy pics because they believe the images can't be saved and circulated. Data is data: Whenever an image is sent, it never truly goes away. (For example, the person on the receiving end can take a screenshot of the image before it disappears.) Snapchats can even be recovered. And while recent studies revealed that "sexting" (sending sexual messages and images, usually via text message) is not as popular as parents had feared, "disappearing photo" apps like Snapchat might embolden kids to send more explicit photos and texts than they would have before through traditional texting.

**Purpose: Tellonym** - This is an anonymous messenger app. It calls itself "the most honest place on the internet." This app is extremely popular in middle schools and high schools and it allows kids to ask and answer questions anonymously.

**What parents need to know:** It is a regular occurrence to see cyber bullying, violent threats, and sexual content. It also offers unmonitored access to the internet. The age restrictions are inconsistent ranging from 12 to 16, but this app is inappropriate for anyone younger than being in their late teens.

**Purpose: TikTok** is an app for creating and sharing short videos. Users can create short music videos of 3 to 15 seconds and short looping videos of 3 to 60 seconds. It encourages users to express themselves creatively through video Special effects can be added to the videos. Users can build up a following among friends or share posts publicly.

**What parents need to know:** Thirteen is the minimum age, but there isn't a real way to validate age so anyone can download the app. Also, parents express concern that there is a lot of inappropriate language (swearing and sexual content) in the videos so it's not appropriate for young children. Lastly, by default, all accounts are set to public so strangers can contact your children. Many are highly motivated to get more followers and likes for their videos.

**Purpose: Tinder**'s developers describe the app as "the fun way to connect with new and interesting people around you." But it's mainly used as a dating tool or an anonymous hook-up (read: one-night stand) locator by 20-somethings, college students, and even younger teens and tweens.

**What parents need to know:** The app is rated ages 17+ but Tinder's privacy policy allows teens as young as 13 to register (the app connects with Facebook — which is also technically for ages 13+ — to pull in photos for users' Tinder profiles). Tinder helps people find others in their geographic location and allows users to view each others' photos and start instant messaging once both people have "liked" one another. The geo-location features and anonymous nature of the app put kids at risk for catfishing, sexual harassment, stalking, and worse.

**Purpose: Tumblr** is like a cross between a blog and Twitter: It's a streaming scrapbook of text, photos, and/or video and audio clips. Users create and follow short blogs, or "tumblogs," that can be seen by anyone online (if they're made public). Many teens have tumblogs for personal use: sharing photos, videos, musings, and things they find funny with their friends.

**What parents need to know:** Porn is easy to find. This online hangout is hip and creative but sometimes raunchy. Pornographic images and videos and depictions of violence, self-harm, drug use, and offensive language are easily searchable. Privacy can be guarded but only through an awkward workaround. The first profile a member creates is public and viewable by anyone on the internet. Members who desire full privacy have to create a *second* profile, which they're able to password-protect. Posts are often copied and shared. Reblogging on Tumblr is similar to re-tweeting: A post is reblogged from one tumblog to another. Many teens like -- and, in fact, want -- their posts to be reblogged.

**Purpose: Twitch** is an online site that allows users to watch or broadcast live streaming or pre-recorded video of broadcaster's video game gameplay. A Twitch broadcast often includes audio commentary from the player, and video of the player might appear on the edge of the screen via their webcam.

**What parents need to know:** Twitch and its user-generated content is not always the safest platform for kids. Live streaming is naturally unpredictable, which is part of the appeal for many viewers, but this makes it difficult for parents to monitor what their children are watching.

**Purpose: Voxer** - This walkie-talkie PTT (push-to-talk) app allows users to quickly exchange short voice messages. They can have chats going on with multiple people at a time and just have to tap the play button to hear any messages they receive. Although it largely has an adult following, including some people who use it for their job, it's becoming popular among teens who enjoy its hybrid style of texting and talking.

**What parents need to know:** Hurtful messages from cyberbullies can be even more biting when they're spoken and can be played repeatedly. Surprisingly, the app is rated ages 4+ in the App Store.

**Purpose: VSCO** is a photo creation app that gives users the tools to shoot, edit and post images to a profile, kind of like Instagram.

**What parents need to know:** You should know that you have to manually turn on privacy settings and limit location sharing. There are also in-app purchases for more serious photo editing tools that could cost you some serious money if your kid decides to download them.

**Purpose: WhatsApp** allows you to send messages, pictures, videos and even voice recordings, as well as make voice and video calls over the internet for free, rather than using your mobile network which costs you money.

