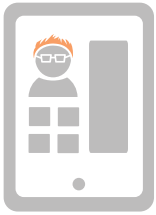
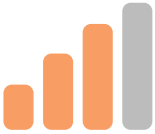
# NET CETERA

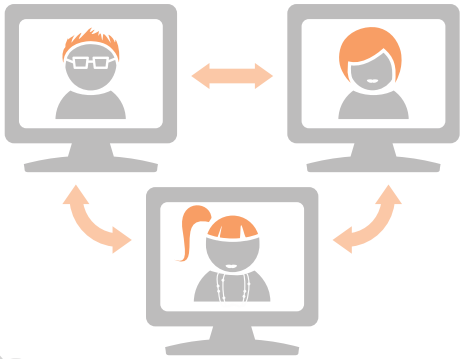
## Chatting with Kids About Being Online





# People of all ages are:

connecting with friends and family online





downloading apps and accessing content

sharing what they're doing — and where they are

sharing photos and videos from mobile devices

building online profiles and reputations

Communicating online is a way of life, yet it comes with certain risks:

- **Inappropriate conduct**
  The online world can feel anonymous. Kids sometimes forget that they're still accountable for their actions.
- **Inappropriate contact**
  Some people online have bad intentions. They might be bullies, predators, hackers, or scammers.
- **Inappropriate content**
  You may be concerned that your kids could find pornography, violence, or hate speech online.

Technology is constantly evolving. So are the risks associated with it. You can reduce these risks by talking to your kids about how they communicate — online and off — and encouraging them to think critically and act in a way they can be proud of.

**This guide from the Federal Trade Commission covers issues to raise with kids about living their lives online.**


Talking to Your Kids . . . . . 2

Communicating at Different Ages . . . . . 4

Socializing Online . . . . . 8

Using Mobile Devices . . . . . 12

Making Computer Security a Habit . . . . . 18

Protecting Your Child's Privacy . . . . . 23

# TALKING TO YOUR KIDS

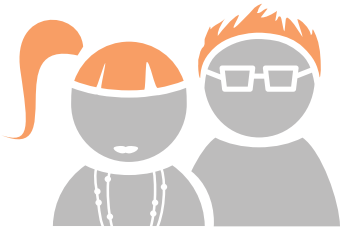
The best way to protect your kids online? Talk to them. While kids value the opinions of their peers, most tend to rely on their parents for help on the issues that matter most.

## Start early.

Young kids see their parents using all kinds of devices — and also might be playing games or watching shows on them. As soon as your child starts using a phone, mobile device, or computer, it's time to talk to them about online behavior and safety.

## Initiate conversations.

Even if your kids are comfortable approaching you, don't wait for them to start the conversation. Use everyday opportunities to talk to your kids about being online. For example, news stories about cyberbullying or texting while driving can spur a conversation with kids about their experiences and your expectations.



## Communicate your expectations.

Be honest about your expectations and how they apply in an online context. Communicating your values clearly can help your kids make smarter and more thoughtful decisions when they face tricky situations. For instance, be specific about what's off-limits — and what you consider to be unacceptable behavior.

## Be patient and supportive.

Resist the urge to rush through these conversations with your kids. Most kids need to hear information repeated, in small doses, for it to sink in. If you keep talking with your kids, your patience and persistence will pay off in the long run.

Work hard to keep the lines of communication open, even if you learn your kid has done something online that you find inappropriate.

Listening and taking their feelings into account helps keep conversations afloat. You may not have all the answers, and being honest about that can go a long way.

