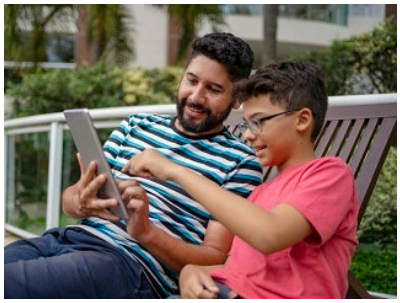
5 Keys to Monitoring Kids Online Activity

By Caitlin Bootsma



Technology is here to stay. Not only is it here to stay, it's everywhere! Televisions, mobile phones, iPads, interactive video games, smart watches, you name it and it's hooked up online.

The following are five starting points for guiding kids to use the internet and technology safely and well. Each family may come up with their own limits around technology use, but every family should think through how they want to approach these areas of monitoring online activity.

Use Protective Software: One of the most foundational things you can do to manage what your kids access online is accountability and filter software on all of your online devices. Systems like Covenant Eyes, Bark Home Web Filter, Circle, and options on your router or with your internet provider can help you not only limit what sites and apps kids access and when, but also allow you to see their online activity.

Share Passwords and "Friend" or follow Your Kids' Accounts: Many parents establish some ground rules when their kids are old enough to have their own email and social media accounts. These rules may include friending or following them so that you see what's happening on their pages and/or sharing passwords—though it's important to know that many platforms allow them to block some people from seeing everything. Other rules can include only connecting with people they know in real life and not sharing any personal information such as address, phone number, email, or banking information. You can go through their accounts with them to ensure they are as safe as possible.

Discuss Photo/Video Sharing: Photo/video sharing should only be done with people they know in real life. Let them know any images they choose to share remain online permanently, and that once they share a photo or video, they can't get it back. If anyone ever asks them to send photos or videos of a sexual nature, they should immediately inform a safe adult.

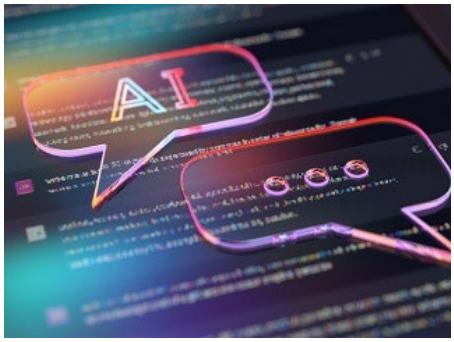
Keep Online Activity Visible: Consider only having your kids use technology in public spaces in the house. This can help reinforce the message that they should not be accessing anything inappropriate and also make it easy for them to talk to you if they encounter anything questionable. Another option to consider is to remove access to electronic devices during bedtime hours. However, keep in mind that children may take electronic devices with them, or may use technology in places apart from your home, which means that regular conversations are important!

Regularly Talk about Online Activity: It can be easy for adults and kids to become isolated in their online activity; it can easily become their own world, separate from the family. Make technology use part of your dinner table conversation—did they hear from any friends today? Read an interesting article? See something new they want to watch? Like any other area of their lives, technology is a sphere where you can provide invaluable guidance and feedback.

As we know from our own lives as adults in the digital era, the internet has a lot to offer. It also has a number of risks, including safety, online addictions, wasting time, and more. We have the opportunity to help guide our kids how to use the internet safely and well!

Artificial Intelligence - Deepfakes and Child Abusers

By Robert Hugh Farley, M.S.



Introduction

Law enforcement has established that preferential-type child abusers, and sometimes situational-type child abusers, almost always maintain a "collection." Those collections generally consist of pornography, child pornography (better known as child sexual abuse materials, or CSAM), and "trophies," or "souvenirs" of the sexual abuse of a child.

Abusers, while perusing their collections, will often manipulate some of the photos or images of children for their own sexual purposes. Sadly, the abuser manipulation or editing of images of children has increasingly become more problematic with the use of technology. In fact, this abuse changed dramatically in 2023/2024 with the use of artificial intelligence, or what is commonly known as "AI."

Background

Child abusers manipulating the images of children in their collections is not a new phenomenon. One early technique was the "cut and paste" method. With scissors, the abuser would cut a child's face or particular body part from a photograph. The clipping would then be pasted onto another photograph, which created a sexually suggestive depiction.

