

Protecting Kids' Privacy Online

Quick Facts

Your kids' personal information and privacy are valuable — to you, to them, and to marketers. Fortunately, there are ways you can safeguard that privacy when your kids are online.

- Check out sites your kids visit, and see what kind of information the sites ask for or allow kids to post.
- Talk to your child about the risks and benefits of disclosing certain information, especially in a public forum.
- Take a look at the privacy policy, which should say what the site does with the information it collects. Then you can decide how you feel about it.
- Ask questions. If you're not clear on a site's practices or policies, ask about them.
- Be selective with your permission. In many cases, websites need your okay before they're allowed to collect personal information from your kids.
- Know your rights. For example, as a parent, you have the right to have a site delete any personal information it has about your child.
- Report a website. If you think a site has collected or disclosed information from your kids or marketed to them in a way that violates the law, report it to the FTC.

Whether to study or socialize, play games or learn something new, it's likely your kids are spending time online. And as a parent, chances are that you're spending time thinking about ways to make sure they make smart and safe choices when they do. Among the many choices they're faced with online is how to deal with their personal information.

The Children's Online Privacy Protection Act — COPPA — gives parents control over what information websites can collect from their kids. Any website for kids under 13, or any general site that collects personal information from kids it knows are under 13, is required to comply with COPPA. The Federal Trade Commission, the nation's consumer protection agency, enforces this law.

Thanks to COPPA, sites have to get a parent's permission if they want to collect or share your kids' personal information, with only a few exceptions.

That goes for information sites ask for up front, and information your kids choose to post about themselves. Personal information includes your child's full name, address, email address, or cell phone number.

Under COPPA, sites also have to post privacy policies that give details about what kind of information they collect from kids — and what they might do with it (say, to send a weekly newsletter, direct advertising to them, or give the information to other companies).

If a site plans to share the child's information with another company, the privacy policy must say what that company will do with it. Links to the policies should be in places where they're easy to spot.

What Can You Do?

Your kids' personal information and privacy are valuable — to you, to them, and to marketers. Here's how to help protect your kids' personal information when they're online.



Check out sites your kids visit. If a site requires users to register, see what kind of information it asks for and whether you're comfortable with what they tell you. If the site allows kids to post information about themselves, talk to your child about the risks and benefits of disclosing certain information in a public forum. You also can see whether the site appears to be following the most basic COPPA requirements, like clearly posting its privacy policy for parents and asking for parental consent before kids can participate.

Take a look at the privacy policy. Just because a site has a privacy policy doesn't mean it keeps personal

continued on Page 2

information private. The policy should tell you what the site does with the information it collects; then, you can decide how you feel about it. Remember, if the policy says there are no limits to what it collects or who gets to see it, there are no limits.



Ask questions. If you're not clear on a site's practices or policies, ask about them. If the site falls under COPPA, the privacy policy has to include contact information for the site manager.

Be selective with your permission. In many cases, websites need your okay before they're allowed to collect personal information from your kids. They may ask for your permission in a number of ways, including email or postal mail. Or, you may give your consent by allowing them to charge your credit card. In addition to considering when to give your permission, consider how much consent you want to give — in many cases, it's not all or none. You might be able to give the company permission to collect some personal information from your child, but say no to having that information passed along to another marketer.

Know your rights. As a parent, you have the right to have a site delete any personal information it has about your child. Some sites will let you see the information they've collected. But first, they'll need to make sure you really are the parent, either by requiring a signed form or an email with a digital signature, for example, or by verifying a charge made to your credit card. You also have a right to take back your consent and have any information collected from your child deleted.

Report a website. If you think a site has collected or disclosed information from your kids or marketed to them in a way that violates the law, report it to the FTC at <https://www.ftccomplaintassistant.gov> or 1-877-FTC-HELP (382-4357).

More Tips for Parents

Talk, and talk often. Make sure your kids know what information should be private, and what information might be appropriate for sharing. When they give out their personal information, they give up control of who can reach them, whether it's with a marketing message or something more personal. On the other hand, sharing some personal information may allow them to participate in certain activities or to get emails about promotions and events they're interested in.

Depending on what they do online, also remind your kids that once they post information online, they can't take it back. Even if they delete the information from a site, older versions may exist on other people's computers and be circulated online.

Know what sites your kids go to. Talk with your kids about the sites they like to visit. Do some exploring on your own to get to know how the sites work and what privacy settings and controls they offer.

Make agreements. Be sure your kids know what your family has decided is okay — and not okay — to divulge online. Consider writing down a list of the rules your family has agreed on, and posting them where everyone can see them.

Let your kids know you'll keep an eye on the sites they visit. One option is to check your browser history and temporary files, though keep in mind that older kids may know how to delete these files or keep them from getting recorded. If you'd like more controls, check to see what privacy settings your browser offers or consider software that offers a range of controls. Visit <http://kids.getnetwise.org> to learn more.

Know how your kids get online. Kids may get online using your family computer or someone else's, as well as through cell phones and game consoles. Know what limits you can place on your child's cell phone - some companies have plans that limit downloads, Internet access, and texting on cell phones; other plans allow kids to use those features at certain times of day. Check out what parental controls are available on the gaming consoles your kids use, as well.

By OnGuard Online. Public domain

Additional article on Internet security

Visit the Live And Work Well website, liveandworkwell.com, to access the article "Stop. Think. Click. 7 Practices for Safer Computing."

Cyberbullying

What is Cyberbullying?

Cyberbullying is bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and websites.

Examples of cyberbullying include mean text messages or emails, rumors sent by email or posted on social networking sites, and embarrassing pictures, videos, websites, or fake profiles.