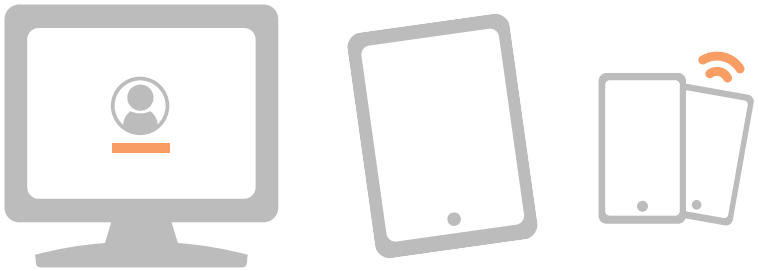
# COMMUNICATING AT DIFFERENT AGES

## Young Kids

### Supervision is important.

When very young children start using mobile devices or a computer, they should be supervised closely by a parent or caregiver. If little kids aren't supervised online, they may stumble onto content that could scare or confuse them.

When you're comfortable that your young children are ready to explore on their own, it's still important to stay in close touch. You may want to restrict them to sites or apps that you've visited and know to be appropriate — at least in terms of their educational or entertainment value.





### Consider parental controls.

If you're concerned about what your kids see online, consider tools with these features:

- **Filtering and blocking.** These tools limit access to certain sites, apps, words, or images. Some products decide what's filtered; others leave that to parents.
- **Blocking outgoing content.** This software prevents kids from sharing personal information online or via email.
- **Limiting time.** This software allows you to limit your kid's time online and set the time of day they can access the internet.
- **Browsers for kids.** These browsers filter words or images you don't want your kids to see.
- **Kid-oriented search engines.** These perform limited searches or filter search results for sites and material appropriate for kids.
- **Monitoring tools.** Software that alerts parents to online activity without blocking access. Some tools record the addresses of websites a child has visited; others provide a warning message when a kid visits certain sites. Monitoring tools can be used with or without a kid's knowledge.
- **Disabling in-app purchases from your device.** These settings can limit or keep kids from making in-app purchases from your device.

## Tweens

Tweens need to feel "independent" but not alone as they start exploring on their own. Many 8- to 12-year-olds are adept at finding information online, but they still need guidance to help them understand which sources are trustworthy.

### Think about limits.

Consider setting limits on how long and how often they can be online — whether on computers, phones, or other mobile devices. For younger tweens, parental controls can be effective. However, many middle school kids have the technical know-how to get around those controls.

## Teens

Teens are forming their own values and beginning to take on the values of their peers. Many are eager to experience more independence from their parents. However, they need to learn how to exercise judgment about being safe online and act in accordance with their family ethic.

Teens have more internet access through mobile devices — as well as more time to themselves — so it isn't realistic for you to try to be in the same room when they're online. They need to know that you and other family members can ask them about what they're doing online.



## WHAT CAN YOU DO?

### Talk about credibility.

It's important to emphasize the concept of credibility. Even the most tech-savvy kids need to understand that:

- not everything they see on the internet is true
- information or images they share can be seen far and wide
- people online may not be who they appear to be or say they are
- once something is posted online, it's nearly impossible to "take it back"

### Talk about manners.

Because they don't see facial expressions, body language, and other visual cues, teens and tweens may feel free to do or say things online that they wouldn't offline. Remind them that real people with real feelings are behind profiles, screen names, and avatars.

### Talk about expectations.

When you talk to your kids, set reasonable expectations. Anticipate how you will react if you find out that they've done something online you don't approve of.

If your child confides in you about something scary or inappropriate they've encountered online, try to work together to prevent it from happening again.

# SOCIALIZING ONLINE

Kids share pictures, videos, thoughts, plans, and their whereabouts with friends, family, and sometimes, the world at large. Socializing online can help kids connect with others, but it's important to help your child learn how to navigate these spaces safely.

## Oversharing

Some pitfalls that come with online socializing are sharing too much information, or posting pictures, videos, or words that can damage a reputation or hurt someone's feelings.

## WHAT CAN YOU DO?

### Remind your kids that online actions have consequences.

The words kids write and the images they post have consequences offline.