Another image manipulation technique involved child abusers filming videos of themselves in sexually suggestive poses or during a self-sexual activity. The molesters would then edit and combine the suggestive video of themselves into a second video with children, which essentially resulted in a video depicting child sexual abuse.

Additional image manipulation techniques were developed as an unintended consequence of the Internet and social media. By way of example, for many years, parents should be aware of the danger of posting innocent images of their children on social media. During the COVID-19 pandemic, the term "sharenting" was dubbed to describe parents who "over-share" and frequently post numerous images and videos of their children's lives and interactions online. Unfortunately, child abusers troll social media, and the Internet in general, looking for images of children to capture and modify into something lewd and pornographic.

Artificial intelligence

Artificial intelligence, or AI, is technology that enables computers and machines to simulate human intelligence and problem-solving capabilities. AI can perform tasks that would otherwise require human intelligence or intervention.[1]

The Logic Theorist was a program funded by Research and Development (RAND) Corporation, and initially designed to mimic the problem-solving skills of a human. It is considered by many to be the first artificial intelligence program and was presented in 1956 at the Dartmouth Summer Research Project on Artificial Intelligence (DSRPAI), which was hosted by John McCarthy and Marvin Minsky. In this historic conference, McCarthy, imagining a great collaborative effort, brought together top researchers from various fields for an open-ended discussion on artificial intelligence, the term which he coined at the very event.[2]

From 1957 to the 1980's, AI continued to grow and flourish. Computers could store larger amounts of information and became faster, cheaper, and more accessible. Machine learning algorithms also improved, and people got better at knowing which algorithm to apply to their problem. Today we live in the era of "big data," an age in which we have the capacity to collect and sift through huge quantities of information too cumbersome for a person to process. Digital assistants, GPS guidance, autonomous vehicles, and generative AI tools, like Open AI's Chat GPT, are just a few examples of the AI that is exploding in world news, business and in our daily lives.

Of course, people with inappropriate, unsafe or abusive intentions are also taking advantage of the exploding AI technology. This was seen recently in January 2024, when innocent images taken of Taylor Swift were manipulated using an AI tool into "deepfake" sexually explicit content and were then posted online, and viewed over 45 million times before they were taken down. In this same way, new AI technology has become more accessible and made it easier for child abusers to create and share explicit images of children.

AI - Deepfakes and child abusers

A deepfake is an artificial image or video (or a series of images) generated by a special kind of machine learning called "deep" learning, hence the name, "deepfake."[3] This is much different than the use of apps like Photoshop, Face swap, Snapchat, etc., some of which are designed for amusement and clearly fake. Deepfakes are far more dangerous, as the application of deep learning that is used to produce the false image creates an environment in which humans frequently cannot discern whether the images or videos are real or fake.

Today child abusers are increasingly using publicly-available AI platforms to create and then distribute deepfake CSAM, which is criminally referred to as child pornography. For instance, in May 2024, the FBI arrested a Wisconsin man for creating and distributing approximately 13,000 "hyper-realistic images of nude and semi-clothed prepubescent children," several of whom were involved in sexually explicit conduct. Evidence from the Wisconsin man's laptop allegedly showed he used a popular "Stable Diffusion" AI model, first released in 2022, which turns text descriptions into photo-realistic images. This is only one example of many.

According to a U.S Department of Homeland Security publication, AI allows for the creation of CSAM in a variety of ways:

- Abusers can use AI to take an image of a child and make it appear as though the child is nude or the child is engaged in sexual acts.
- Abusers can use AI to create an image of a child being sexually abused via text prompts.
- Abusers can use AI to teach other abusers how to engage with children online (i.e., grooming).
- Abusers can re-victimize CSAM victims repeatedly, by using AI to edit previously created and shared CSAM to create new CSAM.

Conclusion

Over the years, law enforcement has repeatedly found that child abusers are on the cutting edge of technology and use that technology for the sexual exploitation of children. If you become aware of any sexually explicit images or videos, please contact the National Center for Missing and Exploited Children's Cyber Tipline at https://report.cybertip.org/. You can also contact law enforcement.

Social Media Rules to Follow with Children

By The VIRTUS® Programs

As an employee or a volunteer within your diocese or organization, there may be times where you need to communicate via technology with children and youth within your ministry or program. This brings us to a question we frequently hear at the VIRTUS® Programs: Do we need to treat in-person interactions more carefully than electronic interactions?

