

A PARENT'S GUIDE TO DIGITAL SAFETY

Navigating Uncharted Waters

Practical tools for building trust, open conversation,
and lasting safety skills with your child





Introduction

Connection Before Control: A Skills-Based Approach to Online Safety

The internet is a part of everyday life for young people. It offers opportunities to learn, connect, create, and explore. Like any environment, it also comes with risks.

This toolkit is designed to help parents and caregivers support their children's online safety using a prevention approach that emphasizes relationship-building, trust, communication, and skill development. Rather than relying on fear or trying to eliminate all risk, this approach focuses on helping young people gradually build the knowledge, judgment, and confidence they need to navigate digital spaces safely.

WHAT THIS TOOLKIT IS

A starting point.

This resource gives parents and caregivers foundational knowledge, practical strategies, and conversation tools to support their child's online safety. Additional resources are included at the end for families who want to go deeper on any topic covered here.

WHAT THIS TOOLKIT ISN'T

A rulebook.

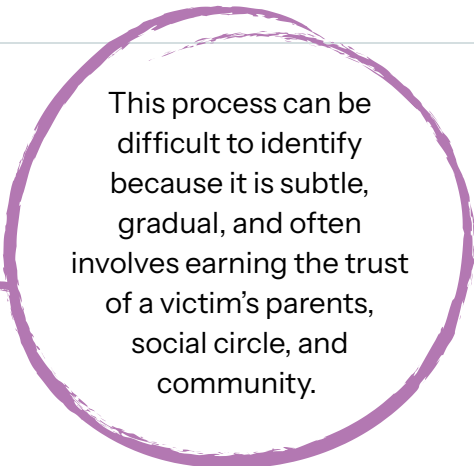
This toolkit does not tell you when or whether your child should have access to a personal device — that decision belongs to your family. Every household has different values, rules, comfort levels, and needs, and those differences are valid. What works for one family may not work for another.



Understanding the Issue

Key Definitions

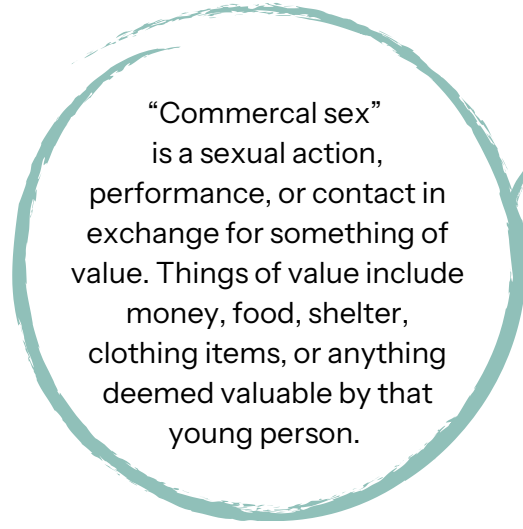
Grooming: A process in which a person builds trust or a relationship with a child or teen in order to manipulate, exploit, or abuse them. Grooming can occur online, in person, or both.



This process can be difficult to identify because it is subtle, gradual, and often involves earning the trust of a victim's parents, social circle, and community.

Online Exploitation: When someone uses technology or online platforms to manipulate, pressure, deceive, or harm another person for personal gain.

Sextortion: A form of exploitation in which someone threatens to share real or fabricated intimate images, videos, or personal information unless the victim provides money, additional images, sexual content, or other demands.



"Commercial sex" is a sexual action, performance, or contact in exchange for something of value. Things of value include money, food, shelter, clothing items, or anything deemed valuable by that young person.

Human Trafficking: The exploitation of a person through force, fraud, or coercion for labor or commercial sex. When a person under 18 engages in a commercial sex act, it is considered sex trafficking under U.S. law regardless of whether force, fraud, or coercion is present.

What We Know



1 in 3 youth report that some of their closest friendships were formed online.

Online spaces can provide meaningful opportunities for connection, support, and belonging, especially for young people seeking community around shared interests and experiences.

Thorn, 2022



About 2 in 3 youth report that someone they met online asked them to move a conversation from a public platform to a more private space.

