Online Child Exploitation Prevention Initiative

Guidance for School-Based Professionals and School Leaders

Addressing Children's Use of Generative Artificial Intelligence (GenAI) to Create Sexually Explicit Deepfake Imagery

The safety and protection of children are essential to the mission of every school. Each year, tens of millions of reports of child sexual exploitation are made to the CyberTipline run by the National Center for Missing & Exploited Children (NCMEC), with a growing trend of sexually explicit images being produced by individuals using generative artificial intelligence (GenAI) programs.

In many cases, individuals use GenAI to create "deepfake" images: for example, they use GenAI to manipulate benign images of actual children to make it appear as though the children are engaged in sexually explicit conduct.

As GenAI technology continues to advance rapidly, it is critical that school communities equip themselves with the tools and knowledge needed to safeguard children, develop an effective and victim-centered approach to helping children who have been victimized, and implement effective prevention programming. This document aims to help schools in that endeavor in 4 sections:

1. Know the issue
2. Understand the impact
3. What can schools do?
4. Resources, additional information, and requests for guidance

1 Know the issue

What is GenAI and how does it work?

As Harvard University describes it, GenAI "is a type of artificial intelligence that can learn from and mimic large amounts of data to create content such as text, images, music, videos, code, and more, based on inputs or prompts." See **huit.harvard.edu/ai**. To use a GenAI platform, a user first enters a prompt—for example, text, or an image—and, depending on the type of prompt, also enters some kind of instruction to the AI platform regarding what to do with the prompt. In response, the AI platform generates responsive content, such as text or an image.

An emerging trend in the misuse of GenAI technology by minors involves using face-swapping apps, so-called "nudify" apps, or other similar apps and websites to create sexually explicit deepfake images of other minors (often classmates or friends), teachers, and others. The technology is inexpensive to obtain, widely accessible, unrestricted to minors, easy to use, and can create imagery that is photo-realistic and difficult, if not seemingly impossible, to distinguish from non-GenAI images. This problem presents a unique and difficult set of complexities.

Unlike adult offenders who create this kind of deepfake imagery usually to obtain sexual gratification or to extort the pictured minor, when minors create these deepfake images, they often do so, we think, out of curiosity, or as a modern-day form of harassment, bullying, or teasing. These motivations are distinguishable from a motive to sexually exploit the victim, for example, through sextortion.[1] Also, whereas the criminal justice system is well-equipped to deal with adults who create sexually explicit deepfakes, that system is often less equipped to deal with minors who do so, particularly when the motive is curiosity-related or harassment, bullying, or teasing. Finally, minors who create sexually explicit deepfake images of others may not understand the gravity of the harm that their acts can impose upon the pictured individual. Making matters worse, in addition to creating sexually explicit deepfake images of others, minors may also share those images with others on social media, through messaging applications, and otherwise. Taken in combination, these concerns—children, perhaps unwittingly or non-maliciously, causing potentially very acute harms on other children—call for a careful and considered response.

Examples:

politico.com/newsletters/digital-future-daily/2024/05/29/for-deepfake-nude-victims-the-future-is-already-here-00160483;

nbcnews.com/tech/tech-news/beverly-hills-school-expels-students-deepfake-nude-photos-rcna142480;

abc7ny.com/nj-westfield-high-school-artificial-intelligence-pornographic-images/14009286/

2 Understand the impact

Victims of sexually explicit deepfake imagery often suffer considerable harm and trauma, including anxiety, embarrassment, and reputational injury. In addition, victims may experience complex and distressing emotions surrounding who created the image, where and to whom it was circulated, whether additional imagery is out there, and whether the imagery can be removed from circulation. Victims may worry that their friends, family, and others will believe that the imagery is real, and this concern may cause victims of sexually explicit deepfakes not to come forward and seek help. As NCMEC has said, "[f]or the children seen in deepfakes and their families, it is devastating."

[1]In one of its variations, sextortion involves the misuse of GenAI to generate sexually explicit deepfake images in furtherance of an effort to extort children into paying money, sending sexually explicit imagery, or acceding to some other demand. For further information on this issue, please see **missingkids.org/theissues/sextortion**.

3 What can schools do?

Understand the Problem.

Some research shows that teachers, parents, and guardians are less aware than students are of the AI-deepfake problem. As educators strive to create a safe and supportive learning environment for their students, understanding and addressing the threats posed by deepfakes is crucial to maintaining the integrity and safety of our schools. Schools should undertake to learn more about the problem, both at the national level and, perhaps more importantly, at the school-district and individual-school levels. School districts and schools may do this through student surveys, through discussing the issue with school-based professionals (e.g., teachers, mental health professionals, administrators, coaches, and school resource officers), through engagement with parents and guardians, and otherwise.

Understanding the potential legal, social, financial, and psychological implications of GenAI and the creation and distribution of AI deepfakes is also essential. Some key concerns include:

- cyberbullying and harassment of students, including the creation of non-consensual sexually explicit deepfakes, and managing the creation and circulation of sexually explicit deepfakes and determining appropriate responses; and
- consideration of the legal consequences that could attach to the creation and distribution of sexually explicit GenAI deepfake imagery.