You will certainly hear a different answer to this question depending on whom you ask. When it comes to transparency and monitoring interactions—it's just as important to follow appropriate standards for electronic interactions as it is for in-person interactions. It's important to have transparency and monitoring in our actions as we follow appropriate standards in online environments—because they involve situations that are already inherently more isolated than face-to-face communication. In this way, our in-person interactions serve as our baseline approach, and we incorporate more checks and balances in environments involving technology. Technology such as social media, email, text and texting apps can be great tools that help us as we serve others in ministry, and they can be beneficial in expanding avenues of communication. However, like any tool, communication through technology must be used appropriately and safely, or it can cause significant harm.

Below are some general guidelines for safe adults in ministry, whether you are communicating with youth who are involved in your ministry, or who are simply associated with the ministerial environment. Reviewing these guidelines encourage us to engage with healthy boundaries, help us to be proactive with any type of technology, and help us to model appropriate online behavior for the children in our care.

DO NOT

- Do not use your personal social media accounts to "Friend" or "follow" children in your ministry.
- Do not email from a personal email address.
- Do not create a ministry-specific account without your organization's permission.
- Do not "troll" any child or youth's personal social media accounts, comment on them, or try to obtain more information about the child based on what they post.
- Do not take or post photos or videos of youth upon any social media account, unless you have approval from the organization (such as for inclusion in a parish or school newsletter), signed, parental permission, and subsequent permission from the child himself/herself.
- Do not "chat" or "private message" or "text" children one-on-one.

DO

- Read and follow the rules regarding social media usage from your parish, school, diocese or overarching organization. Speak with your organization if they do not have any policy or rules, or if the policy needs to be strengthened.
- Contact children and youth only utilizing social media platforms approved by your organization.
- Request that your organization create a ministry-specific email address that you can utilize to communicate with youth, instead of a personal one.

- Behave with transparency in all electronic interactions, which can mean copying a parent listserv to all interactions, or utilizing an app (approved by your diocese) to text youth so that the content is not coming from your own phone number nor your personal account.
- Keep your own social media profiles and pages tidy and clean; be aware of clothing, what is portrayed by the images you share or are tagged within, perceptions that you could lend to others, be mindful of removing images/jokes involving alcohol, etc. (This is simply a good practice in general, and most useful in case kids do come across your accounts).
- Set your personal accounts to "private" so it isn't as easy for children to "stumble" across your personal material. Your relationship with people in ministry is predicated upon your role, and not your personal life.
- Communicate with youth during appropriate timeframes—the same timeframes that you would generally call a "landline."
- Refer children to your office hours if they contact you "after hours." It helps to clearly state this in advance, that you are available between "xy" hours, and that messages will not receive responses until those office hours.
- Be "friendly" with minors in social media interactions, but avoid being a "peer" type of friend.

Additionally, if you receive a "friend" or "follow" request on a personal social media account from a child or youth, do not accept it. Instead, refer them to the parish, school or program social media account. If you are meeting with a child or youth via a video-based option (such as Zoom), take steps to keep it transparent, such as inviting another adult to participate in the meeting, or having yourself within the sight and hearing of other adults.

One of the most important ways to protect children and youth is to maintain an ongoing dialogue with them about healthy social media interactions. It is also helpful to familiarize yourself with current trends and popular apps, as youth may come to you (one of their safe adults) with questions. Sometimes children may come to you with a disclosure of abuse that happened to them in the past, or that is currently happening—or perhaps is about to happen. We always believe children when this occurs and report it to the appropriate entity. To report any disclosed or suspected sexual exploitation of a child or youth, call the child protective services1 within the state. If a child is experiencing abuse via social media or other electronic means, you can help them to make a report to the National Center for Missing and Exploited Children's CyberTipline2 or make a report on their behalf. You can also contact law enforcement.

Conclusion

Social media can be a wonderful tool that can enhance communication within a parish, school or other program—as long as it's used appropriately and in a way that promotes healthy boundaries. If you have any questions about your organization's social media policy, please reach out to them directly for more information.

Available Resources

For additional information on technology safety, please visit:

NetSmartz https://www.missingkids.org/netsmartz/resources

Common Sense Media https://www.commonsensemedia.org/articles/social-media

National Center for Missing and Exploited Children https://missingkids.org/home