



Children'sSM
Healthcare of Atlanta

Keeping Children Safe in a Digital World

Traci Hurley

Prevention and Training Program Coordinator

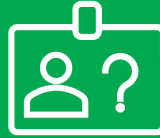
Stephanie V. Blank Center for Safe and Healthy Children at
Children's Healthcare of Atlanta



Technology is complex



Difficult to track



Anonymous



Multiple avenues



Unavoidable



Beneficial



How perpetrators use technology

Perpetrators access youth through:

- Social media and apps (48%)
- Chat rooms (81%)
- Gaming Systems

Perpetrators seek out youth when:

- The youth mentions sex in any way
- The youth appears “needy” or “submissive”
- A screen name mentions sex or sounds young

Perpetrators control by:

- Falsifying a romance or friendship
- Coercion, threats and/or “sextortion”
- False promises of modeling, acting, dancing opportunities
- Lowering inhibitions

“... [if] they’re always online, shows a low sense of parental contact or interest in child.”

“... when a child will do anything to keep talking to you.”





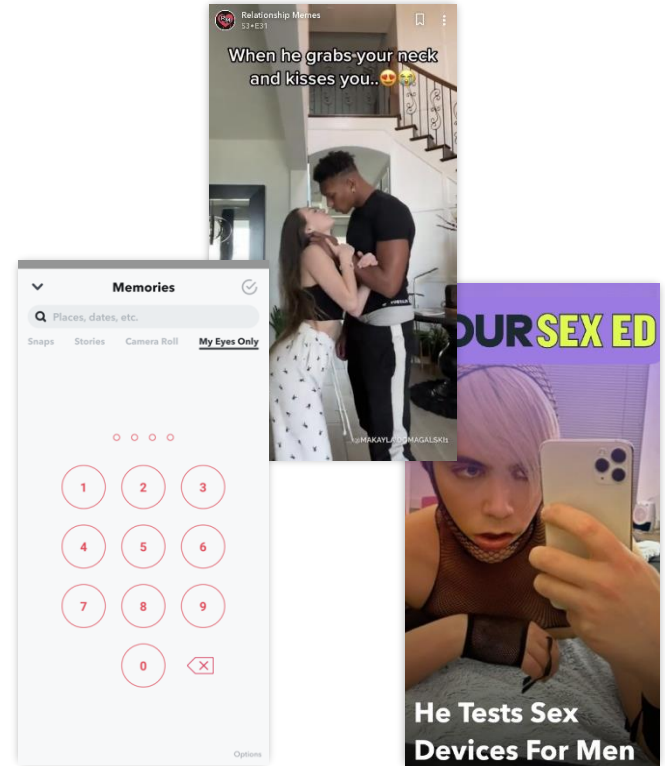
What Apps are Kids and Teens Using?





Snapchat

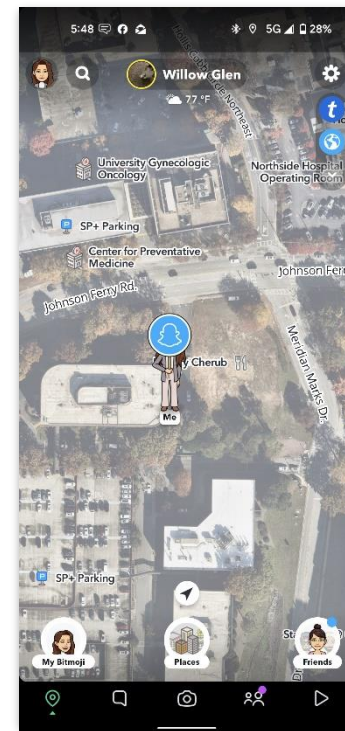
- **“Disappearing” images** make it appear safer to send or receive inappropriate content
 - 1 in 5 kids (13 to 17) said it’s OK to share a nude if it’s on an app that doesn’t save it
- **“My Eyes Only”** acts as a password-protected photo vault
- **Discover page**
 - Features media, current events, public figures/celebs
 - Content skews toward sex, abusive relationships and risky behavior





Snapchat, cont.

- **Location sharing (Snap Map)**
 - Allows users to see where friends and followers are while using the app
 - Option to be hidden on “Ghost mode”
- **“Story”** (My Story, Our Story, Location Stories)
 - Allows users to contribute to a public feed showing real-time events
 - Allows users to communicate directly within the map when near one another
 - Users don't have to know each other to communicate





Snapchat: Family Center

“...which will help parents get more insight into who their teens are friends with on Snapchat, and who they have been communicating with, without revealing any of the substance of those conversations.

