Facebook is an online social media platform that has over 2 billion users across the globe. It was initially for university students but soon expanded out and since 2006, anyone over the age of 13 is able to join the platform. It is available on all devices from your desktop and laptop computer to smartphones and tablets. Users can add photos and videos, update their status, interact with others and catch up with the latest news. Despite requiring users to be over 13, there are no age verification measures and children can easily create an account. It's therefore important that parents familiarise themselves with the main features of the platform to ensure their young ones remain safe if and when they use it.

AGE RESTRICTION 13+

What parents need to know about FACEBOOK

ADDICTIVE NATURE

Facebook can be hugely addictive as it offers a physiological high and a quick reward cycle which comes from the likes and comments on shared posts. Communication is so instant now that teenagers are always checking, and it can sometimes feel like self-worth. This keeps children going back, encouraging them to post things and also increases the Fear Of Missing Out (FOMO) that is commonplace today. On the flip side, because of the way teenagers interact these days through Facebook and Facebook Messenger, they can seem addicted even when they're not.

CYBERBULLYING

Around a quarter of children have experienced online abuse, according to Ofcoms 2019 'Online Nation' report. Figures show that 23% have been cyberbullied, 39% subjected to abusive language and a fifth have been trolled. On Facebook, teenagers can receive communication in a number of ways, from private messages in Messenger to public comments on profiles, pages and posts to pages or groups set up just to torment a victim. Exclusion from pages or groups to cause the victim to feel left out has also been seen.

FUTURE IMPACT

Regardless of age, anything that's posted on Facebook, or other social media platforms, develops a personal brand and leaves a digital footprint that is there forever. It can be difficult to explain the consequences but many universities (and employers) look at Facebook before making a decision on accepting people. It is therefore wise to always think twice before posting anything online you wouldn't want people to hear or see offline.

STRANGERS/FAKE PROFILES

Generally, people are who they say they are online. That said, much like the real world, Facebook isn't free of malicious users and children have received friend requests from people they don't know, including individuals who may look to take advantage of young and impressionable children.

People you may know

OVERSHARING

Facebook encourages you to share "what's on your mind" but children need to be aware of what they're revealing about themselves online. Facebook allows users to share their location, create live videos and much more. Some photos can be traced using file data, too, so it's important to keep a tight group and share only with people you know.

INAPPROPRIATE ADS

While Facebook is getting ever stricter on the content of ads and who they are targeted to, there is still the chance that children could be subject to ads during their experience on the platform. This could be innocuous but is worth bearing in mind when using the app.

LIVE STREAMING

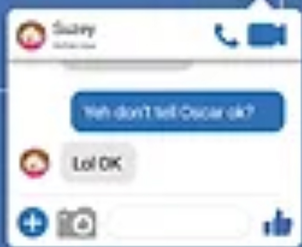
Facebook Live provides users with the ability to stream video live-time to their friends and followers or watch other people's broadcasts live. During the video, people can react and comment and it's difficult to moderate the content given everything happens in real-time. This could mean your child is exposed to inappropriate material or worse still, could be cajoled into doing something online by others which they wouldn't normally do.

LIVE

42 people watching

PRIVATE MESSAGING

Facebook Messenger is closely linked to your Facebook profile and provides the ability to share private messages away from friends and family. It is therefore important that parents ask their children who they are communicating with and ensure that the only people they are exchanging messages with are people that they also know in real life.



National Online Safety
#WakeUpWednesday

Safety Tips For Parents

MAKE PROFILES PRIVATE

Within the settings of a Facebook account, you can choose whether a profile is public or private. Make sure that your child's setting is switched to private. This way they will only be able to interact with friends and people they know within the platform.

LEAD BY EXAMPLE

Show your children how and why you use Facebook. This will help to demonstrate that it can be used safely when used in an appropriate manner and help to reduce the risk of them encountering harmful content.

SHARE DEVICES

Depending on the age of your children, it's worth considering letting them use Facebook from a general family iPad or laptop. This allows them to use it without being constantly connected everywhere they go and may give you more reassurance around what they are doing on the app.

REPORT VIOLATIONS

On Facebook you're able to hide people or groups and report things that are harmful. Make sure you spend some time to show your children how this works and why it's important to do so before they start spending serious time on the platform.

Report this post
Help us understand what's happening. How would you describe it?

RESPECT BOUNDARIES

As with anything, there are potential risks and dangers on Facebook but once you've talked about the ideas of safety on the platform, give children some space. Trust them to make smart choices but always be open to talking about social media.

CHECK-IN

Once they've had some time to use the platform, don't be afraid to check in and see if there's anything on Facebook they'd like to discuss. This isn't always easy but being open with your children is the best way to deal with any issues head on.

Meet our expert

Alex Wright is a former Facebook employee and social media expert with over 15 years' experience working in digital media. He has worked with some of the biggest organisations in the world and has a wealth of knowledge in understanding how social media platforms work and how they engage their audience.

SOURCES: https://facebook.com, https://www.independent.co.uk/life-style/social-media-addiction-young-children-under-five-youtube-instagram …

At National Online Safety we believe in empowering parents, carers and educators with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. Please visit nationalonlinesafety.com for further guides, hints and tips for adults.