**What parents need to know:** It's for users 16 and over. Lots of younger teens seem to be using the app, but this age minimum has been set by WhatsApp. It can be pushy. After you sign up, it automatically connects you to all the people in your address book who also are using WhatsApp. It also encourages you to add friends who haven't signed up yet. Kids can be exposed to inappropriate content and exchange inappropriate content with others.

**Purpose: Whisper** - This 17+ app's motto is: "Share Secrets, Express Yourself, Meet New People." Whisper **is** a social "confessional" app that allows users to post whatever's on their minds, paired with an image. With all the emotions running through teens, anonymous outlets give them the freedom to share their feelings without fear of judgment.

**What parents need to know:** Whisper lets users set up anonymous accounts to make their messages or confessions overlap an image or graphic (similar to e-postcards), which other users can then "like," share, or comment on. Whispers are often sexual in nature. Some users use the app to try to hook up with people nearby, while others post "confessions" of desire. Lots of eye-catching, nearly nude pics accompany these shared secrets. Content can be dark. People normally don't confess sunshine and rainbows; common Whisper topics include insecurity, depression, substance abuse, and various lies told to employers and teachers. Although it's anonymous to start, it may not stay that way. The app encourages users to exchange personal information in the "Meet Up" section.

**Purpose: Wishbone** is the go-to for comparing anything the heart desires! This is popular with teen girls. Wishbone covers everything from fashion, celebrities, humor, music and pretty much anything you can think about.

**What parents need to know::** Wishbone is a controversial comparison app that allows users to compare whatever they want to. A major concern is that it allows users to compare kids against each other and rate them on a scale. It is possible to use the app without revealing any personal information, but in choosing to link the app to other social media accounts, it is possible for Wishbone to accumulate a large amount of personal information from users. As it is a comparison tool, children could use it to compare each other and incite cyberbullying on the app. There is the potential risk of online grooming as adult users could target younger users and take advantage of their trust. If a child connects their Facebook or Twitter account to the app, it will collect information about their friends and those they have in common with on the Wishbone app. Users can send private messages to each other if they follow each other so it's important to make sure teens only follow 'real friends' rather than people they have never met.

**Purpose: YouNow** is an app that lets kids stream and watch live broadcasts. As they watch, they can comment or buy gold bars to give to other users. Ultimately, the goal is to get lots of viewers, start trending, and grow your fan base.

**What parents need to know:** Kids might make poor decisions to gain popularity. Because it's live video, kids can do or say anything and can respond to requests from viewers -- in real time. Though there seems to be moderation around iffy content (kids complain about having accounts suspended "for nothing"), there's plenty of swearing and occasional sharing of personal information with anonymous viewers. Teens can share personal information, sometimes by accident. Teens often broadcast from their bedrooms, which often have personal information visible, and they sometimes will share a phone number or an email address with viewers, not knowing who's really watching. It's creepy. Teens even broadcast themselves sleeping, which illustrates the urge to share all aspects of life, even intimate moments, publicly -- and potentially with strangers.

**Purpose: YouTube** is a place to house and share your videos. You can control privacy settings. It's also a great resource for educational videos and entertainment.

**What parents need to know:** Inappropriate content has been sliced into both all-ages content and children's content. Also, comments on videos can be extremely inappropriate and hurtful. YouTube also has a known pedophile problem which is major cause for concern. YouTube is a video-sharing site and app, and there are many videos on YouTube that may not be age-appropriate for their kids. The site is entirely user-generated and relies on its community to flag videos that violate YouTube's terms of service (mostly for sexual content, language and hate speech). Videos here run the gamut, from commercial to educational to music videos to homemade clips. Many kids love YouTube and rely on it as a way of keeping up with popular culture; videos go "viral" when viewers share the clips they like. YouTube does offer parents the ability to filter out objectionable content and comments using Safety Mode. However, Safety Mode doesn't catch everything, and it's easy to disable.

**Purpose: Yubo**, formerly Yellow, is a social media app encouraging teens to find new friends by allowing them to swipe left or right to connect or reject. If two people swipe right on each other, they can chat and hook up via Snapchat or Instagram.

**What parents need to know:** The App Guidelines do not state that profiles posting adult/inappropriate content will be removed. Also, there are allegations that the content is not properly moderated. Hence, Yubo runs the risk of hosting a collection of disturbing content your children could be exposed to.

# Jailbreak Programs And Icon-Hiding Apps

**Purpose:** These aren't social media apps — and they're confusing — but you should still know about them (especially if you have a tech-savvy teen or have had to take away your child's mobile phone privileges because of abuse).