While many of these interactions are harmless, moving conversations into private channels can reduce visibility and make it harder for others to recognize concerning behavior.

Thorn, 2022



Nearly half of U.S. teens report being online “almost constantly.”

Digital spaces are woven into young people's social lives, education, entertainment, and daily routines, making digital safety skills increasingly important.

Pew Research Center, 2024

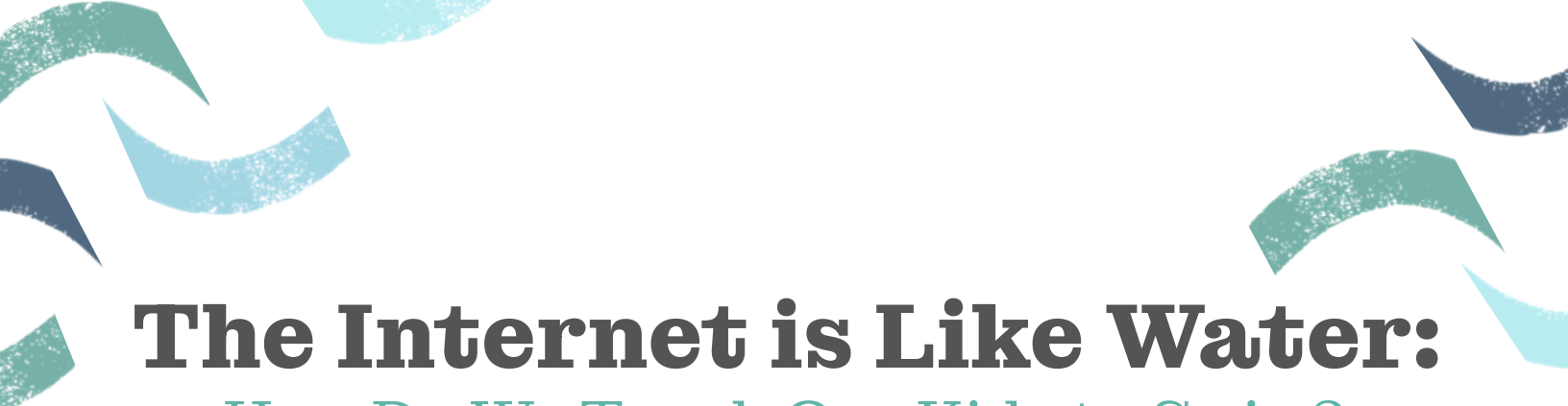


Research consistently shows that supportive relationships with trusted adults are among the strongest protective factors for youth well-being and safety.

Young people are more likely to seek help when they know adults will listen, remain calm, and respond without judgment, particularly when navigating online challenges.

CDC, 2024; Mathews et al., 2025





The Internet is Like Water:

How Do We Teach Our Kids to Swim?

Most parents would not keep a child completely away from water until age 13 and then expect them to know how to swim safely. Instead, we gradually teach skills, supervise practice, and increase independence as children demonstrate readiness.

The internet works the same way. Some online spaces are like your local community pool and others are more like the open ocean at high tide.

Adults who stay close, build skills gradually, and give kids room to practice raise children who know what to do when the current gets strong.

1

Start in the Shallow End

There is no age limit on the shallow end! Whenever you choose to introduce the internet or digital spaces, this is a good place to start.

- **Get in the pool with them**

- Explore apps, games, and websites together

- **Teach basic safety rules**

- Do not share personal information
- Tell a trusted adult when something feels confusing or upsetting

- **Draw connections between online and physical spaces**

- Some places are safe for kids, others are more appropriate for older youth, and others are for adults only
- Family norms and values related to kind language, inclusivity, and respectful behavior still apply when you are online

- **Build communication skills and trust**

- Let children know they can always come to you with questions.
- Praise them for asking for help or reporting a problem.



TRY THIS

"I know you're going to come across stuff online that's uncomfortable or hard to figure out. I'd rather you come to me than try to handle it alone. No judgment."

- Respond calmly when mistakes happen so they continue to seek support.

