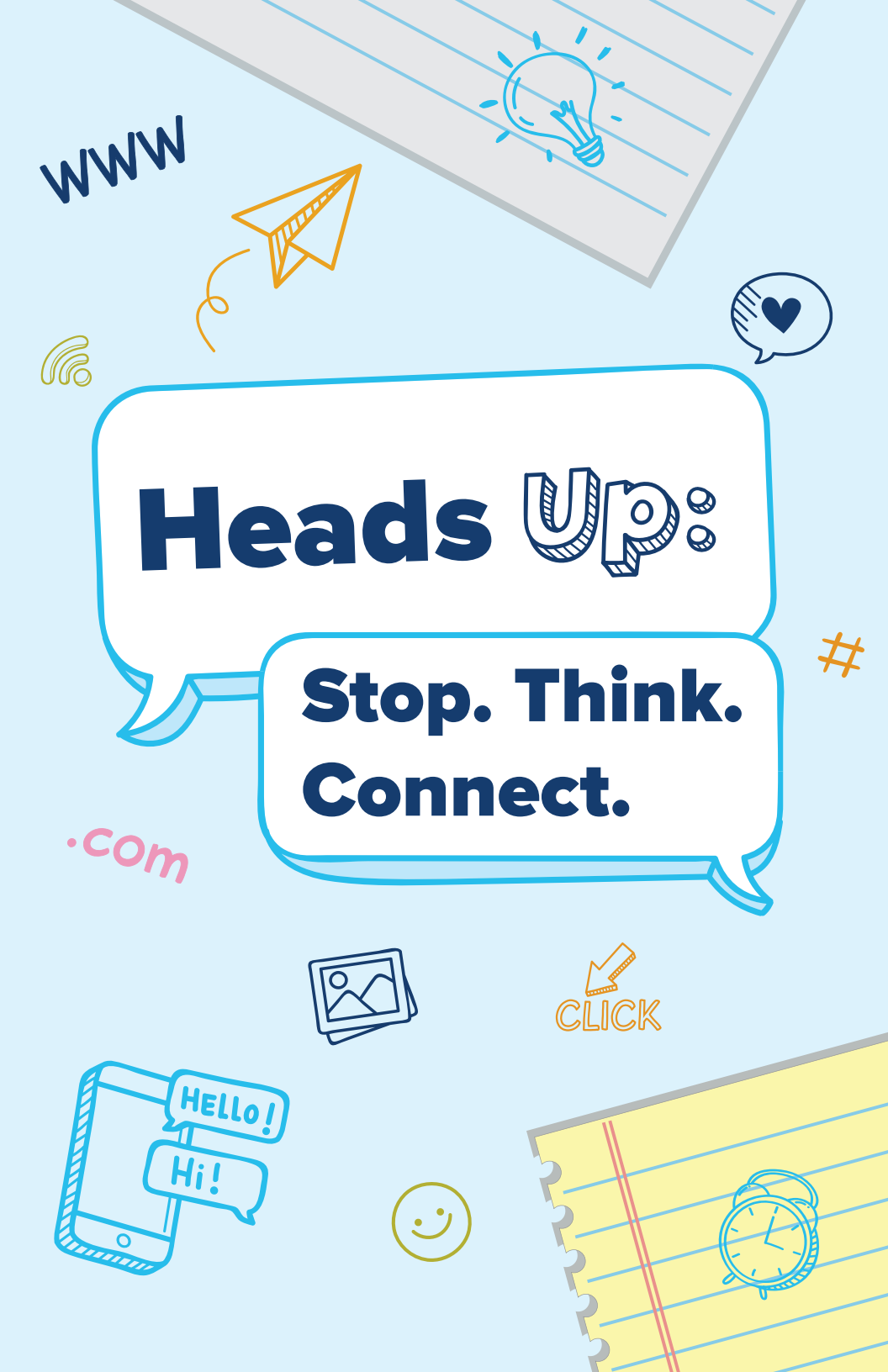
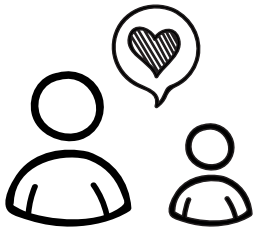

WWW
Heads Up:
Stop. Think.
Connect.
.com
CLICK
HELLO!
Hi!



To help kids in your life be safe online, *Heads Up: Stop. Think. Connect.* has some ideas to help you start a conversation with them. Pick a section and read it together to see how to share with care, be kind online, stand up to cyberbullying, and protect their (and your) personal information online. These tools can help you show kids how to make good choices and use technology responsibly. And, by talking with them, you let kids know they have a trusted adult to help them when they make mistakes.