**Why Parents Should Worry:** "Jailbreaking" an iPhone or "rooting" an Android phone basically means hacking your own device to lift restrictions on allowable applications — meaning, the user can then download third-party apps not sold in the App Store or Google Play store (read: sometimes sketchy apps). It's hard to say how many teens have jailbroken their mobile device, but instructions on how to do it are readily available on the Internet. Cydia is a popular application for jailbroken phones, and it's a gateway to other apps called Poof and SBSettings — which are icon-hiding apps. These apps are supposedly intended to help users clear the clutter from their screens, but some young people are using them to hide questionable apps and violent games from their parents. Be aware of what the Cydia app icons look like so you know if you're getting a complete picture of your teen's app use.

# Next Steps for Parents

1. Sit down with your child and find out which apps he/she is using, how they work, and whether he/she has experienced any issues on them, such as cyberbullying or contact from strangers.

2. Look into apps and products that help you monitor your child online.

- If your main concerns are web browsing and social media safety, there are several parental control apps that you can check out. Qustodio, OpenDNS FamilyShield, KidLogger, Spyrix Free Keylogger, Kaspersky Safe Kids, and Wondershare Famisafe are some of the recommended ones.
- If your main concern is filtering web content and setting internet time limits for multiple kids and/or devices, there are several options available. FamiSafe, Pumpic, Net Nanny, MMGuardian, Funamois, Kidslox, OurPact, Cedar Creek, Secureteen and Norton Family are some of the options.

# Tips for Protecting Your Child Online

- You can set up age limits on your child's device. The 2013 Pew Research Center survey found that nearly 40 percent of teens say that they have lied about their age to gain access to a site or create an account, so restricting kids' access to apps by age rating is a wise move.

- You can't join every site or app and monitor your child's every move online; teens will always find a new platform that their parents don't know about yet. Rather than hovering or completely barring your child from downloading every social media app, sit down and go over some general rules to keep him smart and safe online.

- Tell your child to let you know if someone is hurting him/her or making him/her feel uncomfortable online, even if the person is acting anonymously. The Cyberbullying Research Center's "Questions Parents Should Ask Their Children About Technology" is one guide to help with your discussion. https://cyberbullying.org/questions-parents-should-ask-their-children-about-technology. They also have a printable anti-bullying pledge and parent/child online agreement that might be useful tools. https://cyberbullying.org/resources/parents

- Make a rule that your child must ask for permission before downloading any apps — even free ones — just so you're aware of them. When your child wants to join a new social media platform, go through the security settings together to choose the ones you're most comfortable with. Advise your child not to share passwords with anyone, including best friends, boyfriends, or girlfriends.

# Some Tech Questions Parents Can Ask

- What method(s) do you use to connect to the internet? Let’s learn more about how that method works (e.g., watch a video online).

- Why do you think sharing personal information, like credit card numbers, over an unsecured network is risky?

- Why is it important to be careful about sharing our family’s Wi-Fi password?

- How are you using privacy settings to protect your information?

- Did you know that images may contain metadata telling when and where they were taken? Let’s see if your digital device/platform has a way to turn that off.

- Do you ever use location services to check-in to places? What steps are you taking to protect your location when you don’t want to share it?

- Have you ever felt pressured to share your password with someone? What did you do?

- Why is it important to have a different password for every account?

- How can we make sure your privacy is respected? How can we make sure I have the tools I need to keep you safe?

- What personal information are you cautious about sharing online?

- What clues do you look for to tell if a website/app/platform is trustworthy?

- What can you do if someone you’ve shared personal information with breaks your trust?

# Some Social Media Question Parents Can Ask

- Do you really know all of your friends on Facebook and followers on Twitter or Instagram? Have you ever accepted a friend request from someone you aren't sure that you know?

- Have you ever gotten a friend request from someone who is already your friend? And did you accept the second friend request anyway, but wondered what was going on?

- Do you know which bits of your personal information are publicly available (to people that you have not specifically "friended")? Have you ever checked out your page to see what it looks like to a stranger? Do you periodically check your privacy settings?

- Do you have any photos on Facebook or Instagram or Snapchat that you do not want your parents, your college's admissions officer, a future employer, or a future significant other to see?

- Do you take quizzes and surveys while on Facebook?

- When was the last time you changed your password?

- Does your password contain general words or phrases or place names or dates that you have posted online, or that are available in your social media profile?

- Do you use the same user name and/or password for multiple social media applications?

- Have you lied about your age to gain access to a social media application?

- Have you ever received a message (of any type), asking you to log in and verify something on one of your social media applications?