

// E-SAFETY FACT SHEET

AI, Deepfakes & Your Face

Synthetic images, cloned voices,
and what the law now says
for Students, Teachers, and Parents

Generative AI can now produce convincing fake images, video, and audio of a real person from very little source material — often a single photo taken from a public profile. For young people this creates two distinct situations: being targeted by synthetic content, and being tempted to create it about someone else. Both carry serious consequences, and both are now covered by federal law.

A fake image causes real harm. “It isn’t real” is not a defence in law, and it is no comfort to the person whose face is in it.

This sheet explains what the technology makes possible, what to do if someone is targeted, what the legal position is, and where to get help.

In this document:

- 01 Know the risks
- 02 What can you do?
- 03 The law, resources, and help

1 Know the risks

A. How Little It Takes

Producing a convincing fake no longer requires skill, equipment, or expense. A face from a public profile photo and a few seconds of audio from a video are enough. This matters for e-safety in a specific way: the ordinary, harmless images young people post are now potential source material, and the old assumption that a photo has to be private to be dangerous no longer holds.

B. Explicit Deepfakes of Classmates

Apps that generate sexualised images of real people have been used in schools, by students, against other students. Schools across the country have dealt with incidents of this kind. Two things are worth being blunt about with young people. First, the harm to the person depicted is severe and real — humiliation, anxiety, withdrawal from school. Second, creating or sharing sexualised imagery of a minor is a serious criminal matter regardless of whether the image was generated rather than photographed, and regardless of the age of the person who made it.

C. AI-Enhanced Sextortion

Offenders no longer need a young person to send an explicit image in order to threaten them with one. A benign photo taken from a social profile can be altered, and the altered image used as leverage to demand money or real imagery. Victims sometimes feel less able to seek help precisely because they know they never sent anything — and because they fear nobody will believe the image is fake. Paying or complying does not end it; it confirms the target will respond.

D. Voice Cloning and Impersonation

A short clip of someone speaking — from a video, a stream, a voice note — is enough to clone a voice. This is used in urgent-sounding phone calls: a relative apparently in trouble, needing money immediately, with the voice sounding exactly right. The defence is not detection but procedure: verify through a separate channel, or use a pre-agreed family code word.

E. Fabricated Evidence and Misinformation

Synthetic images and video are used to bully, to fabricate apparent misbehaviour, to spread false claims about individuals, and to manufacture screenshots of things people never said. A fake can circulate through a school in an afternoon, and a correction never travels as far as the original.

F. The Detection Trap

Advice to look for extra fingers, odd lighting, or strange blinking is already unreliable, and it gets worse every year. Teaching young people to spot fakes by eye builds false confidence. The durable skills are different: check whether a credible source is reporting the same thing, consider who benefits from you believing it, and be most sceptical of content that arrives with urgency attached.

2 What can **you** do?

If synthetic images of you are being shared

FIRST	This is not your fault, and you are not in trouble. You did nothing wrong by having a photo online. The person who made it is responsible.
STEP 01	Don't delete anything. Screenshot the content, the account, and the URL. Evidence matters, and it disappears fast.
STEP 02	Tell a trusted adult — a parent, teacher, counsellor, or school safeguarding lead. Do not try to handle it alone.
STEP 03	Report and request removal in-platform, and use the takedown routes on the next page. Platforms are now legally required to act.
STEP 04	Don't negotiate with anyone demanding money or images. Stop replying, keep everything, and report it.

For students — before it happens

- ▶ Tighten who can see and download your photos. Private accounts reduce the pool of source material considerably.
- ▶ Agree a **family code word** for urgent phone requests. A cloned voice can't guess it.
- ▶ Treat any urgent, emotional message — however real it looks or sounds — as unverified until you've checked another way.
- ▶ **If a friend is targeted, don't forward it.** Sharing is what causes the harm, and passing it on can itself be an offence. Report it and support them instead.

For students — before you make one

- ▶ Generating or sharing sexualised images of a classmate is not a prank. It can be a **federal crime**, a state crime, and grounds for serious school discipline.
- ▶ Being a minor yourself is not protection. Students have faced criminal charges and expulsion.
- ▶ "It's obviously fake" and "it was a joke" are not defences — not legally, and not to the person in the image.
- ▶ If you have already made or shared something, telling a trusted adult now is better than every alternative.

For parents & caregivers

- ▶ Raise it before it happens, calmly, as something that occurs in schools rather than a hypothetical.
- ▶ Make clear in advance that **you would react with support, not blame**. Fear of being blamed is the main reason young people stay silent about this.
- ▶ Set up the family code word, and remove public photos you no longer want available.
- ▶ If your child is targeted, keep evidence, report to the school and the routes overleaf, and get support for the emotional impact — it is often severe.

For teachers & schools

- ▶ Have a **response plan before an incident**, agreed with your safeguarding lead and legal counsel. Improvising is where schools go wrong.
- ▶ Treat the depicted student as a victim throughout. Reactions that imply fault or shame cause additional, lasting harm.
- ▶ Preserve evidence and follow mandatory-reporting duties — this is a law-enforcement matter, not only a discipline one.
- ▶ Teach the legal reality directly. Many students genuinely do not know that generated imagery is treated as seriously as photographed imagery.

3 The law, resources, and help

Where the law stands

FEDERAL	The TAKE IT DOWN Act was signed into law on 19 May 2025. It makes knowingly publishing nonconsensual intimate imagery a federal crime — and it applies to AI-generated “digital forgeries” of real people, not only real photographs.
TAKEDOWN	Since 19 May 2026 , covered platforms must provide a clear removal request process and act on valid requests within 48 hours . The FTC enforces this.
STATE	All 50 states and DC have laws addressing image-based sexual abuse, and many specifically cover AI-generated imagery. Details vary by state.
MINORS	Sexualised imagery of a minor is treated with particular severity, and federal penalties are higher where the depicted person is a minor.

Summary only, current as of publication, and not legal advice. Consult qualified counsel or law enforcement about any specific situation.

- ▶ **NCMEC Take It Down** — free service helping minors anonymously request removal of explicit images of themselves, real or AI-generated: takeitdown.ncmec.org
- ▶ **NCMEC CyberTipline** — report exploitation of a child: report.cybertip.org · 24-hour hotline 1-800-843-5678
- ▶ **FTC takedown complaints** — report a platform that failed to act on a valid removal request: takeitdown.ftc.gov
- ▶ **Cyber Civil Rights Initiative** — free 24/7 helpline for victims of image-based sexual abuse: 1-844-878-2274 · cybercivilrights.org
- ▶ **FBI IC3** — report sextortion, online crime, and financial loss: ic3.gov
- ▶ **988 Suicide & Crisis Lifeline** — free, confidential support 24/7: call or text 988

For anyone who has been targeted. The distress this causes is serious and it is not proportional to whether the image was real. Support is available, it is confidential, and asking for it is not an overreaction.

// Warning signs a student may have been targeted

- ▶ Sudden reluctance to attend school, or to be photographed
- ▶ Distress, anger, or withdrawal after being online
- ▶ Deleting or locking down social accounts abruptly
- ▶ Secrecy about messages, paired with visible anxiety
- ▶ Changes in friendships, or apparent exclusion from a group
- ▶ Any mention of images they say aren't real

A student who says an image of them is fake should be believed and supported first, and the facts established afterwards — not the other way round.

getintocyberjobs.com · A free resource for K-12 students and teachers across the US.

This fact sheet is for general educational purposes and is not legal advice. Legal requirements change and vary by state; consult qualified counsel and follow your school's safeguarding and mandatory-reporting procedures. If a child is in immediate danger, call 911.