SMART PHONE SAFETY

SMART PHONES SAFETY RISKS

- Cyberbullying
- Geolocation
- Inappropriate Content
- Sexting
- Viruses & Malware

HOW KIDS USE MOBILE PHONES

The best way to find out how your kids are using their phones is to ask them. Activities popular with kids include photo and video sharing, texting, gaming and a growing number of social networking apps that are not limited to the ones you might have heard of, such as Facebook and Twitter. Apps come and go and technology changes, the parenting part hasn't changed much. You still need to ask questions and set limits.

8 Tips for Smart Smartphone Use

Share with Care. Use the same good sense about what you say or share with your phone as you would in person. Once shared, texts, photos, and videos are tough to take back. They can be copied and pasted elsewhere.

Know what your apps know. Pay attention to any permissions apps request as you install them. If an app asks to access your location, contact list, calendar or messages or to post to your social networking services, consider if the app really needs that information to function.

Share location mindfully. A growing number of apps let you share your location and track where friends are. If you use a location feature, think about who could see that and whether you want them to know where you are.

Phones are personal. Letting other people use your phone when you're not around is like letting them have the password to any of your social network accounts. They can impersonate you, which gives them power to mess with your reputation and relationships. Lock your phone when you're not using it, and use strong and unique passwords for all your apps.

Keep it kind. Cyberbullying can be mobile too. Treat people well on phones as you would face-to-face.

Avoid accidents. Never send or read texts while driving, bike riding and other activities that require your full attention.

Draw up a family contract. Use a family cellphone contract and talk with your children about why each point is important.

Find missing phones. Use a find-my-phone app that can help locate the phone and delete all personal data if it's lost or stolen.

"The best way to ensure that your children are using safe and appropriate apps is to talk with them about each app they use and do a little research to make sure it's appropriate for your child."

HELP KIDS PROTECT THEIR SAFETY, PRIVACY AND SECURITY

Limit who can locate you. All modern phones are equipped with geolocation technology that can pinpoint the phone's location. That can enhance safety and convenience by allowing parents to track kids, users to find lost phones and first responders to find people in an emergency. There are also app that use location or share it with other users or companies. With the exception of E911, it's possible to turn off geolocation, either for the entire phone or just specific apps.

Be app-savvy. When you're downloading apps, look at the reviews and pay special attention to the permissions they seek. Do a bit of Web searching to see if an app you're installing is from a reputable developer, and only download apps from offical sources like Google Play or the Apple App Store. Not all apps are appropriate for all users. You and your children should periodically review the apps on their phones together and consider deleting any that you're not comfortable with. There are also parental controls that can help you manage your child's use of apps.

APPS EVERY PARENT SHOULD KNOW ABOUT

Gone are the days of Facebook as the one-stop shop for all social-networking needs. While it may seem more complicated to post photos on Instagram, share casual moments on Snapchat, text on WhatsApp, and check your Twitter feed throughout the day, tweens and teens love the variety.

You don't need to know the ins and outs of all the apps, sites, and terms that are "hot" right now, and if you did, they wouldn't be trendy anymore. But knowing the basics such as what they are, why they're popular, and what problms can arise when they're not used responsibily can make the difference between a positive and negative experience for your child.

The following applications are not all inclusive, and will change over time in popularity. As time goes on newer applications will be available and it is important to stay in the know as to what dangers applications can pose. Some apps don't appear dangerous, and maybe aren't inherently dangerous but can pose a threat to our children if it's used inappropriately.


Audio Manager, Hide it Pro

Audio Manager is an app that users can hide messages, photos, videos, and other apps in. The app is designed to look like an audio manager by it's icon, but it can be used to hide content kids don't want their parents to know about. At first glance, the app can be used to turn the volume up and down, but if you press on the Audio Manager title, the Hide It Pro app will launch—a secret vault of pictures, videos, messages, apps, etc. The app disappears from the recent apps list—it can't be tracked. The app has two lock screens with a password. The app has an escape pin/password "for times when you get caught." It also has built in encryption (to military standards) to secure the most important files.