Part of our Social Media & Live Streaming Series

NOS Social Media & Live Streaming

Brought to you by NOS National Online Safety

www.nationalonlinesafety.com

What you need to know about...

FRIENDS & FOLLOWERS

What are they?

'Friends & Followers'

What makes social media actually 'social' are the connections users make with other users on the platforms. Every social networking site handles these connections differently, calling them 'connections', 'friends' and 'followers', amongst others. Having friends and followers is how we find out what other people say and do. Your friends and followers are much more likely to see your online content than those outside of your network, which is why it's important to be mindful of who you connect with and what you share. On some platforms, if two accounts follow each other, this may allow additional communication channels such as private messaging.

Know the Risks

Access to private information

This may include your child's home address, school, date of birth, names of siblings or other relations, as well as seeing photos that inadvertently contain sensitive information. This is completely harmless information for genuine friends or family but could cause issues in the hands of a criminal.

Catfishing

'Catfishing' is the common name given to an individual posing as someone else on social media. They do this to try and befriend typically young and vulnerable people who they 'talk' to then take advantage of. Unfortunately, there are many examples of this happening across the world that have had real-life consequences.

Online bullying

Once a connection is made on social media, there is the potential to send private messages between individuals. It is difficult for social networks and other users to see what is being said between accounts. This provides an opportunity for bullies to victimise individuals and can create a dangerous spiral of online activity.

Safety Tips

Check privacy settings

Platforms such as Facebook allow users to modify their privacy settings, which means people who are not friends can't see all your profile information. It's also possible to hide this information for some or all of your connections. Always make sure your child's accounts are set to private.

Talk about strangers

Make sure children understand that they should only connect with people that they know or can completely trust. They should be wary of anyone messaging them frequently who they don't know in real life or have never spoken to or actually seen online. Catfish will stick to text-based messaging only, to keep their identity secret.

Delete old connections

Children should be mindful that everything they share will probably exist online forever and that they shouldn't share anything that gives too much information away. Every now and again, they should delete old connections that they no longer spend time with. Old accounts can easily be hacked, exposing personal information to strangers.

Further Support

Encourage an open dialogue

It is really important that your children knows that they can speak to someone about anything they're not sure of online. It is crucial that they know they won't be judged or told off for anything they've done; it is far more important to know if they're in danger or worried about something.

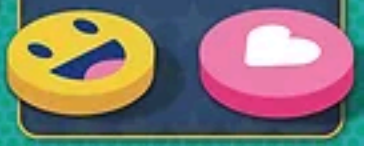
Seek additional guidance

If your child wants to spend a lot of time online and is displaying compulsive or addictive behaviour, is negative, struggles with schoolwork and reduces real-life interactions or has frequent changes in mood, they could be experiencing negative interactions online. Speak to them and seek support from their school or your local safeguarding team if you think your child has been affected.

Our Expert

Emma Davis

Emma Davis is a cyber security expert and former ICT teacher. She delivers cyber awareness training to organisations nationally and has extensive knowledge and experience of managing how children access services and apps online.



www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety Instagram - @nationalonlinesafety

ConnectSafely

FAMILY GUIDE TO

Parental Controls

- Advice for Parents, by Parents
- Thoughts About Monitoring & Filtering Software
- Screen-Time Limits
- What Parental Controls Can't Do
- Talking to Kids About Devices

What's Inside

For more info, visit ConnectSafely.org/controls

GO

Join @ConnectSafely on social

CONNECT

What are parental controls and what do they do?

There are a variety of control tools and monitoring tools available to parents. Some are software products or mobile apps that you buy or subscribe to. Others are free and some are already present on your phone, tablet or computer operating systems or available from your internet service provider. Some extensions work within popular browsers to limit access to certain types of content. There are internet routers and gateways that offer controls across your entire network. Some apps and sites have their own parental controls.

Depending on the product, these tools can:

- Filter out (block) inappropriate websites & other content
- Limit the ability to download or purchase apps or certain types of apps
- Monitor and report on sites or apps a child uses
- Monitor what your child is posting or viewing on social media
- Monitor and/or limit what your child can type or is exposed to, such as cyberbullying or hate speech
- Limit total screen time or screen time of specific apps or types of apps
- Limit the ability to watch videos, movies or TV shows based on age ratings
- Block music with inappropriate lyrics
- Control the use and access of certain devices on your home network
- Limit what a child can find using a search engine
- Ask a child or teen to rethink what they're about to send or post if it may be inappropriate or hurtful to others.

Should I install internet filtering or monitoring software?

Filters can usually prevent young children from accidentally stumbling on troubling or inappropriate material, but they are less effective at keeping older kids and teens from deliberately visiting blocked sites. There are several ways to get around filters, including using another computer, mobile phone, or tablet that's not filtered. Whether and how to use filtering and monitoring tools is a parental decision that should be based on your understanding of what's best for your child.

There are some children and teens who need very strict controls and others who can do just fine without them, based on conversations and adherence to household rules. Only you know what's best for your child.