- **Kids should post only what they're comfortable with others seeing.** Parts of your children's profiles may be seen by a broader audience than you — or they — are comfortable with, even if they use privacy settings. Encourage your kids to think about the language they use online, and to think before posting pictures and videos, or altering photos posted by someone else. Employers, college admissions officers, coaches, teachers, and the police may view these posts.
- **Remind kids that once they post it, they can't take it back.** Even if they delete the information from a site, they have little control over older versions that may be saved on other people's devices and may circulate online. And a message that's supposed to disappear from a friend's phone? There are still ways to save it.

### Tell kids to limit what they share.

- **Help your kids understand what information should stay private.** Tell them why it's important to keep some things to themselves. Information like their Social Security number, street address, phone number, and family financial information is private and should stay that way.
- **Talk to your teens about avoiding sex talk online.** Teens who don't talk about sex with strangers online are less likely to come in contact with predators. In fact, researchers have found that predators usually don't pose as children or teens, and most teens who are contacted by adults they don't know find it creepy. Teens should ignore or block them, and trust their gut when something feels wrong.
- **Tell kids it's more than what they post.** Information may be collected and shared even if kids are not posting it. For example, what sites they visit, social media activity, or answers on quizzes may be shared or used for advertising.

### Limit access to your kids' profiles.

- **Use privacy settings.** Many social networking sites, chat, and video accounts have adjustable privacy settings, so you and your kids can restrict who has access to kids' profiles. Talk to your kids about the

importance of these settings, and your expectations for who should be allowed to view their profile.

- **Review your child's friends list.** Suggest that your kids limit online "friends" to people they actually know. Ask about who they're talking to online.

## Cyberbullying

Cyberbullying is bullying or harassment that happens online. It can happen in an email, a text message, an online game, or on a social networking site. It might involve rumors or images posted on someone's profile or circulated for others to see.

## WHAT CAN YOU DO?

### Help prevent cyberbullying.

- **Talk to your kids about bullying.** Tell your kids that they can't hide behind the words they type and the images they post or send. Bullying is a lose-lose situation: Hurtful messages make the target feel bad, and they make the sender look bad. Often they can bring scorn from peers and punishment from authorities.
- **Recognize the signs of a cyberbully.** Cyberbullying often involves mean-spirited comments. Check out your kid's social networking pages from time to time to see what you find.



Could your kid be the bully? Look for signs of bullying behavior, such as creating mean images of another kid.

- **Encourage your kids to speak up.** Cyberbullying usually stops pretty quickly when someone speaks up. If your kids see cyberbullying happening to someone else, encourage them to try to stop it by telling the bully to stop, and by not engaging or forwarding anything. If your kid sees a friend post something thoughtless, encourage them to talk to that friend.

Another way to help stop bullying online is to report it to the site or network where you see it.

### What to do about a cyberbully.

- **Don't react to the bully.** If your child is targeted by a cyberbully, keep a cool head. Remind your child that most people realize bullying is wrong. Tell your child not to respond in kind. Instead, encourage your kid to work with you to save the evidence and talk to you about it. If the bullying persists, share the record with school officials or local law enforcement.
- **Protect your child's profile.** If your child finds a profile that was created or altered without their permission, contact the site to have it taken down.
- **Block or delete the bully.** Delete the bully from friends lists or block their user name, email address, and phone number.

# USING MOBILE DEVICES

What age is appropriate for a kid to have a phone or a mobile device? That's something for you and your family to decide. Consider your kid's age, personality, maturity, and your family's circumstances.

## WHAT CAN YOU DO?

## Phones, Features, and Options

### Decide on the right options and features.

Your wireless company and mobile phone should give you some choices for privacy settings and child safety controls. Most carriers allow parents to turn off features like web access, texting, or downloading apps. You also can disable in-app purchases so your kid doesn't accidentally rack up huge charges playing their favorite game.

### Get smart about smartphones.

Many phones offer web access and mobile apps. If your children are going to use a phone and you're concerned about what they might find online, choose a phone with limited internet access or turn on web filtering.