Calculator%

Calculator% is an app that stores photos and videos hidden behind a calculator. To anyone that starts the app, it looks like a calculator, but if you put in a passcode it will open up the private area. The app has built in protection for those who try to open the app without the correct passcode. The app will take a photo of the individual along with GPS location. How to access photos: press the decimal button, enter 1000, press the decimal button again, and then enter the password. Users can't recover their passcode if they forget it.


Vaulty

Vaulty is an app that hides pictures or videos on the phone the user doesn't want anyone to see. Vaulty has password protection where users use a pin or text password to enter. If someone tries to look in the app and enters a wrong password, it takes a photo of the individual and save it in the Vault for the next time the user logs in. The app also has an online backup of hidden pictures and videos in the event the phone is lost or stolen. Users can create more than one vault and set a different password for each.


Keepsafe

Keepsafe secures personal photos and videos by locking them down with PIN protection, fingerprint authentication, and military-grade encryption.


FotoX

"Never get caught off guard with sensitive material on your phone. Hide and protect your private photos and videos in private gallery."


AppLock

AppLock can lock Facebook, Whatsapp, Gallery, Messenger, SnapChat, Instagram, SMS, Contacts, Gmail, Settings, incoming calls and any app you choose. The app prevents unauthorized access and guards privacy. The app can hide

pictures and videos. The app has random keyboard and invisible pattern lock. The app is advertised in the Android store as: “Never worry about parents check your Snapchat or Musical.ly!”

 Kik Messenger

Kik is an app that lets kids text for free. It’s fast and has no message limits, character limits, or fees. Because it’s an app, the texts won’t show up on your child’s phone’s messaging service or parental control devices that monitor the phone’s text messages. Stranger danger is an issue since it allows communication with strangers who share their Kik usernames to find people to chat with. The app allegedly has been used in high-profile crimes, including the murder of a 13-year-old girl and a child-pornography case. There’s also a Kik community blog where users can submit photos of themselves and screenshots of messages to contests. Kik is loaded with ads and in-app-purhcases. Kids have confirmed they frequently encounter adult content or are targeted for inappropriate discussions that often lead to requests for pictures. Other hidden dangers are porn bots, automated programs that try to disguise themselves as suggestive, personalized messages to trick users into clicking onto porn sites. Chat now opens doors to users outside of your teen’s trusted circle of friends and contacts on Kik. Anonymity and selection is a reason sexual predators us Kik. They have stated it not only helps them remain anonymous, it lets them look for clues in teens’ usernames regarding personal issues that may leave them vulnerable. Kik also allows users to search for people to chat with by age range.

 Yellow-make new friends

Yellow is an app “to make new friends and chat.” This app functions similar to Tinder in that users “swipe” to like or pass. If both users like each other, they get to chat. The FBI has issued warnings that predators are using this app because they go undetected by bypassing security measures. Users must enter a birthdate, but the app has no way of verifying the birthdate users input. Predators are creating profiles to pose as teens to find victims. FBI agents have stated, there is a possibility inappropriate pictures and text messages can be shared through the app. The app is known as, “Tinder for Teens.”

 WhatsApp

WhatsApp lets users send text messages, audio messages, videos, and photos to one or many people with no message limits or fees. The app automatically connects with the users address book after sign up.

 Omegle

Omegle 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. Prior to 2013, the site did not censor contributions through a profanity filter, and users may have encountered nudity or sexual content on camera. After January 2013, Omegle implemented a “monitored” video chat, to monitor misbehavior and protect people under the age of 18 from potentially harmful content. To complement the monitored video chat, Omegle also has an “unmonitored” video chat.

 Tinder

Tinder is a *location-based* app that facilitates communication between mutually interested users. The app is most commonly used as a dating app. The rating system can be used as a means to cyberbully. A group of kids can target another kid and intentionally make his or her rating go down.

 Blendr

Blendr is an app that combines *GPS location* sensing with a social networking framework, to provide users with the opportunity to meet people who are within a close physical proximity. Users provide a photograph and basic information about their interests, and then are able to browse other people who are nearby to their present location.

 GroupMe

This app doesn't charge fees or have limits for direct and group messages. Users can also send photos, videos and calendar links.

 Instagram

Instagram lets users snap, edit, and share photos and 15-second videos, either *publicly* or with a private network of followers. Teens are on the look out for likes as a measure of "success." Photos and videos 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. Private messaging is also an option.

