

times2

I made an app to stop school photos being stolen for sex abuse images

A new crime wave in which faces are scraped for deepfake videos has left parents and teachers powerless. This woman is fighting it. By [Claire Cohen](#)



Carole Osborne

TIM JOBLING FOR THE TIMES

It sounds like something from the latest television drama. A group of teachers are gathered in a meeting when a terrifying email comes in: 25 photos of pupils have been stolen from the school’s website and run through AI software to create graphic child abuse images. Unless they pay a ransom of £250,000 in cryptocurrency, the email says, the pictures will be uploaded to the dark web, where any predator can access them. A couple of deepfakes are attached as proof.

Except this isn’t fiction — all over Britain, in a new crime wave, schools are being sent extortion emails by tech-literate gangs demanding huge sums to prevent fake images of children being posted online.

Last week the Internet Watch Foundation (IWF) reported that another unnamed secondary school had been targeted by such a blackmail attempt and 150 images that could be classified as child sexual abuse material had been created.

Carole Osborne was in one crisis meeting last year at a school in Norfolk, where she lives. “It caused panic,” she recalls of the staff’s reaction. “It was like, ‘What do we do?’ There was no real solution.”

At the time the 48-year-old single mother felt as helpless as the teachers. The owner of a communications agency, she worked with schools on marketing material, newsletters and social media to help them to attract new students amid a declining birth rate — much of which relies on photographs of happy pupils smiling in their school uniforms. Now those innocent images were at risk, with potentially devastating consequences.

“I walked out of that room in shock and immediately called the five other head teachers I was working with to warn them this was happening,” she says. “Every single one said, ‘We’ve already heard and we don’t know what

to do about it.’ One head told me, ‘We’re just crossing our fingers that nothing happens to us.’”

Another admitted that it had already happened to them a few weeks earlier and they hadn’t paid the ransom or reported it to the police, just hoped it would go away. “At that point I realised it was a big problem,” she says.

Osborne went into “mama bear” mode, terrified this could happen to her own daughters, then 14 and 17. After spending weeks researching a solution for schools — there wasn’t one — she decided to take matters into her own hands. Twelve months on she’s launching an app, called Aidos, which gives them the power to alter pupils’ faces in photographs before they are shared online, using good AI to combat bad. Protecting children has become an obsession.

“I’ve never felt so driven. I go to sleep thinking about it and I wake up thinking about it. It means so much if I can protect even 100 children...” she says, her voice catching with emotion. “I hate the fact that this is happening. I hate the fact that we, as parents, even have to think about it. I just hate that kids are being used in this way. That’s what keeps me going.”

Until now, reports of explicit deepfakes in schools have meant students making images of each other or teachers. “My daughter was next to me on the sofa the other day and someone had sent a video they’d made of another pupil. It’s so common,” Osborne says.

It’s a disturbing new frontier. A child’s photo can be stolen from a website in seconds, their face “scraped” using AI and applied to abusive imagery destined for the dark web. The horrendous images are, Osborne says, “designed to cause as much alarm as possible. As a parent, I’d be terrified.”

And the impact can be catastrophic. One mother of three, who runs student workshops and has been into

schools where this has happened, told me that pupils are consumed by shame, withdraw from family and friends, and in the worst cases become suicidal.

Stephen Gilbert, a data analyst from west London, received an email from the Kido nursery chain last September informing him that photos of his children, aged one and three — as well as their addresses and medical information — had been stolen.

Hackers had posted a gallery of 20 pupils on the dark web and threatened to share up to 8,000 more if the nursery failed to pay a ransom, thought to be about £600,000. Some parents received phone calls, demanding they pressure Kido to pay or their child’s picture would be shared.

As a parent, Gilbert, 49, says, your mind immediately goes to terrible places. “It’s not a place for anyone with good intentions, so when I discovered that there was the possibility of the information being put onto the dark web, that was a heart sinking into the stomach moment for me,” he says. “It was devastating to know that — it’s a shopping list for paedophiles, basically.”

The hackers claimed to have deleted the images after the police got involved but may have already sold the information on to other criminals. Gilbert has no idea whether his children’s photos were posted. The terrifying thing, he adds, is that once images are on the dark web, they’re out there for ever for anyone to find.

