

PROTECTING YOUR KIDS ONLINE 2.0

CONNECT

Set some ground rules.

Establish clear guidelines like what types of sites kids can visit, apps they can download, and when they can have access to electronics. Consider “blackout” periods that require disconnection.

Research before you buy.

It’s important to learn about a device’s capabilities before you buy. Will it allow unknown people to communicate with my child? Will this allow children to make unchecked purchases?

Go beyond safeguards.

Installing monitoring software doesn’t guarantee your child will be safe online. Time, attention and active conversation are the best tools to protect them.

REPORT!

If your kids are dealing with cyberbullies or potential online enticement, report it to the website, cell phone provider, law enforcement or CyberTipline.org

LEARN

Know the platforms.

Online enticement happens across all platforms, so be aware of the sites, games and apps your children frequent. Ask them to show you how they use them.

Be proactive.

Teach your kids to spot common tricks used by online offenders. In NCMEC CyberTipline reports, the most common tactics used to entice a child online were:

- Engaging the child in sexual conversation/roleplay as a grooming method.
- Directly asking the child for sexually explicit images of themselves, or offering to mutually exchange images.
- Developing a rapport with the child through compliments and other supportive behaviors such as “liking” their online posts.
- Sending unprompted sexually explicit images of themselves.
- Pretending to be younger.
- Offering incentives for explicit content.

Spot the Red Flags.

A child who is experiencing online enticement may be:

- Spending increasing time online.
- Getting upset when he or she is not allowed on their device.
- Taking extra steps to conceal what they are doing online.
- Receiving gifts from people you don’t know.

ENGAGE

Talk about it!

Your kids might not tell you everything, but ask anyway. Regular conversations about safety can go a long way in increasing trust and communication.

Get involved.

Challenge them to a duel. If you have kids who like to play online games, ask if you can play, too. When you respect their interests, they’re more likely to respect your rules.

Don’t pull the plug.

Taking away internet access because they may have made mistakes online doesn’t solve the problem. Talk to them about protecting themselves and respecting others online.



For more resources, visit MissingKids.org/NetSmartz

Copyright © 2010-2019 National Center for Missing & Exploited Children. All rights reserved.



Internet Safety at Home

As adults and children alike have turned to digital tools for school, work, and socialization, **online safety matters now more than ever.**

Here are **five tips** for keeping kids safer online, adapted to fit the current “safer at home” environment.

Tip 1:

Keep the Ground Rules



Even if our online habits have changed significantly, you can still set boundaries that work for your family and schedule. Involving children in setting these rules may help them stick to the guidelines.

Consider:

- Distance learning tasks **before** social media or gaming
- **No devices** during meals
- At least ____ **minutes** of non-electronic activities per day
- **“Digital curfew”**: no devices after a certain hour

Tip 2:

Modify How You Monitor



Even the strictest monitoring programs and content blockers can't ensure that children are totally protected online. The best tools for keeping kids safe are time, attention and active conversation about digital behaviors.

Consider:

Setting up **workstations** for children and teens that provide **quick visual access** to the screens for **easy check-ins** from parents/caretakers as they telework or complete household tasks.

Tip 3:

Engage with the Platforms



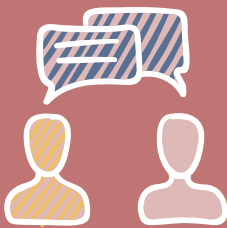
Take advantage of this time at home and online to get more familiar with the technology platforms your child likes to use. Taking a genuine interest in the games and platforms your child enjoys will help you better understand what your child is doing online.

Consider:

If you're teleworking, **take a short break** to join your child on a round on the **game console**, or forward a funny **meme or video** you saw on one of the social media channels they use. It's a quick way to show you're willing and able to be **involved** in your child's online life.

Tip 4:

Chat IRL



Chat "in real life" with your children. With our social lives being conducted entirely online these days, it's important to have face-to-face discussions about how children and teens are maintaining healthy relationships online, and to give them opportunities to also talk about anything unhealthy or uncomfortable happening to them online.

Consider:

Showing that you're willing to **listen and respond calmly**, even if what you hear is uncomfortable or troubling.

Tip 5:

Don't Take the Tech



Taking away internet access because a child has made a mistake online rarely solves the problem. Taking access away during a lockdown would likely do far more harm than good. Beyond affecting a child's ability to complete distance-learning tasks, it would all but completely isolate them from friends and other family; a support system that is essential right now. Find ways to give consequences that don't involve removing online access entirely.

Consider:

If you must, **limit access** (shorter window for digital socializing, gaming, restricted use to certain public areas of the house, etc.) **rather than** removing it entirely.

NetSmartz®

For more resources visit MissingKids.org/NetSmartz

Copyright © 2020 National Center for Missing & Exploited Children. All rights reserved.

A program of the



PARENTS' GUIDE TO SMART PHONE SAFETY

SMART OR SCARY?

Smartphones are essentially little computers, so you might be a little worried when handing one over to your child. Take some time to understand the risks and implement a few safeguards so that you can help your child use smartphones safely.



THE RISKS

▪ CYBERBULLYING

With the constant connectivity of smartphones, your child may be more susceptible to cyberbullying or have more opportunities to cyberbully others.