### Get familiar with location-based services.

Many mobile phones have GPS technology installed. Kids with these phones can pinpoint where their friends are — and be pinpointed by their friends. Tell your kids to limit these features so they're not broadcasting their location to the world. Explain that there can be downsides to letting anyone and everyone know where they are. But there also are GPS services (offered by some carriers) that let parents map their kid's location.

### Password protect phones.

A password, numeric code, gesture, or fingerprint can lock a phone from intruders. Not only can this prevent "pocket-dialing," but it also can help keep information and photos from falling into the wrong hands.

## Develop Rules

### Explain what you expect.

Talk to your kids about when and where it's appropriate to use their phones and other mobile devices. You also may want to establish rules for responsible use. Do you allow calls, texting, or playing games on apps at the dinner table? Do you have rules about cell phone use at night? Should they give you their phones while they're doing homework, or when they're supposed to be sleeping?

### Set an example.

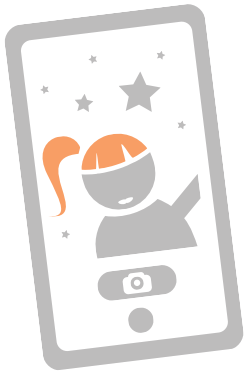
It's illegal to drive while texting or talking on the phone without a hands-free device in most states, but it's dangerous everywhere. Set an example for your kids, and talk to them about the dangers and consequences of distracted driving.

## Mobile Sharing and Networking

Socializing and sharing on-the-go can foster creativity and fun, but could cause problems related to personal reputation and safety.

### Use care when sharing photos and videos.

Most mobile phones have camera and video capability, making it easy for teens to capture and share every moment. Encourage kids to get permission from the photographer or the person in the shot before posting videos or photos. It's easier to be smart upfront about what media they share than to do damage control later.



### Use good judgment with social networking from a mobile device.

The filters you've installed on your home computer won't limit what kids can do on a mobile device. Talk to your teens about using good sense when they're social networking from their phones, too.

## Mobile Apps

### What should I know about apps?

Apps might:

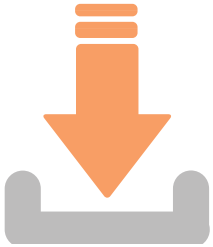
- collect and share personal information
- let your kids spend real money — even if the app is free
- include ads
- link to social media

But the apps might not tell you they're doing it.

### WHAT CAN YOU DO?

Here's what you and your kids can do to learn about an app before you download it:

- look at screen shots
- read the description, content rating, and user reviews
- do some research on the developer, including outside reviews from sources you respect
- check what information the app collects



### Can I restrict how my kids use apps?

Before you pass the phone or tablet to your kids, take a look at the settings. You may be able to:

- **restrict content** to what's right for your kid's age
- **set a password** so apps can't be downloaded without it, and kids can't buy stuff without it
- **turn off Wi-Fi and data services** or put the phone in airplane mode so it can't connect to the internet

The best way to keep up with kids' apps is to try them out yourself, and talk to your kids about your rules for buying and using apps.

## Texting

### Encourage manners.

If your kids are texting, encourage them to respect others. Texting shorthand can lead to misunderstandings. Tell them to think about how a text message might be read and understood before they send it.

### Safeguard privacy.

Remind your kids to:

- ignore texts from people they don't know
- learn how to block numbers from their cell phone
- avoid posting their cell phone number online
- never provide personal or financial information in response to a text

### Recognize text message spam.

Help your kids recognize text message spam and explain the consequences:

- it often uses the promise of free gifts — or asks you to verify account information — to get you to reveal personal information
- it can lead to unwanted charges on your cell phone bill
- it can slow cell phone performance

## WHAT CAN YOU DO?

Review your cell phone bill for unauthorized charges, and report them to your carrier. Tell your kids:

- **to delete messages that ask for personal information** — even if there's a promise of a free gift. Legitimate companies don't ask for information like account numbers or passwords by email or text.
- **not to reply to — or click on — links in the message.** Links can install malware and take you to spoof sites that look real, but that exist to steal your information.