TRY THIS

"I'm really glad you told me about that. That took courage, and it was exactly the right thing to do. Let's figure out next steps together."

2

Practice with a Lifeguard on Duty

- Continue checking in regularly about online experiences

- Help children recognize:

- Advertising and persuasive content
- Scams and misinformation
- Unsafe requests from others
- AI-generated and manipulated content

- Encourage critical thinking

- “How do you know this information is true?”
- “What would you do if someone asked for personal information?”

For more information and guidance on AI-generated content including ‘deepfakes’ check out [the guide by Amaze.org](#) in the Resource section



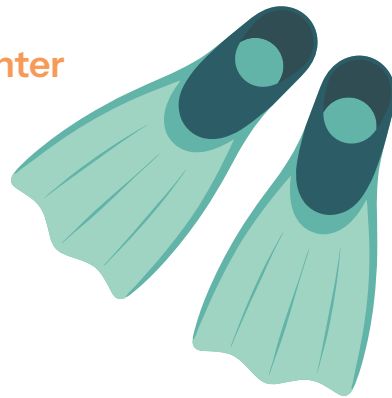
Think of parental controls as **life vests**:

Not a permanent solution or substitute for learning water safety. They can reduce risk while children are learning, but lasting safety comes from skill-building, communication, and gradually increasing independence.

3

Build Strong Swimmers

- **Gradually increase independence and responsibility**
 - Explore apps, games, and websites together
- **Discuss real-world situations they may encounter**
 - Peer pressure
 - Sharing images
 - Online relationships
 - Digital footprints
 - Financial scams
- **Focus on decision-making skills rather than rules alone**
- **Keep communication open so teens are more likely to seek help when challenges arise**



Remember:
Even strong
swimmers
need support

No swimmer is safe in every situation, and no young person will make perfect choices online.

Aim to create an environment where your child knows:

- They can come to you without fear of immediate punishment.
- Mistakes are opportunities for learning.
- Asking for help is a sign of strength.

What Parents Can Do Today

1

Build connection before problems arise

- Have regular conversations about online life (check out [5 Family Conversation Starters](#), available under Resources).
- Show curiosity rather than judgment.
- Ask what apps, games, creators, and platforms your child enjoys.
- Review and sign a [Family Technology Agreement](#) (available under Resources).
- Discuss screen use, privacy, and respectful online behavior.
- Explain why family rules exist, and involve kids in setting them when possible to increase buy-in and accountability.
- Revisit expectations as children grow and technology changes.

2

Help children learn how to:

- Protect personal information.
- Evaluate online content.
- Set boundaries with others.
- Recognize manipulation or pressure.
- Seek help when something feels wrong.

3

Make a plan before you need one

- Talk through real scenarios so your child can practice asking for help and you can practice responding.
- Print and review our one-page [Quick Response Guides](#) (available under Resources) for specific guidance on how to handle disclosures.



Conclusion

Prevention is Possible

You've got the foundation: why a prevention approach works, how to talk with your child about online safety, and what skills to build along the way. None of this requires perfection. It requires presence: staying close, responding calmly, and giving your child room to practice with your support nearby.

No one learns to swim by avoiding the water, and no child learns to navigate the internet by avoiding it either. With your guidance, they'll learn to read the current, ask for help when they need it, and build the confidence to keep swimming on their own.

And you're not in this alone. At Everstrong, we have resources, tools, and handouts to support all adults, including parents, teachers, and caregivers, in having these conversations with youth.



Find out more at Everstrong

Visit www.everstrong.org for resources, handouts, and guides to support your conversations with kids. Check out the sources, links, and resources at the end of this toolkit to dive even deeper.