Monitoring tools can inform parents of what their kids are doing but some kids — especially teens — feel that it's an invasion of their privacy and many would argue that it's not necessary or helpful. When it comes to monitoring tools, another risk is "too much information." Do you really want to look at every text message and review every website your child visits?

Every family must make its own decision based on a number of factors including:

- The child's age and maturity
- The child's sensitivity to certain types of content that may be "appropriate" but still upsetting
- The child's propensity to take risks
- The child's impulse control
- The child's willingness to adhere to family rules
- The parent's values and concerns over types of content and activities
- Any special circumstances or needs that affect your child

Filters are less effective at keeping older kids and teens from deliberately visiting blocked sites.

How to chose a filtering or monitoring product

The first thing you should do is consider what, if anything, you need for your child. Do you want to block age-inappropriate sites, do you want to restrict what apps they can download, do you want to protect them from being cyberbullied or bullying others? Do you want to know what your kids are doing online and, if so, how much information do you want? Some programs will give you nearly everything; others give you a summary, and some just flag what they consider to be troublesome content or behavior.

Before you spend money, check out the tools that may already be controls on your devices or available from the maker of your device or operating system.

Free family-friendly tools and apps include:

- Amazon Kids+ Parental Controls (Fire tablets and other Amazon devices)
- Apple: Parental controls for iOS (iPhone, iPad and iPod Touch)
- Apple: Screen Time on Mac
- Google Family Link (Free for Android devices as a download)
- Microsoft: Controls for Windows 10 & Xbox
- YouTube Kids, Messenger Kids, TikTok Family Pairing

There are of course many third-party tools, some are free and others cost money. ConnectSafely does not recommend specific tools, but here are links to credible independent sources for reviews of parental control tools:

- CNET: Best apps to put on kids' phones to keep them safe
- Common Sense Media: Parents' Ultimate Guide to Parental Controls
- ConsumerAdvocate.org: Top 10 Parental Control Apps of 2021
- Digitaltrends: The best parental control apps for Android and iOS
- PC Mag: The Best Parental Control Software (updated annually)
- PC World: Screen Time, Family Link, and FreeTime vs my 7-year-old son: Which parental controls are best?
- Tom's Guide: The best parental control apps for Android and iPhone 2021

Network-level control devices

Many internet service providers have parental control options as part of the settings for their gateways (a single device that includes both an internet modem and a router) or other devices. There are also third-party routers and devices that work with PCs, game consoles, phones and any other devices that are either hardwired or connected by WiFi to your home network. These devices, however, may not work if

your child's device has a cellular connection that doesn't require access to the home network. The service you already use may offer these controls and — if you have a third-party router — check with that company's website to see if they offer parental controls.

Shared devices

It's not uncommon for two or more family members to have access to the same device. Many devices, including Macs, Windows PCs, Android phones and TV streaming devices, allow you to create more than one account so that you can have different settings for different users. Other controls have passwords that enable adults or older children to bypass controls. Check with your device maker's or operating system's website for instructions to see what options are available.

Screen-time limits

There are apps that you can use to limit how much time your child spends on a device or a service. Some are built-into devices themselves and others are part of services, apps or games aimed at children. These limits can help you control not only how much time a child spends using the device but the time-of-day as well, allowing you to set a "bed-time" for when the device must be turned off. These tools can be useful, especially with younger children, but should always be part of a larger discussion about the use of devices and media. Many parental control tools offer screen time manager as one of their features.

Stealth mode

While many don't even allow parents to secretly control or monitor their child's online behavior, some apps can run in "stealth mode" so that the child may not be aware

The best web filter is the one located between the child's ears and it lasts a lifetime.

that they're in use. Except in very rare situations, we at ConnectSafely don't recommend the use of stealth mode. As a general rule, it's a good idea to talk with your kids about the controls and why you're using them. Besides, your child will likely figure out it's there anyway and if you do find something that concerns you, you don't want their first response to be "why are you spying on me." It's better to get that out of the way at the beginning.

It's a good idea to talk with your kids about the controls and why you're using them.

What about parental controls built-into services and apps?

Some social media services and apps have their own controls, such as limiting the type of content your child can see or who your child can interact with. Sometimes these controls kick in automatically depending on your child's age, while others give parents the ability to manage or even monitor their child's experience with that service. It's a good idea to look at the service's default settings for your child's age group and see if you wish to adjust it if possible. Because of these safeguards, it's important that children be honest about their age because they may not be available or they may be different if the service doesn't know your child's age.

Beyond parental controls, most social media apps and services have settings to control privacy and security, who you interact with and more. Parents should talk with their kids about these controls and what is appropriate for their children. For more, check out ConnectSafely's Parent's Guides and Quick Guides to popular apps and services.

Safe searching

Google offers SafeSearch and Bing has its own feature to restrict the sites you can find. These settings do a generally good job at restricting what your child can find in a search but they're not perfect and they only work on the search engines where they are configured.

Streaming, TV and internet video

Most streaming services and devices also let parents control the type of content their kids can watch. Check with both your streaming device such as Roku, Apple TV and Amazon Fire TV, as well as services you subscribe to for what controls they offer. Also, be aware that YouTube and other online video services have content that may be inappropriate for your child. You can block the entire service or, in some cases, specific types of videos or you can restrict your kids to only child-friendly services like YouTube Kids or other family-friendly brands like Amazon Kids, Disney and PBSKids.