Parents can also easily and confidentially report any accounts that may be concerning directly to our Trust and Safety teams, which work around the clock to help keep Snapchatters safe.

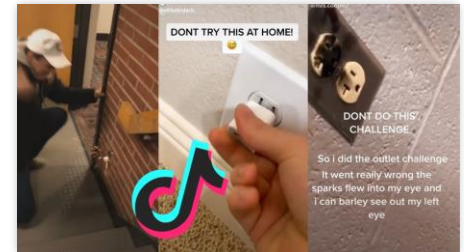
We’re also equipping parents and teens with new resources to help them have constructive and open conversations about online safety.”



Most downloaded app worldwide (since April 2021)

Considerations with TikTok:

- Inappropriate content is very easy to find (explicit/sexual lyrics, dangerous situations, pornography, etc.)
- Some TikTok challenges are harmless and some present dangerous situations
- Commercial element encourages purchases
- **Powerful algorithm:**
“Its algorithm stands out among other social media, such as YouTube and Instagram, for quickly assessing interests of users and providing a highly personalized stream of videos.”



Source: Wall Street Journal: [How TikTok Serves Up Sex and Drug Videos to Minors](#) and [‘The Corpse Bride Diet’: How TikTok Inundates Teens With Eating-Disorder Videos](#)

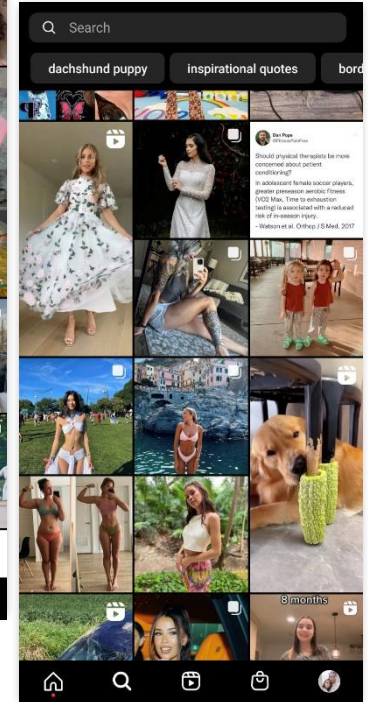
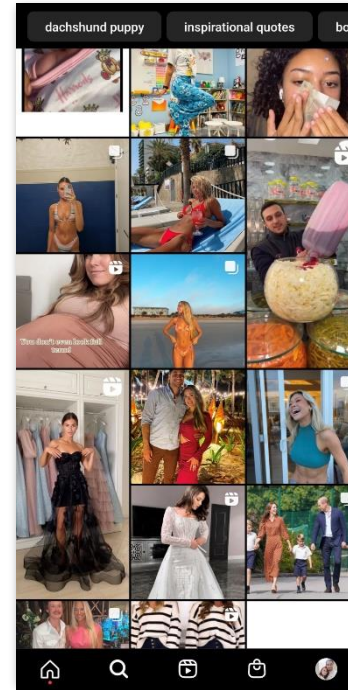
- **Entirely user-generated**
 - Relies on community to flag videos that violate YouTube's terms of service (mostly for sexual content, language and hate speech)
- **Dangerous behaviors** for attention or video views
 - YouTube “celebrities” and influencers
- **Parental Controls** (3 tiers of supervision)
 - *Explore* for those 9+
 - *Explore More* for those 13+
 - *Most of YouTube*, a mode with access to everything except content marked 18+
 - Kids with supervised accounts won't get personalized ads and can't comment or create



“Finsta” accounts are secret second accounts, intended to avoid parent oversight.

Considerations with Instagram:

- Potential Security Risks:
 - Direct messages (DM)
 - Using hashtags
 - Including personal information
 - Location sharing and geo-tagging
- Mental Health Concerns:
 - Pressure to curate a “perfect” life
 - Mature/harmful content on *Explore* page
 - Comment section can breed cyberbullying



Messaging apps

Used instead of texting

- Accessed via app or web browser
- Uses data or wi-fi



Common messaging apps:

- WhatsApp
 - Most popular messaging app with 1 billion users
- Facebook Messenger
 - “Free texting from Facebook”
 - Get messages instantly
- GroupMe





Real-time communication apps are difficult to monitor and control.