More information



Sources

- Thorn. (2022). Youth Perspectives on Online Grooming. www.thorn.org/research/grooming-and-sex-tortion/
- Pew Research Center. (2024). Teens, Social Media and Technology.
- Centers for Disease Control and Prevention (CDC). Risk and Protective Factors Framework.
- Substance Abuse and Mental Health Services Administration (SAMHSA). Protective Factors and Prevention Framework.
- CDC. (2024). Risk and protective factors: Adverse childhood experiences (ACEs). Centers for Disease Control and Prevention. www.cdc.gov/aces/risk-factors/index.html
- Mathews, A., et al. (2025). Desperately seeking non-judgmental supports: Young people's perceptions of adult responses to technology-facilitated harms. PubMed. pubmed.ncbi.nlm.nih.gov/41582859/

Learn More

- Common Sense Media www.commonsensemedia.org
- National Center for Missing & Exploited Children (NetSmartz) www.missingkids.org/netsmartz
- Futures Without Violence (Linkup Lab) www.linkuplab.org
- Amaze (tagged Amaze-on-Tech) www.amaze.org

Check out Amaze.org for helpful, age appropriate, illustrated videos on all kinds of topics impacting youth. Search the tag “Amaze-on-Tech” for all things internet safety



Resources

Following are additional resources to support your conversations with children and teens. These are also available as stand-alone downloads from our website.



Family Technology Agreement



Five Family Conversation Starters



Quick Response Guide for Disclosures



Deepfake Guide

Family Technology Agreement

for families with children (6-12)



Respect & Kindness

Child: I agree to treat others kindly online and never post or share hurtful words, pictures, or messages.

Parent: I agree to model kindness online, listen calmly to my child, and help them handle unkind or unsafe behavior in healthy ways.



Privacy & Protection

Child: I agree to keep my personal information private and tell my parent if someone I don't know messages me, even in a game.

Parent: I agree to help my child learn what personal information is, check privacy settings together, and explain how online games and chats can be used to trick or exploit kids.



Screen Time & Balance

Child: I agree to follow our family rules for screen time and take breaks to play, rest, and spend time offline.

Parent: I agree to help set fair limits for screen time and show balance by putting my own device away during family moments.



Truth & Trust

Child: I agree to tell my parent right away if I see or experience something online that makes me uncomfortable or confused.

Parent: I agree to stay calm and supportive when my child tells me about a mistake or unsafe situation online.



Responsibility & Digital Footprint

Child: I agree to think before I post or send something, because once it's online, it can be hard to take back.

Parent: I agree to teach my child that their online choices create a digital footprint and that learning from mistakes is part of growing up online.



Additional Agreements for Our Family:

Child: _____

Parent: _____

Family Signatures and Accountability

By signing this agreement, we promise to use technology in ways that are safe, respectful, and balanced. If one of us struggles to follow these agreements, we'll talk about it without blame or shame, listen to each other, and make a plan together to repair trust and strengthen our habits moving forward.

Child(ren): _____

Parent(s)/Adult(s): _____

Family Technology Agreement

for families with teens (13-18)



Respect & Kindness

Teen: I agree to communicate respectfully online and avoid gossip, shaming, or sharing private information about others.

Parent: I agree to talk with my teen about online conflict and model respect and empathy in my own digital use.



Privacy & Protection

Teen: I agree to protect my personal information and be careful with messages or game invites from people I don't know, especially when they offer gifts, game rewards, or in-app purchases.

Parent: I agree to talk openly with my teen about online grooming and exploitation risks in games, apps, and private chats, and to review privacy and safety settings together.



Screen Time & Balance

Teen: I agree to notice how social media and gaming affect my mood and sleep and take breaks when I need them.

Parent: I agree to set realistic screen time goals with my teen, model balanced technology use myself, and support healthy routines for connection, school, and rest.



Truth & Trust

Teen: I agree to be honest about the apps and platforms I use and to ask for help when I feel unsafe or pressured online.

Parent: I agree to be honest about our family's tech expectations, respect my teen's growing independence, and keep communication open and judgment-free.



Responsibility & Digital Footprint

Teen: I agree to think about how my posts and messages reflect who I am and to take responsibility if I make a digital mistake.

Parent: I agree to guide my teen in building a positive digital reputation and encourage technology use that helps them learn, create, and contribute positively.



Additional Agreements for Our Family:

Teen: _____

Parent: _____

Family Signatures and Accountability

By signing this agreement, we promise to use technology in ways that are safe, respectful, and balanced. If one of us struggles to follow these agreements, we'll talk about it without blame or shame, listen to each other, and make a plan together to repair trust and strengthen our habits moving forward.

