AbusePrevention®

Virtual Instruction – Navigating Online Resources and Child Safety

Gregory S. Love, Esq.
Kimberlee D. Norris, Esq.
April 17, 2020

Since mid-March, virtually all K-12 education is occurring remotely. In many ways 'social distancing' has limited the risk of inappropriate physical touch, while *increasing* the risk of inappropriate online communication. In the wake of Covid-19, how can schools and ministries mitigate the risk of child sexual abuse through online virtual instruction? The list below suggests current best practices.

DEFINITION OF SEXUAL ABUSE

Keep in mind that child sexual abuse does not require touch; a child does not have to be *physically touched* to be sexually abused. By definition, child sexual abuse is any tricked, forced, manipulated or coerced sexual activity for the pleasure of the abuser. Children and teens may be easily manipulated into sexual activity through online communication applications.

GROOMING PROCESS

Making sense of these suggested best practices requires a working knowledge of the *grooming process of the preferential offender*. The grooming process – the process by which an offender selects and prepares a child for inappropriate sexual interaction – varies based upon the age and gender of the targeted child. At Abuse Prevention Systems (APS), the information describing the *preferential offender* and the offender's grooming process is communicated through Sexual Abuse Awareness Training. Click here to request a free online Sexual Abuse Awareness Training link.

For younger children (K through 6th grade), grooming does not often involve the use of social media, online chat and sexting. The younger student may not have a smart phone, may not have ready access to communication apps and is less likely to pursue sexual content or communication. (*Of course, some very young children are operating a smart phone and engaging in online communication, mimicking an older sibling or television program*.) Younger students are at risk, but not in the same manner or degree as an older child, who is actively clicking, swiping and messaging within communication apps (i.e., Snapchat, Instagram, Skype, TikTok, Twitter, all of which have direct messaging functionality).

USE OF TECHNOLOGY

Keep in mind, normally adjusted individuals do not commonly think like sexual predators. When an educator or parent chooses a platform to deliver online content, he or she evaluates the platform based on intended use and efficiency, and no further. The predator, by contrast, will explore every aspect of the application or platform to understand how to create virtual 'trusted time alone'. This may include the use of direct messaging, one-on-one invitations to communicate and the exchange of images or video content. While creating a plan for distance learning, educators and administrators must *fully* evaluate online systems, including the strengths and weaknesses of each *in light of how a predator may exploit the system*. To skillfully undertake this sort of evaluation, the administrator must first understand the *offender's grooming process,* thereby recognizing *what* the abuser hopes to accomplish, and *how* each online resource may be improperly utilized by the offender.

When administrators understand how an abuser will exploit online access and the strengths and weaknesses of various online platforms or resources, decision makers can implement policies that shore up identified weaknesses.

Middle & High School

In colleges and universities, 'distance learning' is commonplace, relying on systems such as Blackboard, Canvas and other customized online solutions. Distance learning is becoming more widespread and accepted in high schools and home school coops across the country. Common online streaming resources include Zoom, Skype, GoToWebinar and others. In middle and high school environments, students are already exploring online applications in the context of social interaction and relationships. Because middle and high school students are already participating in a virtual world, they are easier to engage, manipulate and deceive by a third party with the wrong motive.

K through 6th

Distance learning is not as commonplace for kindergarten and elementary grades. As a result, children are not accustomed to online applications, usernames, passwords and security settings. Further, an adult or older sibling is usually required to set up and configure online resources (i.e., Zoom, Skype, GoToWebinar). Because children in this age group are less likely to be participating in virtual relationships, they are less likely to be the object of solicitation or deception by an unknown third party. On the other hand, if a younger child is introduced to online communication, he or she is *far* more vulnerable to an adult or older student that the child has been taught to trust and obey if such a person targets the child through this new online environment.

BEST PRACTICES

Administrators and educators should approach the Best Practices referenced below with two realities in mind: the instructional goals desired <u>and</u> the grooming process of the preferential offender. In short: (1) what instruction can be accomplished; and (2) how might an offender attempt to compromise the environment.

Once a plan is created, administrators and educators should create written policies outlining proper expectations of staff members, parents and students. These policies should incorporate the appropriate best practices and the contact information for the individual(s) to be notified if a policy violation occurs.