Doesn't offer parental controls:

- No way for parents to restrict content (user-generated)
- Can't password-protect privacy settings w/in app

Technology and security evolution:

- No Trust and Safety Team prior to 2017
- Team created after Charlottesville protests and now makes up >15% of their staff

The National Center on Sexual Exploitation named Discord to 2022 Dirty Dozen list as major contributor to sexual exploitation of children.



Hiding photos and content

- **Secret photo apps**

- KeepSafe
- Vault



- **“Calculator” apps:**

- Secret Photo
- Smart Hide Calculator

- **Other apps:**

- Secret Photo
- Smart Hide Calculator



Apps and video games to be aware of

*Not an exhaustive list. Always monitor and research before allowing access.



TikTok



SnapChat



Twitter



YouTube



Instagram



Facebook



Facebook
Messenger



GroupMe



WhatsApp



Calendar
Vault



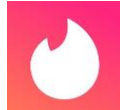
Discord



Telegram



Yubo



Tinder



Parlor



Tumblr



Among Us



Spotafriend
Meet Teens



KeepSafe



Vault



Fortnite



Minecraft



Roblox



Omegle



Chatroulette



Grinder



NGL



Tellonym



Grand
Theft Auto



Cyberpunk





Self-Generated Child Sexual Abuse Material: Attitudes and Experiences

Complete findings from 2019 qualitative and quantitative research among 9- to 17-year-olds and caregivers.

Research conducted by Thorn in partnership with Benenson Strategy Group



Sharing nudes is “increasingly common”

- “When exploring attitudes related to this behavior, 27% of kids aged 9 to 17, and nearly 40% of kids aged 13 to 17, agreed that “it’s normal for people my age to share nudes with each other.”
- Self-reported data is typically low, but kids are clearly talking about it as a form of sexual exploration and romantic flirtation.
- Not likely to change soon.

1 in 5

girls (13 to 17) have shared their own nudes

1 in 10

boys (13 to 17) have shared their own nudes

40%

agree sharing nudes is “normal” for people their age



What are the consequences of sharing nudes?

Child Pornography (CSAM)

It's illegal to disclose intimate videos or pictures if <18yo

36%

of kids (9 to 17) say peers send or share nude photos or videos of other kids

Humiliation
upon private images being shared

**Suspension/
expulsion from school**

Revenge Porn
Sending or posting explicit images or videos of someone without their consent

Sextortion
Threatening to expose info or images to make someone do something

36%

of kids (9 to 17) say peers have had their nudes shared or leaked w/o permission



Sexting (self-generated child sexual abuse material)

Is this something I would do face to face?

Would I be OK if this was posted in my school's hallway?

Questions for youth to ask themselves before sending a photo.

Would I send this to my grandmother?

Would I want someone to ask me for the same thing?





What gaming platforms are kids and teens using?



Fortnite, Minecraft and Roblox

Users range in all ages, including adults:

- Content is user-generated
- Youth can be exposed to a range of inappropriate material

Age restrictions:

- Fortnite: 13+ (no verification)
- Minecraft: 13+ w/standard account, <13 must be verified w/ credit or debit card
- Roblox: No age restrictions

Parental controls:

- [Fortnite](#)
- [Minecraft](#)
- [Roblox](#)



“‘Hunting grounds’ for sexual predators”

“Video games and online chats are ‘hunting grounds’ for sexual predators” – New York Times (2019)

- “In May, a California man was sentenced to 14 years in prison for coercing an 11yo girl “into producing child pornography” after meeting her through the online game Clash of Clans.
- A man in suburban Seattle got a 15-year sentence in 2015 for soliciting explicit imagery from three boys after posing as a teenager while playing Minecraft and League of Legends.
- An Illinois man received a 15-year sentence in 2017 after threatening to rape two boys in Massachusetts — adding that he would kill one of them — whom he had met over Xbox Live.”



Gaming and Digital Safety

Gaming Consoles

- Xbox
- PlayStation
- Nintendo Switch
- Gaming PCs & Desktops

Considerations and Guidelines:

- Any internet connected device needs parental controls **BEFORE** it is given to youth.
- Research and approve all games/applications that are downloaded on gaming consoles.
- Online gaming options should be disabled, especially for younger children.
 - Encourages one-on-one interactions with strangers.



Gaming and Digital Safety

Gaming Headsets and Headphones:

- Xbox Wireless Headset
- PlayStation PULSE 3D Wireless Headset
- JLab Jbuddies Wired/Wireless Headphones

Considerations and Guidelines:

- Frequently disconnect headsets: Check in about who they are talking with and what they are listening to.
- Family Agreement: Headsets are only allowed in common areas of the home, and you will be checking in.
- Cyberbullying: Having headsets on/gaming in private can restrict interactions that could be heard, missing signs of cyberbullying/inappropriate conversations.