Develop policies and procedures.

Given the rapid rise of this issue, current school policies may not sufficiently address students' misuse of GenAI technology to generate sexually explicit deepfake imagery. In addition to understanding the problem, schools should develop and implement pertinent policies and procedures—just as most schools have done with respect to bullying, sexual harassment, and the like. For instance, schools should develop a clearly defined approach to how they will investigate claims that a student has created sexually explicit deepfake imagery or distributed such imagery. Schools should also develop a clearly articulated set of potential interventions for students who create or share such imagery, which may include things like counseling, restorative justice, detention, suspension, expulsion, or referral to law enforcement. Schools must also, of course, abide by governing law, including state laws on mandated reporting.

Develop and implement a victim-centered response program.

Given the gravity of the harm that depicted children often experience, schools need to give careful consideration to how they will engage with victims who are pictured in sexually explicit deepfake images. This, in turn, requires a victim-centered approach that is trauma-informed, that recognizes the scope and gravity of the harm, and that provides victims with counseling, resources, and other appropriate support—including information, for example, about NCMEC's Take it Down program (**takeitdown.ncmec.org**), which allows child victims to take steps to have their imagery removed from certain online platforms. Schools should also ensure that all school-based professionals are aware of the steps to take upon learning that a student has been victimized in this way.

Invest in prevention programming.

It is also imperative that schools implement prevention programming in an effort to teach students that creating and sharing sexually explicit deepfake imagery of others can cause great harm to the depicted individuals. Schools can leverage existing prevention resources from organizations and government agencies (some resources are linked at the end of this document). If developing their own prevention programs, collaboration with key stakeholders is critical to ensure a comprehensive and effective approach.

4 Resources, additional information, and requests for guidance

Combatting the misuse of GenAI to generate sexually explicit deepfake imagery is a complicated and evolving problem that requires a careful, deliberate, and multi-pronged response. Further complicating matters, AI technology is evolving rapidly, and as the technology changes, so will the threats, and so will the appropriate responses and preventative efforts.

Although schools are well positioned to be on the front lines in combatting this problem, schools are not alone in this effort. There are a number of resources available to help schools navigate these issues. For example:

- The Online Child Exploitation Prevention Initiative has developed a set of ten best practices for effective prevention programming: **icactaskforce.org/OCEPI**
- NCMEC, the United States's leading non-governmental child protection organization, has multiple resources that can help:
  - NCMEC runs a 24-hour hotline for children and families: **1-800-THE-LOST (1-800-843-5678)**
  - NCMEC also runs the CyberTipline that allows victims to file formal reports, which NCMEC reviews and assesses before making available to the appropriate law enforcement agency: **report.cybertip.org**
  - NCMEC's Take It Down program allows children to anonymously take proactive steps in an effort to remove sexually explicit content depicting them from various online platforms: **takeitdown.ncmec.org.**
- Various organizations, including NCMEC (**missingkids.org**), A21 (**a21.org**), the Carly Ryan Foundation (**carlyryanfoundation.com**), the Department of Homeland Security (**Know2Protect.gov**), the United States Secret Service (**secretservice.gov/investigations/ncmec**), and the Internet Crimes Against Children Task Force Program (**icactaskforce.org**) are experienced and well-situated to engage with schools on these issues.
- The Center for Democracy & Technology has conducted surveys and published a report on the problem of students using GenAI to create sexually explicit deepfake imagery: **cdt.org/wp-content/uploads/2024/09/2024-09-26-final-Civic-Tech-Fall-Polling-research-1.pdf**; **cdt.org/wp-content/uploads/2024/09/FINAL-UPDATED-CDT-2024-NCII-Polling-Slide-Deck.pdf**
- The non-profit organization Thorn has also published information on children's use of GenAI to create sexually explicit deepfake imagery: **info.thorn.org/navigating-deepfake-nudes**; **info.thorn.org/hubfs/Research/Thorn_DeepfakeNudes&YoungPeople_Mar2025.pdf**.

In addition, OCEPI is available to provide additional information and guidance, and can help schools and school districts develop appropriate policies and practices. Please visit our website, **icactaskforce.org/ocepi**, or reach out to us through the "Contact Us" link on our website.

The Online Child Exploitation Prevention Initiative (OCEPI) consists of individuals and agencies specializing in efforts to prevent children from becoming victims of online sexual exploitation and abuse. Initiative members are experts including federal, state, and local law enforcement, ICAC Task Force members, researchers, educators, prevention specialists, training partners, and child protection organizations.

This project was supported by Grant #15PJDP-23-GK-00804-MECP awarded by the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. The content was developed by the Online Child Exploitation Prevention Initiative. Opinions, findings, and conclusions or recommendations expressed in this publication are those of the Initiative members and do not necessarily reflect those of the Department of Justice.