Being online is a part of your life. You watch and create content, post photos and videos, play games, and share where you are and what you're doing with your friends and family. But there are risks when you post, play, and connect online. Some people and situations you face aren't always what they seem.

Regardless of how fast your fingers fly on a keyboard, phone, or tablet, the best tools you have for avoiding risks online are your brain and time. Stop and think through situations to help protect yourself, your friends and family, your accounts, and your devices. Or you may end up over sharing, embarrassing yourself or others, messing up your computer, or talking to people who aren't who they say they are.

- ✓ SHARE WITH CARE
- ✓ IT'S COOL TO BE KIND
- ✓ STAND UP TO CYBERBULLYING
- ✓ THE PROTECTION CONNECTION

SHARE WITH CARE



Think before you share

What you do online has real-world consequences. The photos, videos, and messages you share affect you, your privacy, your reputation, and those of the people around you — now and in the future. Stop and think before you post.

What you post could have a bigger "audience" than you think.

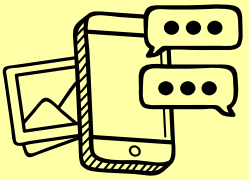
It's impossible to completely control who sees your profile, pictures, videos, or texts — even if you use privacy settings or apps that delete your content after it's viewed or within 24 hours. Anybody who sees your post can take a screenshot or recording. Ask yourself: "Would I want someone to stand up in the middle of lunchtime and share that photo or video with the entire cafeteria?"

What you share might affect others. It can be embarrassing, unfair, and even unsafe to send or post photos and videos without getting permission from the people in them. Get someone's OK first. Before you post, ask them: "Are you okay if I post this on social?" If they say no, don't post it.

Once you post something online, you can't take it back

Even if you delete something you've posted — or the post expires — that photo or comment you don't want people to see anymore could be saved, shared, and live somewhere online — permanently.

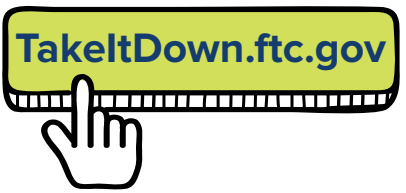
Sexting: Don't do it



You may have heard stories at school or in the news about people "sexting" — sending nude photos from their phones. Don't do it. Period. Creating, forwarding, or even saving sexually explicit photos, videos, or messages puts your friendships and reputation at risk. Worse yet, you could be breaking the law.

Did someone share an explicit photo or video of a child online?

Learn what to do and find help at



A note about social media



According to the U.S. Surgeon General, using social media can hurt you, depending on how much time you spend on the platforms, the type of content you see, and how much it disrupts things like your sleep or exercise — those activities that are essential for your health.

IT'S COOL TO BE KIND



Politeness counts

When you can't see someone's facial expressions, body language, or other visual cues online, you might feel free to post or say things you wouldn't say in person. But texting, posting, direct messaging, playing video games, and emailing are the same as talking to someone face to face. Be mindful about how you communicate and think before you speak or post.

Slow down. It's easy to have misunderstandings online. Before you send a message, ask yourself: "How will this message make other people feel?"



Consider and respect other people's perspectives and feelings online — just like you would in person. Remember: there are real people behind the avatars and profile names.

Tone it down. Don't use all CAPS, long rows of exclamation points, or large bolded fonts. It's the same as shouting.

Don't put everything in the group chat. Before you send a group message or hit Reply All, stop and think: Who needs to see this message?

Don't impersonate

It's wrong and potentially hurtful to create profiles, comments, or posts that seem to come from someone else, like someone in your class or a teacher.

Speak up

If you see a friend post something thoughtless or unsafe, tell them. You may keep your friend out of trouble and from embarrassing themselves. If you see something inappropriate online, report it and tell a trusted adult. Most apps and platforms have a way to report if someone's behavior is threatening or inappropriate.

STAND UP TO CYBERBULLYING



Everyone deserves to feel safe in their daily interactions with other people, whether they're online or face to face.

If someone posts mean comments, hurtful memes, embarrassing pictures, or sends chats or private messages about you, that's bullying. It's not okay. Talk with a trusted adult to get help with the situation and decide how you should respond.

If someone harasses you online, here's what to do:

- **Ignore** the person or block them from contacting you further.
- **Save the records** and ask for help from a trusted adult.
- **Report it.** Many apps and platforms have tools to report someone for inappropriate or threatening behavior.