VR Headsets (Oculus, Sony PlayStation VR, Samsung)

One of the newest forms of technology:

- Limited research about long-term effects
- Young children may fail to discern between reality and fantasy
- May contain sexual scenarios, child abuse, harassment, racism, pornography and other mature content

VRChat Investigation:

“Posing as a 13-year-old girl, BBC researcher Jess Sherwood said she entered a virtual strip club where she saw adult men chase a child while telling them to remove their clothes ... condoms and sex toys on display ... a group of adult men and minors simulating group sex ... instances of grooming.”





What can we do to prevent online exploitation?



What can youth-serving professionals do?

- Maintain security on all public devices.
- Educate caregivers and youth about safe internet usage.
- Stay familiar with emerging trends in tech.
- Determine extent of problem in your school/organization.
- Gather a group of stakeholders to combat the issue.
- Implement new/enforce existing policies to monitor internet usage and/or address online safety and cyberbullying.



What can youth-serving professionals do?

- Talk regularly about online safety.
 - Do you have friends online or friends you don't know in real life?
 - What kind of apps do you use?
 - How long do your parents let you play online?
- Promote an open environment that encourages children to come forward.
- Advocate for training that equips staff.
- Implement layers of protection.
 - Virtual private networks (VPNs) are often used to bypass firewalls and security filters in place to protect youth.



What can parents and other caregivers do?



**Set logical
consequences for
infractions**



**Be prepared to see
and hear things
you won't like**



**Be prepared to
have difficult
conversations**



What can parents and other caregivers do?

- Ask youth the same questions about their online behavior that you'd ask about their real-life behavior.
 - Who are they talking to?
 - Where are they going?
 - How long will they be there?



Setting limits and consequences

- **Set boundaries early on** to keep youth from being manipulated or exploited online.
- **Consistently set consequences** for infractions.
- **Create family online safety agreements** for phones, video games and screen time.
- **Install parental controls and monitoring** on all internet connected devices.
 - Set strict privacy settings.
 - Turn off geo-location services.
 - Create joint accounts.
 - Approve all new followers/friends.
 - Get all login info for phone and social media sites.

“Being online is an earned privilege, not a right.”





“I would feel more comfortable talking to my parent or guardian at home about these issues, if I knew that, they wouldn’t scream or yell at me for something I am just learning and new to.”

– Cis girl, 13 to 17, White, Midwest (2019 Thorn Study).



Device Safety



Technology considerations

Smart Devices

- Echo Show
- Smart Watches
- Apple Air Tags
- Fire HD Tablets, Fire TV Stick/Gaming Bundle
- Computers, Laptops, Tablets, Phones etc.
- Wireless Earphones (Air Pods, Google Buds, etc.)

Considerations and Guidelines:

- **BEFORE giving internet connected devices to youth:**
 - Have parental controls and monitoring applications set up in advance.
 - Make family agreements, contracts, and safety plans.
 - Discuss good digital citizenship and digital footprints.
 - Awareness to surroundings when earphones are in.
 - Take security measures through your internet provider.
 - Make sure location sharing is turned off.
 - Manually turn on location sharing for specific monitoring apps



Technology considerations

Gift Cards

- Amazon Gift Cards
- Xbox Gaming Pass
- PlayStation Store Gift Card
- Roblox Digital Gift Card



Considerations and Guidelines:

- **BEFORE** activating or providing gift cards:
 - Have a conversation about purchasing responsibilities:
 - Purchases should not be made until they are approved by caregiver.
 - Set consequences if inappropriate purchases are made or something is purchased without permission.
 - Monitor what gift cards are being used for.
 - Games or points/tokens, audio books, clothing, etc.



Technology considerations

When should youth be allowed to use technology?

- All children develop at their own rate. You know your child best.
- Most tech professionals recommend waiting until 8th grade for a phone and 16 for social media.

What else should you consider when making decisions about technology?

- What is the purpose?
- How old is the youth?
 - Do they respect and obey rules?
 - Are they mature enough?
 - Are they responsible with their belongings?
 - Do they know how to use the tech responsibly, safely, appropriately and moderately?
- Are *you* ready to responsibly monitor the technology in your home?