Teen(s): _____

Parent(s)/Adult(s): _____

Let's Talk:

5 Family Conversation Starters to Promote Online and Offline Safety

Why These Conversations Matter

Kids and teens face new situations every day, both online and in person. Regular, open conversations help them build confidence, make safe choices, and know they can always come to you for help.

Tip: The best time for these talks is when things feel calm, like during car rides, meals, or walks. Keep it casual and listen more than you lecture.



1. Who are the safe adults you can talk to if something feels uncomfortable or confusing?

Help your child name trusted adults before a problem happens and discuss what makes an adult trustworthy (some ideas: someone who cares about them, respects boundaries, and doesn't ask them to keep secrets).

Try this: Make a short list together and keep it somewhere visible.

2. What values are most important to you—and how do those values guide your choices online and in person?

Talk about what your family stands for (some ideas: kindness, honesty, respect, helping others, courage).

Try this: Ask how it feels when actions match or don't match those values. Share your own examples of moments when you had to make a tough but values-based choice.

3. What should you do if someone online asks you for pictures or personal information?

Help your child recognize unsafe requests and know they can always come to you for help.

Try this: Remind them that it's never their fault if something uncomfortable happens online, and you'll always listen and help them stay safe.

4. How do you know when a situation feels safe or unsafe?

Teach your child to notice body signals—like a tight stomach, fast heartbeat, or wanting to leave.

Try this: Talk about how those feelings are our body's way of keeping us safe and what to do if that happens.

5. What can we do as a family to help everyone feel safe and respected?

Create family habits that promote safety and respect (some ideas: device-free dinners, checking in before changing plans, reviewing privacy settings together, regular family check-ins, weekly game or family fun night).

Try this: Talk together about what helps each person feel safe and respected. Work as a team to create family agreements that make sense for everyone—rules that protect, not punish, and that everyone helps shape



Keep the Conversation Going

Safety grows from connection. Small, honest talks over time build trust and make it easier for kids to ask for help when something doesn't feel right.

Helpful Family Resources:

- *NetSmartz* – National Center for Missing & Exploited Children: missingkids.org/NetSmartz
- *Common Sense Media* – Family Tech Agreements: commonsensemedia.org/family-tools
- *Second Step*® – Safety & Social-Emotional Learning: secondstep.org



Navigating Disclosures: Quick Response Guides

General Concerns

Whether your child made a mistake, witnessed something upsetting, or was targeted by someone else, a supportive response keeps the door open for next time.

Step	What to do
1. Take a deep breath	Your child reads your face before you say a word. Staying calm — even if you feel shocked or upset — keeps the door open for them to keep talking. Say: “I’m really glad you told me. We’re going to figure this out together.”
2. Listen before you ask	Let them tell the story their way first. Avoid interrupting or jumping to conclusions. Say: “Tell me what happened — I’m listening, no rush.”
3. Support, not blame	Focus on support over blame. This is what makes kids feel safe coming to you no matter what’s happened. Say: “This isn’t your fault. I’m here to help you through it.”
4. Decide on next steps together	Work together to decide what action to take — whether that’s saving evidence, blocking someone, reporting content, adjusting privacy settings, or simply deciding nothing further is needed right now. Involve your child in the decision so they feel like a partner, not a bystander. Say: “Let’s figure out together what we should do next — I want your input on this.”
5. Follow up	One conversation isn’t enough. Check in over the next several days and reassure them again that telling you was the right call. Say: “I’ve been thinking about you — how are you doing with everything?”

Sextortion

Sextortion is blackmail using a real or fake image to extort money or more photos — it requires immediate reporting to protect your child from further harm.