## Sexting: Don't Do It

Sending or forwarding sexually explicit photos, videos, or messages from a mobile device is known as "sexting." Tell your kids not to do it. In addition to risking their reputation and their friendships, they could be breaking the law if they create, forward, or even save this kind of message. Teens may be less likely to make a bad choice if they know the consequences.

# MAKING COMPUTER SECURITY A HABIT

The security of your computer, phone, and other mobile devices can affect the safety of your online experience — and that of your kids. Malware could allow someone to steal your family's personal or financial information. Malware is software that can:

- install viruses
- monitor or control your computer use
- send unwanted pop-up ads
- redirect your device to websites you're not looking for
- record your keystrokes

## WHAT CAN YOU DO?

- **Use security software and keep it updated.** Well-known companies offer plenty of free options. Set the software to update automatically.
- **Keep your operating system, web browser, and apps up to date.** Hackers take advantage of software that doesn't have the latest security updates.
- **If your family's accounts support multi-factor authentication, consider using it.** Using your password plus another piece of information to log in helps protect your account, even if your password is compromised. The second piece of information could be a code sent to your phone, or a random number generated by an app or token.



## Teaching Kids Computer Security

Talk to your kids about how they can help protect their devices and your family's personal information.

### Create strong passwords, and keep them private.

Take a look at the passwords that you and your kids use. To better protect your accounts, make passwords at least twelve characters that include upper- and lowercase letters, numbers, and symbols. Avoid common words and phrases, or information like your address. Use different passwords for different accounts. That way, if a hacker gets into one account, he can't get into others.

### Don't provide personal or financial information unless the website is secure.

If you or your kids send messages, share photos, use social networks, or bank online, you're sending personal information over the internet. Teach your kids: if the URL doesn't start with **https**, don't enter any personal information. That "s" means the information you're sending is encrypted and protected.

### Watch out for "free" stuff.

Free games, apps, music, and other downloads can hide malware. Don't download anything unless you trust the source. Teach your kids how to recognize reputable sources.

### Back up your files regularly.



No system is completely secure. If you or your kids have important files, copy them to an external hard drive or cloud storage. If your computer is attacked by malware, you'll still have access to your files.

### Secure your home network.

Your home has a wireless network if you use wireless internet there. Securing that network will protect your family's devices from hackers, along with protecting your personal or financial information.

Here are a few easy steps to secure your network:

- **Activate encryption.** Encryption scrambles the information you send over the internet into a code so others can't access it. It's the most effective way to secure your network.

  Your computer, router, and other equipment must use the same encryption. WPA2 is strongest; use it if you have a choice.

- **Change your router's pre-set password(s).** Hackers know the default passwords, so change it to something more complex (see password tips on p. 19).

- **Keep your router up to date.** Just like your other devices, the software on your router needs occasional updates to be secure and effective.



## Using Public Wi-Fi Securely

Many public places — like coffee shops, libraries, and airports — offer Wi-Fi hotspots. These hotspots can be convenient, but they're often not secure. That could make it easy for someone else to access your family's online accounts or steal your personal information — including private documents, photos, and passwords.

### WHAT CAN YOU DO?

### Don't use Wi-Fi to access personal or financial information.

Remind your kids that Wi-Fi is unsecured. That means other users on the network can see what you see and send. Your family's personal information, private documents, login credentials and more could be up for grabs.

The easiest solution? Make it a family policy to save your online shopping, banking, and other personal transactions for when you are on your home network. Then make sure your home network is encrypted. If you're on the go, use your mobile data — and tell your kids to do the same.

### Use secure websites.

A secure site will encrypt your information while you are signed in to it — even if the network doesn't. How will your kids know if a site is secure? Tell them to look for **https** in the web address of every page they visit — not just when they log in.