Why Cyberbullying is Different

Kids who are being cyberbullied are often bullied in person as well. Additionally, kids who are cyberbullied have a harder time getting away from the behavior.

- Cyberbullying can happen 24 hours a day, 7 days a week, and reach a kid even when he or she is alone. It can happen any time of the day or night.
- Cyberbullying messages and images can be posted anonymously and distributed quickly to a very wide audience. It can be difficult and sometimes impossible to trace the source.
- Deleting inappropriate or harassing messages, texts, and pictures is extremely difficult after they have been posted or sent.

Effects of Cyberbullying

Cell phones and computers themselves are not to blame for cyberbullying. Social media sites can be used for positive activities, like connecting kids with friends and family, helping students with school, and for entertainment. But these tools can also be used to hurt other people. Whether done in person or through technology, the effects of bullying are similar.

Kids who are cyberbullied are more likely to:

- Use alcohol and drugs
- Skip school
- Experience in-person bullying
- Be unwilling to attend school
- Receive poor grades
- Have lower self-esteem
- Have more health problems

October is Cyber Security Awareness Month

To help you stay safer and more secure online, visit the STOP.THINK.CONNECT website at stopthinkconnect.org. The U.S. Department of Homeland Security endorses the STOP.THINK.CONNECT federal campaign.

Prevent Cyberbullying

Parents and kids can prevent cyberbullying. Together, they can explore safe ways to use technology.

Be Aware of What Your Kids are Doing Online

Talk with your kids about cyberbullying and other online issues regularly.

- Know the sites your kids visit and their online activities. Ask where they're going, what they're doing, and who they're doing it with.
- Tell your kids that as a responsible parent you may review their online communications if you think there is reason for concern. Installing parental control filtering software or monitoring programs are one option for monitoring your child's online behavior, but do not rely solely on these tools.
- Have a sense of what they do online and in texts. Learn about the sites they like. Try out the devices they use.
- Ask for their passwords, but tell them you'll only use them in case of emergency.
- Ask to "friend" or "follow" your kids on social media sites or ask another trusted adult to do so.
- Encourage your kids to tell you immediately if they are, or someone they know is being cyberbullied.



Explain that you will not take away their computers or cell phones if they confide in you about a problem they are having.

Establish Rules about Technology Use

Establish rules about appropriate use of computers, cell phones, and other technology. For example, be clear about what sites they can visit and what they are permitted to do when they're online. Show them how to be safe online.

Help them be smart about what they post or say. Tell them not to share anything that could hurt or embarrass themselves or others. Once something is posted, it is out of their control whether someone else will forward it.

continued on Page 4

OEAP Awareness Training

9 to 11 a.m., Oct. 29, 2014

4200 Surface Road

Discover how the OEAP can assist you with your professional, personal and behavioral health concerns. Open to all state employees.

Encourage kids to think about who they want to see the information and pictures they post online. Should complete strangers see it? Real friends only? Friends of friends? Think about how people who aren't friends could use it.

Tell kids to keep their passwords safe and not share them with friends. Sharing passwords can compromise their control over their online identities and activities.

Understand School Rules

Some schools have developed policies on uses of technology that may affect the child's online behavior in and out of the classroom. Ask the school if they have developed a policy.

Report Cyberbullying

When cyberbullying happens, it is important to document and report the behavior so it can be addressed.

Steps to Take Immediately

- Don't respond to and don't forward cyberbullying messages.
- Keep evidence of cyberbullying. Record the dates, times, and descriptions of instances when cyberbullying has occurred. Save and print screenshots, emails, and text messages. Use this evidence to report cyberbullying to web and cell phone service providers.
- Block the person who is cyberbullying.
- Report Cyberbullying to Online Service Providers.
- Cyberbullying often violates the terms of service established by social media sites and internet service providers.
- Review their terms and conditions or rights and responsibilities sections. These describe content that is or is not appropriate.
- Visit social media safety centers to learn how to block users and change settings to control who can contact you.
- Report cyberbullying to the social media site so they can take action against users abusing the terms of service.

Report Cyberbullying to Law Enforcement

When cyberbullying involves these activities it is considered a crime and should be reported to law enforcement:

- Threats of violence
- Child pornography or sending sexually explicit messages or photos
- Taking a photo or video of someone in a place where he or she would expect privacy
- Stalking and hate crimes
- Some states consider other forms of cyberbullying criminal. Consult your state's law and law enforcement for additional guidance.

Report Cyberbullying to Schools

- Cyberbullying can create a disruptive environment at school and is often related to in-person bullying. The school can use the information to help inform prevention and response strategies.
- In many states, schools are required to address cyberbullying in their anti-bullying policy. Some state laws also cover off-campus behavior that creates a hostile school environment.

By Stop Bullying Now, U.S. Department of Health and Human Services. Public domain.



**OHIO EMPLOYEE
ASSISTANCE PROGRAM**

Your employee assistance program offers confidential help for personal problems

and concerns. Concerned about a troubled family member who won't get help? Feel tired and exhausted, but don't know if it's burnout, loss of motivation, depression or all three? Late for work too often? Has use of alcohol or drugs created a crisis you are facing right now? The bottom line, never wonder if your concern is appropriate to contact OEAP. So, if you've been putting off taking action to solve a serious issue that is weighing on you, give OEAP a call today.

30 E. Broad Street, 27th Floor
Columbus, OH 43215

800-221-6327/614-644-8545
www.ohio.gov/eap

Robert Blair, Director
Ohio Department of Administrative Services

Debora Branham, *Assistant Benefits Administrator*

Carrie McKean, *Administrative Professional*

OhioDAS
Service · Support · Solutions

Department of Administrative Services