Electronic Communications/Online Classes

- Remember: abusers '*groom the gatekeepers'* to convince gatekeepers that they are trustworthy and responsible individuals.
- Watch for '*common grooming behaviors'*: one-to-one interaction with a single child, special privileges and rule-breaking, including rules related to electronic communication.
- If a boundary is crossed by a minor or adult, report to a supervisor immediately.
- Consider the use of mobile phones or services that facilitate communication without revealing personal phone numbers.
- Avoid one-to-one communication (by telephone, Skype, Facetime, direct messaging); all communication should be public and transparent. Set a policy of at least three students in every class, a parent present (continuously) or at least two teaching staff members.
- Do not permit sending or requesting photos, images or video of individuals; in the event a video-captured presentation is required to be submitted, the submission e-mail (or other form of electronic communication) should include a parent or at least two teaching staff members.
- Do not use electronic communication to discuss or post sexual topics, including memes.
- Do not share personal information unless specifically related to educational purposes. Do not ask minors to share personal information unrelated to educational purposes. Conversations should be related to projects, educational subjects or curriculum.
- Tell students and parents *who to tell* if a violation occurs, or a parent has concerns.
- Enforce consistent boundaries. Electronic communication may feel 'less real' to students *and* adults. Maintain appropriate decorum in all conversations.

With less oversight and outside interaction, children are more at risk for abuse or neglect.
If child abuse or neglect is suspected, follow reporting requirements in your state.
(See STATE child welfare reporting information HERE.)
WHEN IN DOUBT, REPORT.

Written Communication

- In teaching contexts, copy at least one parent in all written communication to a single student. Request that all student replies include a parent or at least two teaching staff members.
- Do not permit individual direct messaging (i.e., text, Skype, Instagram, Snapchat, Twitter, WhatsApp).

Texting

- Do not use texting to discuss or post sexual topics, including memes.
- If text messaging is contemplated or permissible, *notify parents* that text messages may occur between minors and an adult staff member, and give parents an opportunity to *opt out* on behalf of their child.
- Send and reply to text messages with minors in *group messages* with another staff member copied.
- Do not permit sending or requesting photos, images or videos of individuals.

Social Media

- Communicate with minors through designated ministry group pages on social media platforms.
- Ask staff members to designate their social media profiles as *private* to limit access to personal information.
- Do not allow staff members to 'friend' or 'direct message' minors.

Video Conferencing

- If video conferencing technology is utilized, ask staff members and minors to have an appropriate background, personal dress and professional demeanor. Dress should be similar to what each individual would wear in public; no pajamas, bathing suits, or partial nudity.
- *Record* all video conferencing occurring with students and inform staff members of this policy.
- Designate one or more staff members to scan recorded conferencing after the fact.
- Consider 'drop in monitoring' of video conferencing occurring with students or minors.

Zoom

Zoom is one of the most popular online learning tools. Zoom and other video conferencing applications have the ability to record. Each Zoom class should be recorded and uploaded such that an independent designated person may access and view recorded classes to ensure appropriate content and interaction. *This practice protects students AND staff members.*

Caveat: Zoom has experienced security challenges wherein unknown third parties have hacked into Zoom meetings and uploaded violent or sexually explicit content.
Zoom is currently working to provide security updates.

Skype

Skype is useful, but requires that every user have a Skype ID. Use great care to ensure that each student's Skype ID is kept confidential. This can be difficult in a group setting, as each student will have access to all other participants' Skype IDs. This becomes problematic if one or more student's Skype ID is inadvertently posted on social media or in a public forum. A third party may use a publicly posted Skype ID to solicit, befriend or send inappropriate content to a minor.

YouTube

Avoid assigning projects referencing YouTube videos – especially to younger children. YouTube is convenient but includes sidebars of 'suggested videos' on the same page. Many of these suggestions are highly inappropriate and contain adult content. If the same content is available through Vimeo (or another platform with controlled content) use this alternative. *Parents are often involved in the early stages of distance learning but stop monitoring once their child gets into a rhythm*. Administrators should encourage parents to *STAY ENGAGED.*

STAFF TRAINING
While many staff members and volunteers are working from home, consider getting a jump on the upcoming ministry/education season by training at the next level. The various depths of training are described below, and can be delivered, tracked and refreshed using the **Abuse Prevention Systems Online Platform**.

All child-serving staff members and volunteers should complete **Sexual Abuse Awareness Training**. Managerial employees should complete **Sexual Abuse Awareness Training** and **Skillful Screening Training**.