### Don't stay permanently signed in to accounts.

Recommend that your kids log out when they've finished using a site.

## Phishing Scams

Phishing is when scam artists send texts, emails, or pop-up messages to get people to share their personal and financial information. Scammers use this information to access your accounts, steal your identity, and commit fraud.

### WHAT CAN YOU DO?

Here's how you and your kids can avoid getting tricked by scam artists.

- **Don't reply to texts, emails, or pop-up messages that ask for personal or financial information**, and don't click on any links in the message.
- **Be cautious about opening any attachments** or downloading any files from emails you receive, regardless of who sent them. Unexpected files may contain viruses that your friends or family members didn't know were there.
- **Get your kids involved**, so they can develop their scam "antennas" and careful internet habits. Look for teachable moments — if you get a phishing message, show it to your kids to help them understand that things aren't always what they seem.

### How to report phishing scams.

Forward phishing emails to **Spam@UCE.gov**. They will be added to a database that law enforcement agencies use to pursue investigations. If you or your kids were tricked by a phishing scam, report it to **FTC.gov/Complaint**.



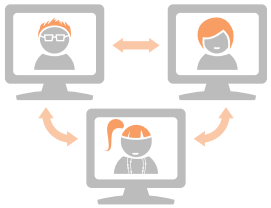
# PROTECTING YOUR CHILD'S PRIVACY

As a parent, you have control over the personal information companies collect online from your kids under 13. The Children's Online Privacy Protection Act (COPPA) gives you tools to do that.

The Federal Trade Commission enforces the COPPA Rule. If a site or service is covered by COPPA, it has to get your consent before collecting personal information from your child, and it has to honor your choices about how that information is used.

## What is COPPA?

The COPPA Rule was put in place to protect kids' personal information on websites and online services — including apps — that are directed to children under 13. The Rule also applies to a general audience site that knows it's collecting personal information from kids that age.



COPPA requires those sites and services to notify parents directly and get their approval before they collect, use, or disclose a child's personal information.

**Personal information in the world of COPPA includes, for example, a kid's:**

- name
- address
- Social Security number
- photos, videos, and audio recordings of the child
- persistent identifiers, like IP addresses, that can be used to track a child's activities over time and across different websites and online services
- phone number or email address
- physical whereabouts

## How Does COPPA Work?

Let's say your child wants to use features on a site or download an app that collects their personal information. Before they can, you should get a plain language notice about what information the site will collect, how it will use it, and how you can provide your consent.

The notice should link to a privacy policy that's easy to understand. The privacy policy must give details about the kind of information the site collects, and what it might do with the information — say, if it plans to use the information to target advertising to a child, or give or sell the information to other companies. In addition, the policy should tell you how to contact someone who can answer your questions.

Sites and services have some flexibility in how they get your consent. For example, some may ask you to send back a permission slip.

Others may have a toll-free number you can call. If you agree to let the site or service collect personal information from your child, it has a legal obligation to keep it secure.

## What Are Your Choices?

- **Understand the site's information practices.** Start by reading how the company plans to use your child's information.
- **Be picky with your permission.** Decide how much consent you want to give. For example, you might give the company permission to collect your child's personal information, but not allow it to share that information with others.
- **Know your rights.** Once you give a site or service permission to collect personal information from your child, you're still in control. As the parent, you have the right to review the information collected about your child. If you ask to see the information, keep in mind that website operators need to make sure you are the parent before providing you access. You also have the right to retract your consent any time, and to have information collected about your child deleted.

### What if it looks like a site or service is breaking the rules?

If you think a site has collected information from your kids or marketed to them in a way that violates the law, report it to the FTC at **FTC.gov/Complaint**.

# FTC.gov/KidsOnline

To order brochures about keeping kids safe online, visit **FTC.gov/Bulkorder**.

STOP | THINK | CONNECT™

Federal Trade Commission // May 2018