 Tumblr

Tumblr is a streaming scrapbook of text, photos, videos and audio clips. Users create and follow short blogs, or "tumblogs" that can be seen by anyone online (if made public). Pornographic images and videos are easy to find, and depictions of violence, self-harm, drug use, and offensive language are easily searchable. The first profile a member makes 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.

 Musical.ly

Musical.ly is a performance and video sharing social network that mostly features teens lip syncing and to famous songs. "Musers," as devoted users are called, can build up a following among friends or share posts publicly. All accounts are public by default. When kids post a video, everyone can see it and follow them. With a private account, only approved followers can see their creations. When signing up it does not ask users to enter a birthdate or age. Anyone can sign up easily with an email. Even with a private account, their profile is still public. Other users can search for their account and see their profile picture, username and a short bio. Once a child opens an account, they cannot delete it.

Predators are using the app to target young kids. A parent found his 8-year-old daughter was being "groomed" by an individual through this app.

 Live.ly

Live.ly is the sister app of Musical.ly. This app is a live stream platform. Users will be able to broadcast through the live.ly app and streams will be viewable on musical.ly. Streamers can easily forget they have strangers peering into the bedroom

they are broadcasting from, watching them answer personal questions from anonymous viewers. Watching the broadcasts requires no registration or age verification.

 Yik Yak

Yik Yak is a *location based* app that helps users connect with the people near them. The app allows users to post text only "yaks" that can be viewed by the 500 Yakkers who are the closest to the person determined by GPS location tracking. Users have used the app to bully their peers anonymously.

 Whisper

Whisper is an online community that allows users to post statements to the public, as well as send private messages to other users without revealing their identities. Whisper's anything goes culture is packed with cruelty, cyber bullying, racism, homophobia, and vulgarity. Whisper also revelas users locations.

 Keek

Keek allows users to upload video status updates. Users can also reply back with text or video comments, and share content to other major social media networks.

VIRTUAL PREDATORS

Predators are using several apps to make fake profiles and befriend children to draw them into sex trafficking rings. Predators target young impressionable boys and girls through these social apps. Predators "groom" their victims and gain trust over time. What is "grooming?" It is befriending and establishign an emotional connection with a child, and sometimes the family, to lower the child's inhibitions for child sexual abuse. It lures minors into trafficking children, illicit businesses such as child prostitution, or the production of child pornography. Groomers often pretend to be younger and may even change their gender. Many give a false physical description of themselves; some send pictures of other people pretending it is them.

Other websites that are potentially dangerous to children: chatroulette.com, chat-avenue.com, chatstep.com, chatrandom.com, camzap.com, tinychat.com, and tohla.com.

PARENTAL CONTROLS

There are two major types of parental controls. The first *is family rules or guidelines* that you establish with your children, and the second is *technology tools* provided by cellphone companies, smartphone makers, and app developers. In many ways, the first kind is more effective, because it involves teaching your children self-regulation and –protection, which are with them wherever they go and can last a lifetime. Monitoring and Web filtering apps are available, but don't let them give you a false sense of security because there are no substitutes for the moral compass and cognitive filter kids develop for their own well-being.

Because phones have Web browsers, they can be used to view any type of Web content, including content you might consider inappropriate for your children.

Parental controls in Google Play:

For family members under 13

If you created a Google Account for your kid under 13, you can set up parental controls for them.

How Google Play parental controls work

- Parental controls work on Android devices where your kid is signed in to their Google Account.
- A parent in the family group needs to use their Google Account password to set up or change their kid's parental control settings.

Set up parental controls

1. Open the Family Link app.
2. Select your kid.
3. On the "Settings" card, tap **Manage Settings** > **Mature content restrictions**.
4. Choose your filters:
   - **Apps, Games, Movies, and TV**: Choose the highest maturity level of content you want to allow for download or purchase.
   - **Music and Books**: Choose whether you want to restrict downloads or purchases of explicit content.

Note: Parental controls don't prevent seeing restricted content as a search result or through a direct link.

For family members 13 or older

How Google Play parental controls work

- Parental controls only apply to the Android device you added them on. To add parental controls on another device, repeat the steps below on the other devices.
- If you have multiple users on a device, you can set up different parental controls for each person.
- The person who sets up parental controls will create a PIN that needs to be entered to remove or change the parental controls.