What parental control tools can't do

Parental control tools only work on devices, networks or services where they are installed. They likely won't work if your child logs on away from home on someone else's device and network-level controls may not work if a child connects via a cellular network or a WiFi network away from home. And, while parental controls can be used as part of your efforts to teach your children good online habits, they are not a substitute for parenting and don't — on their own — typically teach the important traits of self-control, critical thinking and consideration for others. They also don't work once a child grows up and away from their parents, which is why it's so important to teach and reinforce critical thinking skills and self-control.

Be a good role model

How you act in front of your children can have a bigger impact than on what tools you're using or what you say. It's fine to put time-limits on your children's use of technology but make sure they don't see you over-using your technology, especially during family time when you should be interacting with them.

Weaning from filters

Your child will be an adult before you know it and it will be up to them — not you — to regulate what they do and how they act online. If you use filters or monitoring tools, think about how to wean your kids away from them as they get older and more responsible. Some products give parents the ability to gradually loosen up controls or monitoring as a child matures. As children get into their teen years, consider loosening up or removing any filters or monitoring products, especially if they're older teens who will soon be on their own and fully responsible for their own online and offline behavior.

Closing thoughts for parents

When it comes to parenting, one-size definitely doesn't fit all. Most of our advice here is for average kids with average risk but there are kids whose needs are different who may require stronger controls or monitoring. As with most parenting decisions, you need to think about your specific child and specific needs as well as your own risk tolerance.

Ultimately, the only filter that can fully protect your child for life isn't the one that runs on a computer or a phone but the one that runs in the software between their ears. It's important to teach critical thinking skills and media literacy to help children make good decisions on and offline now and as they mature. With any luck, your child will grow up, become independent and maybe even move away from home, so — ultimately — it's important they develop their own controls rather than relying on those imposed by parents or schools.

About ConnectSafely

ConnectSafely is a Silicon Valley, California-based nonprofit organization dedicated to educating users of connected technology about safety, privacy and security. We publish research-based safety tips, parents' guidebooks, advice, news and commentary on all aspects of tech use and policy.

ConnectSafely

ROBLOX

A QUICK-GUIDE FOR PARENTS

What is Roblox?

Roblox is an online platform where anyone can create and share games. There are literally millions of user-generated 3D game worlds on Roblox. Some games are free to play, while others cost "Robux," the online currency that players use to buy games and items such as clothes or accessories.

Parents should know that most Roblox games include social features, like in-game chat and filtered messaging, though you can turn off these features. Roblox may be your child's first experience with online socializing, which gives you a hands-on opportunity to help your child develop good digital habits that last a lifetime.

How can I help my child stay safe on Roblox?

As with all online social experiences, everyone should be respectful of themselves and others, be mindful of what they post, and understand how to use any privacy settings, security tools, or blocking and reporting features. Roblox also provides parents with tools to restrict certain activities, like chat, within the platform, and to monitor their child's account activity.

Should my child play with people they don't know?

There isn't a single answer for every child or family. Roblox does give you a lot of control over who can interact with your child and how. You can choose who can message them, and who can chat with them. But there can be positive aspects to interacting with new people, as long as your child is careful not to reveal personal information, get into inappropriate conversations or get together with people they meet online, except with parental supervision. Access these controls within the **Privacy** tab in **Account Restrictions**.

What kids want parents to know about... Roblox

"It's really easy to see what your kid is playing."

"There are games for different ages."

"Pay attention to game classifications (e.g. fantasy, role playing, military, horror) to get games that are fun and comfortable to play."

"Most people on Roblox are very nice. If someone is being mean, people will respond. There's a great community."

"Kids can 'mute' people who are annoying them."

"Roblox doesn't let little kids play games aimed at older kids."

"It's easy to report people who are breaking the rules."

"There are a lot of friendly games."

"Any games with bad content will be taken down in a heartbeat by Roblox administrators."

"Chat doesn't let you share bad words or personal information (street addresses, phone numbers are blocked)."

"Most games encourage teamwork and some require it."

*For more information and a printable pdf, visit ConnectSafely.org/Roblox.

How much screen time is best?

This is a harder question to answer than it may seem. The American Academy of Pediatrics has recently revised its screen time recommendations and no longer recommends arbitrary limits. Of course, no online activities should interfere with sleep, exercise, homework, or family time and it's best for children to have set-times when they are allowed to "play" online. And just as with soccer or any other types of games, it's best for children to know when they can and can't play rather than being arbitrarily kicked off by their parents without notice.

> > More advice for parents

Play Roblox with your child.

Whether your child plays Roblox on a computer, smartphone, tablet, or gaming console, we recommend kids (especially younger ones) play with you or another trusted adult nearby, and ideally in a public area of the house like the den or kitchen. You'll want to see what kind of games they're playing, how they're playing (sportsmanship matters online, too), and with whom they're interacting. Better yet, make an account for yourself so you can play games together. This will give you a better sense of how Roblox works and it might be fun for you, too.

