

// SAFEGUARDING RESOURCE · FOR SCHOOL-BASED PROFESSIONALS & SCHOOL LEADERS

Guidance for School-Based Professionals and **School Leaders**

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

Keeping children safe is central to the mission of every school. Each year, tens of millions of reports of child sexual exploitation reach the CyberTipline operated by the National Center for Missing & Exploited Children (NCMEC) — and a growing share now involve sexually explicit images produced with generative artificial intelligence (GenAI) tools.

A common pattern is the "deepfake": GenAI is used to alter ordinary, innocent photos of real children so that they appear to depict sexually explicit conduct.

As GenAI capability advances rapidly, school communities need the knowledge and tools to safeguard students, respond to victims in a trauma-informed way, and run effective prevention programming. This resource supports that work across four sections:

// CONTENTS

- 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?

Generative AI describes systems that learn patterns from large volumes of data and then produce new content — text, images, audio, video, or code — in response to a prompt. A user supplies an input (text or an image) plus an instruction, and the platform generates responsive output.

An emerging misuse trend among minors involves face-swapping tools, so-called "nudify" apps, and similar websites being used to create sexually explicit deepfake images of other minors (often classmates or friends), teachers, and others. The technology is cheap, widely accessible, unrestricted to minors, simple to operate, and produces photo-realistic imagery that can be extremely difficult to tell apart from genuine photographs. That combination creates a uniquely difficult set of problems for schools.

Adult offenders who make this material typically act for sexual gratification or to extort the pictured minor (sextortion). When minors create it, the driver is more often curiosity, or a modern form of harassment, bullying, or teasing. Those motives matter: the criminal justice system handles adult offenders relatively well, but is often less equipped for minors — especially where the motive is curiosity or bullying rather than exploitation.

Minors who create these images frequently fail to grasp the severity of the harm done to the person depicted — and may compound it by sharing the imagery over social media and messaging apps. Children unwittingly or non-maliciously inflicting acute harm on other children calls for a careful, considered response.

// REPORTED CASES

Real incidents have been reported at schools in Beverly Hills, CA and Westfield, NJ, among others — coverage via Politico, NBC News, and ABC7 NY.

2 Understand the **impact**

Victims of sexually explicit deepfake imagery often experience serious harm and trauma: anxiety, embarrassment, and damage to reputation. They also face distressing unknowns — who made the image, where it was circulated, whether more imagery exists, and whether it can ever be fully removed.

Many victims fear that friends and family will believe the imagery is real. That fear can stop them coming forward for help at all. As NCMEC has put it, for the children depicted and their families, the experience is devastating.

Note on sextortion: one variant involves using GenAI deepfakes to pressure children into paying money, sending explicit imagery, or meeting other demands. See missingkids.org/theissues/sextortion.

3 What can **schools** do?

// UNDERSTAND THE PROBLEM

Research suggests teachers, parents, and guardians are less aware of the AI-deepfake problem than students are. Schools should build their understanding at national level and — perhaps more importantly — at district and individual-school level: through student surveys, discussion with school-based professionals (teachers, mental health staff, administrators, coaches, resource officers), and engagement with parents and guardians.

Key concerns to understand include:

- Cyberbullying and harassment via non-consensual explicit deepfakes — and how the school manages creation, circulation, and response; and
- The legal consequences that can attach to creating and distributing sexually explicit GenAI deepfake imagery.

// DEVELOP POLICIES & PROCEDURES

Existing school policies may not adequately cover GenAI misuse. Just as schools have policies for bullying and sexual harassment, they should now define: how claims that a student created or distributed explicit deepfake imagery will be investigated, and a clearly articulated range of interventions — counseling, restorative justice, detention, suspension, expulsion, or referral to law enforcement. Schools must also comply with governing law, including state mandated-reporting requirements.

// BUILD A VICTIM-CENTERED RESPONSE PROGRAM

Given the gravity of harm to depicted children, plan carefully how the school will engage with victims. The approach should be trauma-informed, recognize the scope of the harm, and connect victims with counseling, resources, and support — including NCMEC's Take It Down program (takeitdown.ncmec.org), which lets child victims act to have their imagery removed from certain online platforms.

Ensure every school-based professional knows the steps to take on learning a student has been victimized this way.

// INVEST IN PREVENTION PROGRAMMING

Prevention teaches students that creating and sharing explicit deepfake imagery causes real, serious harm to real people. Schools can leverage existing prevention resources from established organizations and government agencies (see Section 4). If building your own program, collaborate with key stakeholders to keep the approach comprehensive and effective.

Prevention + policy + victim-centered response — schools need all three working together.

4 Resources & further guidance

Combatting GenAI misuse to create sexually explicit deepfake imagery is a complicated, evolving problem requiring a careful, multi-pronged response — and as the technology changes, so will the threats and the right countermeasures. Schools are on the front lines, but they are not alone:

// NCMEC — KEY SERVICES

24-hour hotline for children and families:

1-800-THE-LOST (1-800-843-5678)

CyberTipline — victims file formal reports, reviewed by NCMEC and routed to the appropriate law enforcement agency:
report.cybertip.org

Take It Down — children anonymously take proactive steps to remove explicit content depicting them from various online platforms:
takeitdown.ncmec.org

// ORGANIZATIONS THAT ENGAGE WITH SCHOOLS

- NCMEC — missingkids.org
- A21 — a21.org
- Carly Ryan Foundation — carlyryanfoundation.com
- Dept. of Homeland Security — Know2Protect.gov
- US Secret Service — secretservice.gov/investigations/ncmec
- ICAC Task Force Program — icactaskforce.org

// PREVENTION BEST PRACTICES

The Online Child Exploitation Prevention Initiative (OCEPI) publishes ten best practices for effective prevention programming, and can help schools and districts develop policies and practices:

icactaskforce.org/OCEPI

// RESEARCH & REPORTS

Center for Democracy & Technology — survey research on students using GenAI to create explicit deepfakes: cdt.org (2024 Civic Tech Fall Polling; NCII Polling Slide Deck)

Thorn — research on children's use of GenAI deepfake nudes: info.thorn.org/navigating-deepfake-nudes (Deepfake Nudes & Young People, Mar 2025)

Learn the skills that protect people. Explore free cybersecurity careers content and classroom games at getintocyberjobs.com and gamingforlearning.com

Adapted from guidance developed by the Online Child Exploitation Prevention Initiative (OCEPI) — federal, state, and local law enforcement, ICAC Task Force members, researchers, educators, prevention specialists, and child protection organizations — supported by Grant #15PJDP-23-GK-00804-MECP from the Office of Juvenile Justice and Delinquency Prevention, U.S. Department of Justice. Presented in this format by getintocyberjobs.com, a free K-12 cybersecurity education resource. Opinions expressed do not necessarily reflect those of the Department of Justice.