Deepfakes showing child abuse are shared in chatrooms, commented on by paedophiles and uploaded to different platforms, where they can be manipulated again by AI and turned into video. “My partner has had to compartmentalise it, because if she thought about it too much she’d go into a deep depression,” he says.

It’s hard to pinpoint just how many nurseries and schools have had images stolen, not least because they are

reputational damage and parental fury. A new study of 251 UK primary and secondary school teachers offers a clue: 85 per cent were aware of criminals using AI to generate deepfake abuse images using pictures of pupils and staff, while 23 per cent said it has already happened to them.

According to the IWF, reports of AI-generated child sexual abuse material more than doubled in 2025, with girls making up 94 per cent of the imagery. There does not seem to be much discrimination between private and state schools.

Alarm over how AI can be used by bad actors has spread since it emerged that users of Elon Musk’s Grok had generated three million sexualised images of women and children in less than two weeks this year, flooding social media with them. (It now claims to have banned the feature.)

In the UK it is illegal to generate, possess or share child sexual abuse material, whether it features real children or those generated by AI. Amendments to the Crime and Policing Act have gone through the Lords to stop AI tools creating child sexual abuse material in the first place and order tech firms to remove images within 48 hours.

Simon Bailey, the National Police Chiefs’ Council lead for child protection for eight years until 2021, tells me: “This has become an epidemic. There is an appetite for the most severe images of child abuse and artificial intelligence is being used to create it at scale. The frightening fact is that you simply cannot differentiate between an AI image and a real one with the naked eye.”

In February pictures of staff at Alderman Peel High School in Wells-next-the-Sea, Norfolk, were stolen from social media and digitally altered using AI before being posted on a website soliciting sex; profiles that

“I hate the fact that this is happening. I hate the fact that we, as parents, even have to think about it

“Teachers feel embarrassed and scared of their families seeing it,” Osborne says. “It’s a complete violation.”

Osborne emphasises that schools aren’t to blame. Technology is moving too fast for them to keep up, she explains. What’s needed, campaigners say, is for the government to fund AI training for teachers and pupils, and for online platforms to be proactive in cracking down on images.

In the meantime, Osborne aims to help schools to stop this crime in its tracks. Open-source AI can be used to blur faces and apply filters to disguise someone’s identity, but in many cases the process can be reversed by criminals with the know-how. Plus, it will have been trained on real human faces, so there’s a risk that the features of an actual child could be used.

Aidos, which she worked on with Bailey, replaces the face of a child, or teacher, with an artificially generated one of the same age, ethnicity and emotion. Crucially, the photo’s source code is encrypted and the metadata deleted, meaning the process can’t be undone and the child is untraceable.

The original picture is never online, instead stored in a server only accessible by the school and so secure that, Osborne says, the ethical hackers she paid to break into it have failed. Plus, you must have an official school email address to access the app, which costs schools £295 a year to protect 100 images of its students and £395 to protect 200 images. There were 150 schools on the waiting list for her app, and since it soft-launched a few weeks ago 50 have been using it.

Schools aren’t completely alone: most contact the police and there are investigations continuing. But officers have struggled to locate the extortion gangs and no arrests have been made.

As far as Osborne knows, no school has yet paid a ransom, which means the deepfakes could well have been distributed. Some children spend hours combing the dark web for deepfake abuse images of themselves, meaning they’re exposed to the worst content imaginable.

Hypervigilance is also a common reaction: “I’ve spoken to young people who have described walking down the street and being looked at by a man for longer than they’re comfortable with,” Bailey says. “Their instant thought is, have you seen pictures of me being raped?”

You may be asking why on earth any parent would agree to their child’s image being used online. “Most parents consented before this became a problem but the risks have changed now,” Osborne says. “Consent needs to be updated. They need to be asked: ‘Can we use your child’s image but protect their face using AI?’”

Not everyone is receptive. “I had a conversation with one head who said, ‘But there’s no threat to us because the parents consented to their children’s images being used,’” Bailey says. “I replied, ‘But did they consent before knowing about this specific risk?’ He stormed off.”

He thinks that if Aidos were in every school, there wouldn’t be a problem. “This is a rare crime that can be completely eradicated and that technology — using AI for good — can absolutely end, full stop.”

But whether they use the app or not, the most important thing, he and Osborne agree, is for schools to make a plan. As Osborne puts it: “You can’t bury your head in the sand any longer. This is happening.”