Read and discuss Roblox's Community Rules.

Review Roblox's Community Rules with your child, especially the "guiding principles" which are easy to understand. Also consider drawing up a family agreement that outlines your expectations for their online behavior. Make it a discussion (never a lecture) and remember to explain to your child that along with rights and privileges come responsibilities. You'll find examples of family contracts at ConnectSafely.org/contracts.

Use parental controls.

Roblox defaults to more restrictive settings for users under 13. For additional parental controls, go to **Settings** (gear icon) and **Parental controls**. Here parents can disable chat or messaging, restrict access to a curated list of age-appropriate games, and set a monthly limit on how much money, if any, the child can spend on Roblox's in-game currency. Parents can also enable an account PIN which requires a 4-digit code to make any changes to settings. We recommend parents use these features for very young or new players, but for most families, the goal should be to help children learn to make good decisions on their own as they mature.

Passwords and other personal information.

Starting at an early age, talk with your kids about the importance of keeping passwords and other personal information private. Friends can become ex-friends, and use your child's account in mean or inappropriate ways. Scammers can also lure kids into giving private information in exchange for "free" Robux. Help your child get into the habit of creating unique passwords with a combination of numbers, letters, and special characters, and updating all passwords regularly. More on this at ConnectSafely.org/passwords.

Reporting and blocking.

Players can use the **Report** links located throughout the platform and in the **Report** tab of every game menu (click the flag next to the offending player's name). Talk to your child about what to report (including bullying, inappropriate behavior, scams and other violations) and how to make a report. Or, ask your child to come to you if they experience a problem so you can report together. You can block players by going to the three dots in the upper right corner of the player's profile and selecting **Block**.

ConnectSafely

PARENT'S QUICK-GUIDE TO

Instagram

What is Instagram?

Instagram is a social media app used to share photos, videos, and messages. With features like Stories, Feed, Live, Instagram TV, and messaging, teens use Instagram to celebrate big milestones, share everyday moments, keep in touch with friends and family, follow their favorite celebrities, and build communities of support and meet others who share their passions and interests.

Is there a minimum age for Instagram?

The minimum age is 13, in compliance with the U.S. Children's Online Privacy Protection Act. Although against the rules, some younger children deliberately enter an incorrect date of birth, often with a parent's permission. Instagram will delete underage accounts if they're notified and can't verify that the user is over 13. It's important for your teen to join using their correct birth date because Instagram has special safeguards for minors. For example, Instagram won't recommend public accounts of minors to adults, and adults can't message minors who don't follow them.

Helping Your Teen Keep Perspective

Instagram often represents a highlight reel of someone's life. Some Instagram users spend a lot of effort making themselves look really good via make-up, lighting, wardrobe, and in some cases, even plastic surgery. Others go to great lengths to make their lives seem extra interesting or fun. It's important not to fall into the comparison trap. People rarely post about their sad or boring moments, but everyone has them. And encourage your teen not to compare themselves to others. Even professional models don't look that great most of the time.

What are the risks?

The main things parents worry about are typical of all social media: mean behavior among peers, encountering—or creating—inappropriate or dangerous content, overuse, and of course, privacy. There is also the risk of users comparing themselves to others, which can impact their sense of well-being. Parents are also concerned that people their kids don't know can reach out to them directly. Teens can learn to manage these risks, which is why we wrote this Quick-Guide and our longer Parent's Guide to Instagram (ConnectSafely.org/Instagram).

Are there tools to protect privacy & safety on Instagram?

Yes. Teens can start by keeping or making their account private so that only people they approve can see and comment on their photos, videos, and posts. There are also tools to block people and report inappropriate posts, which we'll go into in more detail on the next page. In addition to banning people who have repeatedly broken its rules, Instagram now flags accounts with "potentially suspicious behavior" and prevents those accounts from interacting with young people's accounts.

More Advice for Safety & Well-Being on Instagram

Make or keep the account private. By default, accounts are private for teens under 16. If your teen's account isn't private they can (and in most cases should) make it private by going to their profile page (tap on the profile pic in the lower right) and **Settings > Privacy**. The slider will turn blue once the account is private. A private account means only people your teen accepts as followers can see or comment on their posts or send them messages.

Finsta: "Fake" but not sinister. Unlike Facebook, Instagram doesn't require people to use their real names, and they allow users to have up to 5 accounts, with the ability to switch between them. Some young people choose to create separate and more private accounts where they share posts that are relaxed and more "real" among a select group of friends. Although Finsta is slang for "fake" Instagram account, there is nothing sinister about it. You might want to ask your teen what they do to assure their privacy and then ask about Finsta.

Prioritize positive connections. Teens, especially younger teens, should only interact with people they know in real life and only accept followers they know. What and who people see on Instagram largely depends on who they follow and what content they search for. Controlling these aspects of an account—and connecting with others and searching for content in a mindful way—will have a big impact on anyone's experience on Instagram.

Manage privacy settings. There are lots of privacy settings to control who interacts with your teen and their content. Visit **Settings > Privacy** and look through the settings together. Your teen can decide who comments on their posts, tags them in photos (we recommend selecting **Manually Approve Tags**), sends them messages, sees their activity status (when they were last online), and more.