Step	What to do
1. Don't pay. Don't comply.	Cooperating or paying rarely stops the blackmail — it often escalates demands. Get help before deciding anything. Say: “We are not paying them. This is a crime, and there’s a way through it.”
2. Block — don't delete	Block the suspect, but do not delete the profile or messages. They’re evidence that can help stop the blackmailer. Say: “We’ll block them now, but we’re keeping everything as evidence first.”
3. Screenshot everything	Capture messages, usernames, the profile, and any payment demands, with timestamps, before blocking. Say: “Let’s save all of this so we have proof of what happened.”
4. Report immediately	Report the account through the platform’s safety feature . File a report with NCMEC’s CyberTipline (cybertipline.org or 1-800-THE-LOST). If images exist, use Take It Down (takeitdown.ncmec.org). Say: “We’re reporting this right now — there are people whose job is to help with exactly this.”
5. Watch for crisis signs	Sextortion can have major, long-term impacts on someone’s mental health. If your child shows signs of panic, hopelessness, or despair, treat it as urgent. Say: “If things feel like too much, we can call 988 right now, together.”
6. Remind them it's not their fault	The blackmailer is to blame — not the child. Even if they made a choice they regret, what’s being done to them is a crime. Say: “You didn’t do anything wrong. They did.”

Sources: NSPCC, UNICEF Parenting, National Center for Missing & Exploited Children (missingkids.org/sextortion)

Deepfakes/ AI Nudes

1. Overview
2. Deepfake Content Examples
3. Mentoring Tipsheet
4. Video Discussion Guide

What is a “deepfake” or AI nude?

Deepfakes, or AI nudes, are digitally altered or generated images or videos created using artificial intelligence (AI) to make it appear that a real person is naked or engaged in sexual activity when they are not.

These are often called “deepfakes”, but calling them “fake” can minimize their impact and harm. The person depicted experiences real violations of privacy, dignity, and bodily autonomy, and the images can spread online in ways that are impossible to control. Manipulating someone’s image without consent is about exerting power and control over their body and identity. Creating or sharing AI nudes is against the law, and if it includes minors, it is considered child sexual abuse material.

Who is targeted?

- The victims are much more likely to be [girls and women](#)
- Female celebrities and [politicians](#) were some of the first targeted by these apps, which have now expanded to target everyday women and girls
- The creators and distributors are much more likely to be [boys and men](#)
- Many apps offer more features, or focus exclusively, on [women’s bodies](#) rather than men’s bodies, so the technology companies are helping create and reinforce this gender imbalance

Why do people create AI nudes?

AI nude generators are often marketed in ways that make them appear harmless, humorous, and easy to use. Many boys and young men are encountering this technology [without seeking it out](#).

[Motivations](#) for creating AI nudes can include:

- Peer pressure and social currency
- Coping with romantic rejection
- Perceived permissibility
- Sexual curiosity
- Spreading rumors or explicit harassment

If you are concerned about immediate harm to a youth’s physical or mental wellbeing, please reach out to a professional using [these resources](#)!



How prevalent are AI nudes amongst youth?



1 in 8 young people (ages 13-20) indicate they personally knew someone who had been the target of AI nudes (13%)



1 in 8 indicate they personally knew someone who had created or redistribute AI nudes of minors (12%)



Nearly 1 in 10 young people do not believe AI nudes harm the person depicted, with the most common reason being that they are not “real”

Examples of Deepfake Content

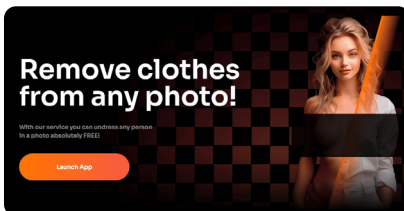
1. Overview
2. Deepfake Content Examples
3. Mentoring Tipsheet
4. Video Discussion Guide

How is AI content generated?



General AI image generators

Users of general AI tools can create images, placing a real person's face or likeness into fabricated scenarios. This can include realistic but fake scenes, making it difficult to distinguish between real and manipulated content. Grok, the AI chatbot from Elon Musk's company, launched an image editing feature that led to widespread creation of sexual images, including many of children.