▪ GEOLOCATION

A GPS-enabled smartphone can reveal your child's location through online posts and uploaded photos.

▪ INAPPROPRIATE CONTENT

With smartphones, your child has mobile access to content you may consider inappropriate, such as pornography or violent videos.

▪ SEXTING

Your child may use the Internet and social apps to send, receive, or forward revealing photos.

▪ VIRUSES & MALWARE

Just like a computer, a smartphone is vulnerable to security attacks if your child accesses unsecured websites and apps.

5WAYS TO BE SMARTER THAN THE SMARTPHONE!

1. Be a parent and a resource.

Establish clear guidelines, including time limits and consequences for inappropriate behavior, but be open so your child will come to you with any problems.

2. Set up smart security.

Smartphones today include a variety of security mechanisms including fingerprint scans, facial recognition and password locks. Enable these to protect access to the phone as well as apps with sensitive data.

3. Update the operating system.

New versions often contain important security fixes.

4. Approve apps before they are downloaded.

Make sure you understand their capabilities and approve their content.

5. Understand location services.

GPS features are useful when using maps, but you'll want to disable location-tagging when your child posts anything online.

For more resources visit MissingKids.org/NetSmartz/Resources

Copyright © 2012-2019 National Center for Missing & Exploited Children. All rights reserved.

NetSmartz®



AI & Child Safety Online:

A Guide for Parents and Caregivers

Generative Artificial Intelligence (GAI) technology allows a user to create new images, videos, audio and text based on user requests or prompts. This technology has many benefits but also poses potential threats to child safety.

Understanding the Issues

Some of the possible challenges you or your child may encounter with GAI include the circulation of misinformation or its use to bully or harass others. But NCMEC is especially concerned about the growing use of GAI tools to sexually exploit children. Risks include:

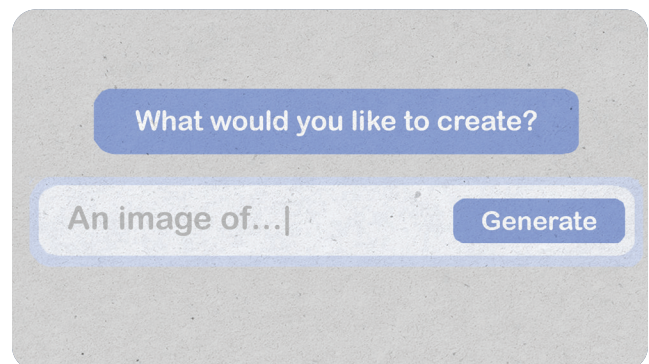
- ▶ **GAI Child Sexual Abuse Material (GAI CSAM):** Illegal, sexual exploitation material depicting children, created or altered using GAI.
- ▶ **Peer Victimization:** Creation and circulation of nude or sexually explicit GAI content among classmates, often created with “nudify” apps, that could be used to bully, harass, exploit or degrade classmates.
- ▶ **Online Enticement:** Creation of fake online accounts to target children with the intent to commit a sexual offense.
- ▶ **Sextortion:** Blackmailing children with GAI CSAM or nude images for money or to coerce them to provide additional explicit content or engage in sexual activity.

Conversations about GAI Safety

Protecting children from the misuse of GAI to exploit children requires education and guidance from trusted adults. Talking about these issues at home can help protect your children and make sure they are comfortable coming to you if something happens.

Getting Started:

-  Ask your child about their activities using GAI and ask them to show you how they use it.
-  Reaffirm to your child that whatever the problem is, you will always be there to help.
-  Share the resources on this page and encourage them to seek out a trusted adult if something happens.



Addressing Creating and Sharing Content:

-  **Discourage Creating and Sharing:** Explain that creating or resharing GAI nude images or CSAM is illegal, harmful and can profoundly impact the person depicted, whether the image is real or created using GAI.
-  **Empower Upstander Behavior:** Encourage taking action as upstanders by refusing to engage with or spread GAI-created images and talking to a trusted adult if they become aware of images being shared. Emphasize that they have the power to stop its spread and protect others.
-  **Foster Empathy:** Ask how they would feel if this happened to them or someone they care about. Reinforce the importance of respecting others' dignity, privacy and well-being.

Supporting a Child Who has Been Victimized:

-  **Support the Child:** Focus on the harm they're experiencing, not on investigating how the picture was created.
-  **Report to law enforcement and the CyberTipline:** Take action to access resources and help.
-  **Stay Calm:** Remain composed to reassure and support the child.

Other Tips

- ▶ Continue to educate yourself about how GAI is being used, new GAI technology that is being released to the public, and potential risks associated with it.
- ▶ Check your child's online privacy settings.
- ▶ Talk to your children's teachers and administrators about how this topic is addressed in school.
- ▶ Carefully read photo consent forms. Ask the organization how they are going to use the photos. Remember, it's okay to say no.

Resources

NCMEC can help with education, reporting and support for victims and their families if something does happen.



Reporting and Additional Support:
CyberTipline.org or
1-800-THE-LOST (1-800-843-5678)

Take It Down

Support to Help Remove Online Content:
TakeItDown.NCMEC.org



Other Support:
gethelp@ncmec.org



For More Information:
NCMEC.org/NetSmartz/GAI