Block and report. Users can block anyone who is bothering them, such as sending them a lot of direct messages or trying to engage them in a creepy conversation. To block a user, go to their profile, tap the three dots, and **Block**. To report inappropriate content or anything that violates Instagram's Community Guidelines, go to the profile, tap on the three dots, and **Report**. Reporting is totally anonymous.

Track time spent on Instagram. Instagram has tools to help people manage time spent in the app. You can set daily reminders to get an alert when it's time for a break, mute notifications, and be notified when know you're "all caught up" on what your friends and communities have posted. Access these controls at **Settings > Your Activity**. At the top, there's a dashboard showing the average time spent in Instagram on that device. Tap any bar to see the total time for a particular day.

About ConnectSafely

ConnectSafely is a Silicon Valley, California-based nonprofit organization dedicated to educating users of connected technology about safety, privacy and security. We publish research-based safety tips, parents' guidebooks, advice, news and commentary on all aspects of tech use and policy.

Revised 10/7/21

RULES 'N TOOLS® CHECKLIST

FOR PARENTS, EDUCATORS, AND OTHER CARING ADULTS

Implement *both* safety rules and software tools to protect children online. Focus on the positives of Internet use while teaching children about the dangers and how to make wise choices online.

"Rules"

- ☐ Establish an ongoing dialogue and keep lines of communication open.
- ☐ Supervise use of all Internet-enabled devices.
- ☐ Know your child's online activities and friends.
- ☐ Regularly check the online communities your children use, such as social networking and gaming sites, to see what information they are posting.
- ☐ Supervise the photos and videos your kids post and send online.
- ☐ Discourage the use of webcams and mobile video devices.
- ☐ Teach your children how to protect personal information posted online and to follow the same rules with respect to the personal information of others.
- ☐ Be sure your children use privacy settings.
- ☐ Instruct your children to avoid meeting face-to-face with someone they only know online or through their mobile device.
- ☐ Teach your children how to respond to cyberbullies.
- ☐ Establish an agreement with your children about Internet use at home and outside of the home *(see Rules 'N Tools® Youth Pledge)*.

"Tools"

- ☐ Set age-appropriate filters.
- ☐ Consider using monitoring software, especially if you sense your child is at risk.
- ☐ Periodically check your child's online activity by viewing your browser's history.
- ☐ Set time limits and consider using time-limiting software.
- ☐ Disallow access to chat rooms and only allow live audio chat with extreme caution.
- ☐ Limit your child's instant messaging (IM) contacts to a parent-approved buddy list.
- ☐ Use safe search engines.
- ☐ Set up the family's cyber-security protections.
- ☐ Utilize parental controls on your child's mobile phone and other mobile devices.

Parental controls should be utilized on all Internet-enabled devices (desktops, laptops; and gaming, mobile, and music devices). However, these resources are not a substitute for parental supervision.

Report any content or activity that you suspect as illegal or criminal to local law enforcement and to the National Center for Missing & Exploited Children at www.cybertipline.com or at 1-800-843-5678.

RULES 'N TOOLS® CHECKLIST

FOR PARENTS, EDUCATORS, AND OTHER CARING ADULTS

Implement *both* safety rules and software tools to protect children online. Focus on the positives of Internet use while teaching children about the dangers and how to make wise choices online.

"Rules"

- ☐ Establish an ongoing dialogue and keep lines of communication open.
- ☐ Supervise use of all Internet-enabled devices.
- ☐ Know your child's online activities and friends.
- ☐ Regularly check the online communities your children use, such as social networking and gaming sites, to see what information they are posting.
- ☐ Supervise the photos and videos your kids post and send online.
- ☐ Discourage the use of webcams and mobile video devices.
- ☐ Teach your children how to protect personal information posted online and to follow the same rules with respect to the personal information of others.
- ☐ Be sure your children use privacy settings.
- ☐ Instruct your children to avoid meeting face-to-face with someone they only know online or through their mobile device.
- ☐ Teach your children how to respond to cyberbullies.
- ☐ Establish an agreement with your children about Internet use at home and outside of the home *(see Rules 'N Tools® Youth Pledge)*.

"Tools"

- ☐ Set age-appropriate filters.
- ☐ Consider using monitoring software, especially if you sense your child is at risk.
- ☐ Periodically check your child's online activity by viewing your browser's history.
- ☐ Set time limits and consider using time-limiting software.
- ☐ Disallow access to chat rooms and only allow live audio chat with extreme caution.
- ☐ Limit your child's instant messaging (IM) contacts to a parent-approved buddy list.
- ☐ Use safe search engines.
- ☐ Set up the family's cyber-security protections.
- ☐ Utilize parental controls on your child's mobile phone and other mobile devices.

Parental controls should be utilized on all Internet-enabled devices (desktops, laptops; and gaming, mobile, and music devices). However, these resources are not a substitute for parental supervision.

Report any content or activity that you suspect as illegal or criminal to local law enforcement and to the National Center for Missing & Exploited Children at www.cybertipline.com or at 1-800-843-5678.