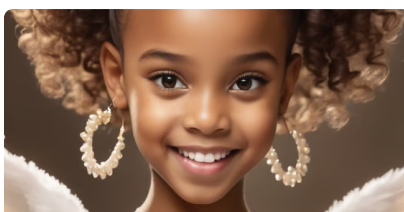
Undressing apps

Users can upload photos of real people, and the app creates a fake image that combines the person's appearance with other images to make it look like their clothing has been removed.



Face swap apps

Users can upload images of anyone and replace the subject's face with a new one, be it celebrity or someone they know.



Lack of age restrictions on images

Many apps have weak or nonexistent safeguards on how images are created, which can enable the creation of content involving minors that is considered Child Sexual Abuse Material.



Mentoring Tipsheet

1. Overview
2. Deepfake Content Examples
3. Mentoring Tipsheet
4. Video Discussion Guide

1

Initiate conversations about consent, dignity, and agency

Discuss digital boundaries:

- Remind them: consent applies to photos, always ask before posting photos of others, and expect others to ask you.
- Model consent with photos: "Can I take a picture of you?" "Can I post this picture of us?"
- Use media (TV, movies, and online content) as conversation starters: "How does this character respect privacy and boundaries online?"

Build empathy and recognize harm:

- "How would you feel if this happened to you or someone you love?"
- "How can you tell if someone is being harmed by an image or video online?"
- Explain why AI nudes are a violation of consent and bodily autonomy, and are a form of sexual violence.

Here is more information on how to speak with youth about [consent](#).

2

Help youth recognize digital harm as serious

- Explain that online images can spread quickly and are hard to remove.
- Warn that AI nudes lead to cyberbullying, blackmail, abuse, and [lasting emotional harm](#).
- Talk about feelings victims experience, like ongoing shame, fear, anger, and loss of safety, especially if peers, family, or their community see the image.
- Inform that creating or sharing AI nudes can have legal consequences, including criminal charges under the [Take It Down Act](#).
- Discuss that schools can also discipline students, including suspension or expulsion.

3

Encourage youth to be active bystanders

If a young person encounters an AI nude, here are some steps they can take:

- Don't share it, as forwarding AI nudes causes further harm and may carry legal consequences.
- If a friend shows them an AI nude, they can say that it's not cool, just like the boy does in the AMAZE video.
- If they come across it on a platform, they can report the content on the platform.
- Check in privately with someone affected, remind them they're not alone, and listen without judgment.
- Tell a trusted adult, such as you, so they do not need to handle it alone.

Organizations supporting victims of deepfakes:

- [Deepfake Victim Guide](#) by EndTab
- [Cyber Civil Rights Initiative](#)
- [Take It Down](#) by the National Center for Missing and Exploited Children
- [Stop Non-Consensual Intimate Imagery](#)



“Deepfakes/ AI Nudes”

1. Overview
2. Deepfake Content Examples
3. Mentoring Tipsheet
4. Video Discussion Guide

Questions to Spark Reflection and Dialogue with Youth



To watch the video, click the thumbnail or head to:

amaze.org/video/deepfakes-ai-nudes-are-not-fake-here-is-why/

1. Why do you think the boy in the video and other boys use undressing apps to generate AI nudes?
2. Why do you think the boy didn't think it was a big deal to create an AI nude of a classmate?
3. How might the girl feel if she found out about the image? And why might these feelings follow her long after the creation of the image?
4. In the AMAZE video, his friend spoke up when he saw the AI nude. Do you think that was hard or easy for him? Why?
5. How can you call out disrespectful behavior without losing a friendship?
6. What can be done to stop the spread of disrespectful and violating AI-generated images?

Wrap Up Points

- 1 Using anyone's image without their consent is a violation of their dignity and **using their image to create an AI generated nude is a form of sexual violence.**
- 2 **Just because an AI nude is “Fake” or fabricated, that does not make it harmless.** AI nudes have a long-lasting impact on the person the image was created of leading to feelings of shame, fear, anger, and hopelessness.
- 3 **Standing up** when you see your friends using this kind of technology may be scary, but it is really a form of kindness as it prevents your friend from doing something that they may not have realized is hurtful.
- 4 While stopping the spread of images is our responsibility, it is also the responsibility of companies and elected officials to **regulate and prevent the use of this technology.**