Set up parental controls

1. On the device you want parental controls on, open the Play Store app.
2. In the top left corner, touch Menu > **Settings** > **Parental controls**.
3. Turn "Parental controls" **On**.
4. Create a PIN. This prevents people who don't know the PIN from changing your parental control settings. If you're setting up parental controls on your kid's device, choose a PIN they don't already know.
5. Choose your filters:
   - **Apps, Games, Movies, and TV**: Choose the highest maturity level of content you want to allow for download or purchase.
   - **Music and Books**: Choose whether you want to restrict downloads or purchases of explicit content.

Once you set up parental controls, you can turn them on or off. When you turn them back on and create a new PIN, your old settings will come back. This helps you share a device with people who don't need parental controls.

Parental controls in Apple iOS:

You can use *Restrictions*, also known as parental controls, to block or limit specific apps and features on your iPhone, iPad or iPod touch.

1. Tap Settings > General > Restrictions
2. Scroll down and tap Restrictions, then tap Enable Restrictions
3. Create a Restrictions passcode. You need your Restrictions passcode to change your settings or to turn off Restrictions.

When you have Restrictions on, you might not see certain apps, features, or services.

Set up Family Sharing and Ask to Buy

With Ask to Buy and Family Sharing, whenever a family member initiates a new purchase or free download, a request goes to the organizer. The organizer can review the item and make the purchase or decline the request right from their own iPhone, iPad or iPod touch. If the organizer makes the purchase, the content will download automatically to their family member's device. If they decline, no purchase or download will take place.

Setting up Family Sharing:

1. Go to Settings > Cloud.
2. Tap Seet Up Family Sharing, then tap Get Started.
3. Confirm that you want to be the family organizer and that you're signed in with your personal Apple ID.
4. Follow the onscreen instructions.

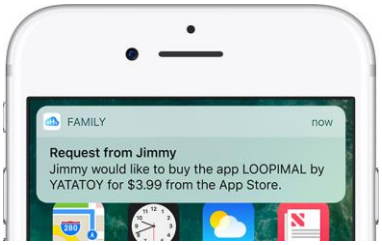
Use these steps to add someone who already has an Apple ID:

1. Go to Settings > iCloud > Family > Add Family Member.
2. Enter your family member's name or email address.
3. Follow the onscreen instructions.

Turn on Ask to Buy

The family organizer can turn on Ask to Buy for any family member who isn't an adult. It's on by default for any children under 13, and you'll be asked to set up Ask to Buy when inviting anyone under 18 to your family group. Use these steps to turn Ask to Buy on or off for family members who are under 18.

1. Tap Settings > iCloud > Family and tap your family member's name.
2. Tap Ask to Buy



Other Resources

There are several programs available to help protect your family online and on their phones. Please research what products are best for your family's needs.

Safe, Smart & Social: Teaching Students How to Shine Online

www.safesmartsocial.com

This site provides social media safety training for parents. This training shows 8 to 18-year-olds how to think about their future and use social media as a positive portfolio of accomplishments to shine online. This site provides montly media tips individuals can sign up for via their website.

Netsmartz

www.netsmartz.org

This site provides an interactive, educational program with age-appropriate resources to help teach children how to be safer on-and offline. The program educates children on how to recognize potential internet risks; engage children and adults in a two-way conversation about on-and offline risks; and empower chilren to help prevent themselves from being exploited and to report victimization to a trusted adult.

TeenSafe

www.teensafe.com

TeenSafe is a subscription service for parents of children between the ages of 7 and 17 that provides smartphone monitoring and control capabilities. TeenSafe Monitor displays your child's text/SMS messgaes, iMessages, and deleted texts/SMS and iMessags in a dashboard formatted for your screen. TeenSafe Control uses mobile device management protocol, similar to the way corporations secure devices used on their networks in order to protect their network from threats. An MDM certificate is installed on your teen's phone and paired with the TeenSafe Control App on your phone, giving you the power to control it remotely.

TeenSafe Blog provides information on various apps your teens may be using and other helpful articles regarding parenting with technology today.