NetSmartz®

Sextortion:

What Parents Should Know

You've likely heard of sexting – sharing and receiving sexually explicit messages and nude or partially nude images by text or through an app. Though sexting can be part of normal adolescent sexual development, there are also risks, particularly **sextortion.**

Sextortion: A type of blackmail used by offenders to acquire additional sexual content from the child, coerce them into engaging in sexual activity, or to obtain money from the child.

Who Are the Perpetrators?

Often, victims know their extorters. They are current or former romantic partners. They may hold an initial sexual image that was sent intentionally by the victim and are now using it to get more content; threatening to spread the picture to friends and family if the victim does not comply.

of the time, the blackmailer is known to the victim.

Other times, the offender was met online. This could be a lone-actor or a coordinated group of extorters who work together to target and elicit explicit content from their victims. This type of extorter may request additional content (often of an increasingly explicit nature) or money.

How Does it Happen?

Sextortion can happen at the hands of both **peers** and **unknown,** online offenders.

When It's an Unknown Offender

Approach

Offenders often approach a child on social media after using it to learn about the child's interests, friends, school, family, etc.

Move platforms

It is common for offenders to make initial contact with a victim on one platform, then ask them to move to a second or third platform, usually those with encrypted messaging systems in order to make tracking their crime more difficult.

Coerce

This includes using tactics like:

- Initially offering something of value such as money or drugs in exchange for a sexual image
- Pretending to work for a modeling agency
- Developing a false rapport with the child
- Secretly recording explicit videos/ messages during chats
- Threatening to physically assault the child or his/her family
- Using multiple identities to contact the child
- Pretending to be younger and/or a member of the opposite sex
- Hacking accounts to steal sexual images, or
- Threatening to commit suicide if no images are sent

VS

When It's Someone Known

Acquire the Image

Often, the extorter is an ex-romantic partner who may have received the image deliberately from the victim while involved in a relationship.

Threaten

The extorter may use the threat of spreading the image to force the victim into staying in/ returning to the relationship after it has ended, or to acquire additional sexual content.

Persist

The harassment rarely stops if a victim complies with the extorter's demands.

What Can I Do About It?

Talk About Technology

Children should grow up expecting that their parents are a part of their digital lives. Regular check-ins about their online interactions should be the norm. Include children in setting rules and limits for their tech-time.

Talk About Sexuality and Relationships

Talking about your family's expectations and values regarding sex and relationships is an important first step. These conversations should happen regularly. Be sure to discuss the characteristics of healthy relationships, such as having and respecting boundaries and practicing consent. Explain that both pressuring someone and being pressured into sexual behaviors that are uncomfortable or unsafe are NOT OK. Similarly, help children understand that they should never forward sexts they may receive from others. Limiting the image's spread reduces the risk of it falling into dangerous hands.

NetSmartz®

For more resources, visit **MissingKids.org/NetSmartz**

A program of the NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN®

ConnectSafely

QUICK-GUIDE TO

Snapchat Reporting

Snapchat has an in-app reporting feature that allows anyone on Snapchat to flag and report concerning or inappropriate content that might violate their Community Guidelines and Terms of Service. There are many questions and misconceptions about reporting, and this guide will help answer those questions and debunk top myths.

Why is it important to report? Snapchat is a community, and we're all in this together. Reporting inappropriate or dangerous content helps protect everyone on the platform.

What kind of content isn't allowed on Snapchat? Snapchat prohibits harassment, bullying, hate speech, impersonation, threats, criminal activity and other harms. Read through Snapchat's easy to understand Community Guidelines and its Terms of Service to familiarize yourself with what's not allowed.

How do I make a report? To report, press and hold on a Snap or Story and select the flag or report icon.

Will the person know I reported them? No. All reports are strictly confidential. Snapchat will never tell the person being reported who reported them. Depending on the nature of the report, Snapchat may need to inform law enforcement, but thankfully this isn't common. If you encounter anything that appears to be illegal or dangerous, or if you have reason to believe someone is at risk of harm or self-harm, immediately contact local law enforcement and report it to Snapchat. (See sidebar, next page, for additional resources.)

What happens after I submit a report? Someone on Snapchat's Trust & Safety Team reviews all reports. If they find the content violates Snapchat's Community Guidelines, they may remove the content or suspend the account. Only if necessary will they reach out to law enforcement.

Parents Ask: What are the Best Ways to Stay Safe on Snapchat?

Snapchat is primarily for communicating with close friends and family, and its privacy settings are on by default for all features, such as location-sharing and user profiles. The app only allows two friends to contact each other if they both accept their friend requests, and also limits the size of group conversations. It's important to talk to your kids about who their contacts are and make sure they're people they actually know in real life. You should also get familiar with the app's privacy and security settings, and make sure your kids understand them too. For example, set privacy settings to "Friends Only," which means only their approved contacts can see what they share. Remind your kids that they should speak to a trusted adult when they see something that concerns them, and avoid meeting up with people they don't actually know in real life.

Will Snapchat tell me what happened on something I've reported? Although they will review all reports, Snapchat does not let you know the outcome. They do provide statistics on reported content in their Transparency Report. In the second half of 2019, Snapchat took action against 3,788,227 pieces of content worldwide, or roughly .012% of total Story postings.