Monitoring and establishing security

Monitoring apps

- Bark app
- OurPact
- Fortify
- Net Nanny
- Web Watcher
- TeenSafe
- AVG Family Safety



Alexa for Kids and Families

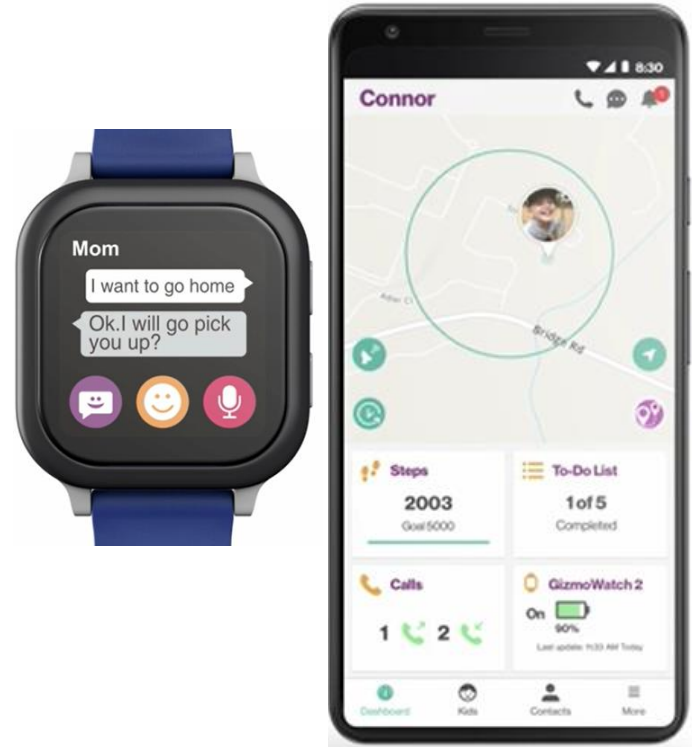
When you create a [profile](#) for your child, Alexa can recognize their voice and automatically give kid-friendly responses on compatible Echo devices throughout the home. Alexa will filter songs with explicit lyrics, block shopping, let kids access parent-approved-content, and give age-appropriate responses. Access the [Amazon Parent Dashboard](#) where easy-to-use parental controls let you review kids' activity and set time limits at no extra charge.



Phones & Watches for Kids

GizmoWatch, Gabb, Troomi, etc:

- Kid-friendly devices designed to cultivate independence while maintaining safety.
- GizmoWatch Features:
 - GPS locator
 - Easy-to-use parental controls
 - Reminders & to-do lists with rewards
 - Step tracker to encourage healthy habits
 - Set up to 10 trusted contacts that kids can send voice notes to, call, or text.



Discuss Good Digital Citizenship

- **Stay safe online**
- **Respect** themselves and others
- **Stand up** to cyberbullying when they see it happening
- **Protect** private information for themselves and others
- **Balance** the time spent using media and doing other activities



Creating a safety plan

A safety plan is a **personalized, practical plan** to help you avoid dangerous situations and know the best way to react when you're in potential danger.

1

Create
ahead of
time

2

Be
realistic

3

Be
specific




4

I.D.
specific
people
to go to
for help



Who is a "Trusted Adult"?

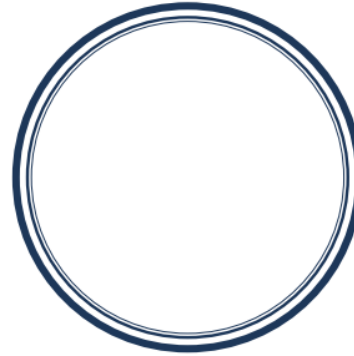
Trusted adults are people whose words and actions make you feel safe. Trusted adults act this way both online and offline.

Actions	Words
Trusted adults...	Trusted adults say things like...
Listen to you when you have a problem or question	I'll answer your questions.
	You can tell me if you have a problem.
	I care about what you think.
Respect your body and your personal space	
	

A trusted adult can be any grownup whose actions and words make you feel safe; a teacher, a mentor, a parent, a coach—anyone who loves you and respects you. It is always OK to ask for help from a trusted adult and to **keep asking** the same person or another trusted adult if they don't understand or if you don't **get the help that you need**.

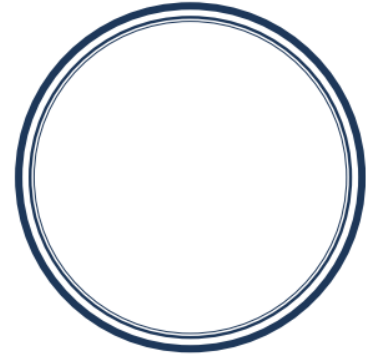
Some of My Trusted Adults

Draw a picture of your trusted adult in the circles. Below the picture, add their name and why you trust this person.