Bullying often makes the person being harassed feel bad — and it makes the bully look bad.

Bullying could also get you in trouble with your school or the police.

If you witness cyberbullying, find ways to become an upstander — someone who intervenes, interrupts, or speaks up to stop bullying. Mean behavior usually stops pretty quickly when someone stands up for the person being bullied.

THE PROTECTION CONNECTION



Protect your privacy

When you do anything online, you leave a trail. Take these steps to make sure that trail doesn't lead to information you may not have intended to share.

Use privacy settings. Find out how to turn on privacy settings for devices, apps, and social media accounts — then do it. This helps you limit who can see where you are, what you post, and who can connect with you.

Check your location settings. Some apps let you see where your friends are. They also share where you are. Think about when it makes sense to share your location. When it doesn't, turn off

location sharing. Features on your devices, like the camera, might have information about where you were when you took a photo. If you don't want to broadcast where you were for every selfie, turn off your location on your phone's camera. Always ask yourself: "Does this app need to know where I am?"



Limit your online friends to people you actually know. Connecting with friends through text, social media, or video games might be fun — but some people aren't who they say they are online. And if you're not careful, you might share personal information with a stranger.

Protect your information

> **Once you give your personal information — like your Social Security number, passwords, or bank account information — to someone you don't know, there's no way to get it back.**

Here's how to protect your information online:

Don't reply to messages that ask for personal information. Even if the message looks like it's from a friend, family member, or a company you know — or says something bad will happen if you don't

reply. Chances are, it's a fake and sent to steal your information. Get a trusted adult to help you report the message as junk or spam.

Check what information an app wants access to — before you download it. Some apps request permission to access information or features they don't need, like your contact list, camera, storage, location, and microphone. Ask a trusted adult for help reading the app's privacy policy to see how your data will be used and if it will be shared. Then decide whether that word game really needs to access your photos.

Talk with a trusted adult before making in-app purchases — especially if they're paying for them.

Protect your accounts

You keep lots of personal information in your online accounts. Here are some steps to take to keep other people out of your accounts.

Create strong passwords.
The longer your password, the harder it is to crack. Use at least 12 characters with a mix of uppercase and lowercase letters, numbers, and symbols. Consider using a passphrase of random words to

make it more memorable. But don't use common phrases, song lyrics, or movie quotes that are easy to guess.

Be unique. Come up with different passwords for your different accounts. That way, if someone gets your password for one account, they can't use it to get into your other accounts. One way to keep track of all your different passwords is to use a password manager.

Keep them private. Don't share your passwords with anybody, not even your best friend or someone you're dating.

Be picky about security questions. Try to choose

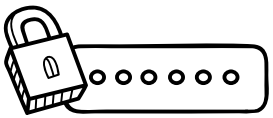


security questions only you can answer. Skip questions with answers someone could find online — like your zip code, birthplace, or mother's maiden name. If you can't avoid those questions, get creative! Treat them like passwords and use random and long answers. Just be sure you remember your answers.

Use multi-factor authentication. Many accounts offer extra protection to your accounts by using "multi-factor authentication" — requiring something in

addition to just a password. Multi-factor authentication combines something you know (like a password) with something you have (like a passcode generated by an app) or something you are (like a fingerprint).

Change passwords quickly if there's a breach. If a company tells you there was a data breach where a hacker could have gotten your password, change the password you use with that account right away. Change it for any account that uses a similar password, too.



Protect your devices

The best way to enjoy being online? Making sure your devices are safe and secure. Start here:

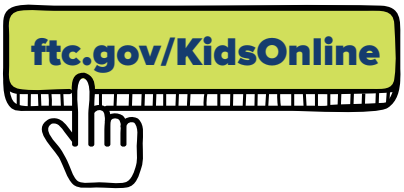
Set security software to update automatically for all of your devices, internet browsers, and operating system. This helps you protect against new security threats.

Don't click links or open attachments. If you get an unexpected text, email, or message online that tells you to click a link or open an attachment, don't do it! Even if it's an offer for free stuff. Links and attachments may hide viruses or spyware that could mess up your phone, computer, or tablet.

Password-protect your devices. It'll help keep your photos, messages, and accounts from falling into the wrong hands.

Keep them in a safe place. Whether it's your phone, laptop, or tablet, don't leave it in public — even for a minute.

Learn more at ftc.gov/KidsOnline



To get free copies of this brochure, visit

ftc.gov/bulkorder

FEDERAL TRADE COMMISSION

August 2023