More Ways to Stay Safe on Snapchat

Privacy settings: Snapchat's privacy settings are essential to understand. The default "My Friends" setting allows people on your Friends list to contact you directly or view your Stories and location (if enabled). We recommend most people, especially anyone under 18, use this most restrictive setting instead of "Everyone." See more on Snapchat's privacy options.

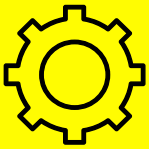
Blocking or removing: When you remove someone from your Friends list, they won't be able to view any of your private Stories, but they'll still be able to view any content you have set to public. Depending on your privacy settings, they may also be able to Chat or Snap you. When you block a friend, they won't be able to view your Story, send you Snaps, or send you Chats.

Need Additional Support?

Crisis Text Line provides additional support and resources to Snapchatters in the US. Text KIND to 741741 to chat with a live, trained crisis counselor. This service is free and available 24/7.

CyberTipline from the National Center for Missing & Exploited Kids receives reports of suspected online exploitation of children, including online enticement of children and child sexual abuse images, and works closely with law enforcement and tech companies. CyberTipline.org or 1-800-THE-LOST.

For more info about reporting, visit Snapchat.com/safety



We recommend most people, especially anyone under 18, use the default privacy setting "My Friends" instead of "Everyone."

About ConnectSafely

ConnectSafely is a Silicon Valley, California-based nonprofit organization dedicated to educating users of connected technology about safety, privacy and security. We publish research-based safety tips, parents' guidebooks, advice, news and commentary on all aspects of tech use and policy.

ConnectSafely

QUICK-GUIDE FOR PARENTS

TikTok

What is TikTok?

TikTok is an app that allows people to view, create and share short videos with friends, family, or the entire world. Although used by lots of adults of all ages, the app is especially popular with teens and young adults, who enjoy using its tools to combine video, popular songs, and graphics into fun sketches, creative shorts and viral videos.

Is TikTok safe for kids?

As with any social media app, a positive experience on TikTok ultimately depends on how it is used. TikTok has built-in safety and privacy features that vary based on the user's age. For example, kids under 13 access a different app experience called TikTok for Younger Users, which offers a curated feed of age-appropriate content. Teens 13-15 have private accounts by default and can't live stream or send direct messages.

Are TikTok accounts public or private?

For people under 16, TikTok accounts are automatically set to private. For people over 16, TikTok accounts are automatically set to public, but everyone has the option to set their profiles — and any TikToks they create — to private.

What are TikTok challenges?

Activities, dances — really anything that can go viral and inspire others to imitate the idea and spread it further. Participating in challenges can make people feel part of the broader TikTok community — say, by learning the latest dance and sharing their version of it — but people should exercise caution when participating in challenges, especially ones that may require a special skill. Talk to your kids about dangerous viral internet challenges and the peer pressure to participate.

Parents Ask: How Can I Keep My Kids Safe?

Start by talking with your teen about how they use TikTok. Make sure they understand that the videos and comments they post affect their or others' reputations and that they should never post anything that jeopardizes their privacy and security. Make sure your teen knows how to block anyone who bullies, threatens, or harasses them, or if they don't want that person to see their content or comment on their videos.

TikTok offers **Family Pairing**, which allows parents and guardians to pair their TikTok account with their teenager's account to guide their teen's use of the app. Parents can decide whether their child can search for content, users, songs or hashtags, set daily screen time (40 to 120 minutes a day), set the account to public or private, limit who can comment on their videos, turn off direct messaging and enable Restricted Mode, which "can limit content that may not be appropriate for some audiences."

More Ways to Stay Safe

Moderation and abuse reporting. To enforce its Community Guidelines, TikTok uses a combination of policies and human- and machine-based moderation practices to handle content that may violate its guidelines. To report a comment: Press and hold on the comment and select Report. To report an inappropriate video, tap the Share arrow and choose Report. Report a profile by going to the profile, tapping on the three dots and selecting Report.

Passwords and other personal information. Talk with your kids about the importance of keeping passwords and other personal information private. Friends can become ex-friends and use their account in mean or inappropriate ways. You'll find password tips at ConnectSafely.org/passwords.

Time management and life balance. Whether it's TikTok or any other app, teens (and adults too) need to put down their phones and interact with others in person. No app should ever keep you or your teen from getting exercise, doing chores, work or anything else that keeps us healthy, happy, and productive. If you need a nudge, use the time management features in the TikTok app or Apple and Android phones.

A note about parental controls. Parental controls have their place, but sometimes conversations can accomplish even more. For general advice on parental controls, including suggestions for talking about them with your kids, visit Connectsafely.org/controls.

For more info, visit ConnectSafely.org/TikTok

Parents can enable Restricted Mode to limit the appearance of content that may not be appropriate for all ages.

About ConnectSafely

ConnectSafely is a Silicon Valley, California-based nonprofit organization dedicated to educating users of connected technology about safety, privacy and security. We publish research-based safety tips, parents' guidebooks, advice, news and commentary on all aspects of tech use and policy.

Revised 5/13/21