Name: _____

I trust this person because



Name: _____

I trust this person because



Key takeaways

Digital safety is just as important as **physical safety**.

It takes a **village** to prevent child maltreatment

Put safety measures in place early!
Prevention starts **before** an event takes place, not after.

Speak up! Talk within your community. Be willing to have **difficult conversations**.

Educate yourself and others. Empower those around you.

Youth spend significantly more time online. Make sure it's a **safe and fun** experience.



Cyberbullying resources

For youth

- [Kidshelpline](#): Call, webchat or email with a qualified counselor
- [Hopeline](#): Call 800-442-HOPE (4673) to speak to trained crisis interventionists
- [IMAlive](#): An online crisis network where youth in emotional distress can talk with someone in a safe space

For parents and caregivers

- [Connect Safely](#): The Parent's Guide to Cyberbullying
- [Child Mind Institute](#): How to Help Kids Deal With Cyberbullying



Resources to help implement online safety

- [Common Sense Media](#): An independent voice for kids, families, and communities everywhere, combining original research with game-changing advocacy efforts to make the digital world work better for all kids
- [Internet Matters](#): Parents and professionals can find the most comprehensive and credible resources, information and support to keep children safe online. gives step-by-step guides to set parental controls on a variety of devices and applications.
- [NetSmartz](#): NCMEC's online safety education program providing age-appropriate videos and activities to help teach children be safer online
- [Love 146 Online Safety Guide](#): A nonprofit organization that's developed child trafficking and exploitation prevention curriculum and created information for youth that covers online safety + a guide on how to maneuver online conversations.
- [Internet Safety 101](#)
- [Stop Bullying](#)
- [Center For Safe and Responsible Internet Use](#)
- [PACER Center-National Center for Bullying Prevention](#)



NetSmartz: Training Resources



K-12 Google Slides by Topic

[View Slides](#)



Internet Safety:
Parents, Guardians &
Community Members

[English](#)

[Español](#)



Advanced Online
Safety: High School (9-
12)

[English](#)

[Español](#)



Online Safety: Middle
School (6-8)

[English \(PC/Mac\)](#)

[Español \(PC/Mac\)](#)



Be Safer Online with
NetSmartz: Grades K-2



Being a Good Digital Citizen:
Grades 3-5



Teaching Modern Safety with
"Into the Cloud"



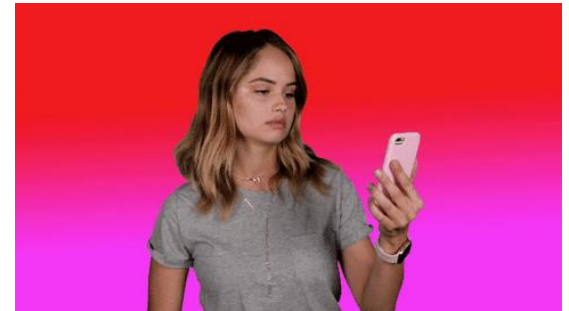
Online Safety Guide

- Gives youth relatable tips and tricks on how to be safe while interacting online.
- Reviews: 5 Internet Safety Rules, 8 Red Flag Phrases, Sexting, and What to do if someone's making you uncomfortable.



Not a Number

- An interactive prevention curriculum designed to teach youth how to protect themselves from exploitation through information, critical thinking, and skill development.



References/citations

- [Centers for Disease Control and Prevention \(CDC\)](#)
- [Wall Street Journal: 'The Corpse Bride Diet': How TikTok Inundates Teens With Eating-Disorder Videos](#)
- [Wall Street Journal: How TikTok Serves Up Sex and Drug Videos to Minors](#)
- [Common Sense Media](#)
- [Self-Generated Child Sexual Abuse Material: Attitudes and Experiences \(2019 Thorn Study\)](#)
- [Rules for Video Games and Screen Time: Video Games and Online Chats Are 'Hunting Grounds' for Sexual Predators](#)
- [VR Safety Tips for Parents](#)
- [Investigation of VRChat](#)
- [Is My Child Ready for A Smartphone?](#)
- [Verizon GizmoWatch2](#)
- [Gabb Wireless](#)
- [Troomi](#)
- [Alexa for Kids and Family](#)





What questions do you have?

CPCTraining@choa.org

traci.hurley@choa.org

404-785-1122

Additional webinar and training opportunities: choa.org/cptraining

