

PLAIN SIGHT

THE 2026 REPORT ON AI, SCHOOL PHOTOGRAPHY AND THE DUTY TO PROTECT



aidos

All images used in this document have been protected by Aidos

Foreword



Carole Osborne
Founder and CEO at Aidos

Every school day, across the UK, photographs of children are shared online across their websites, newsletters, and social media channels. Shared with warmth and pride to celebrate everything from a day in the classroom, sports day through to marking a prize-giving – showing the world what school life looks like. School photography is an important part of how schools tell their story, build their culture and communicate with the families they serve.

But the world those images are being shared into has changed. Faster than most of us have had time to absorb, and in ways that demand a response from every adult with a duty of care to the children in those photographs.

I set up Aidos, a safeguarding technology that protects children’s identities, after witnessing first-hand the distress caused when a school I was working with told me about children’s images being stolen, turned into child sexual abuse material (CSAM), and used to demand a ransom. That experience became my founding purpose for Aidos: to ensure that schools would never have to face that situation without a practical, effective solution available to them.

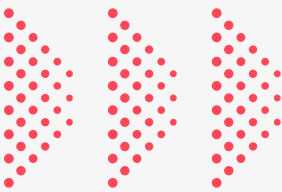
That experience was not an isolated one. The more our team spoke with schools, safeguarding leads and education professionals across the UK, the clearer it became that this threat was far more widespread than the founding incident had suggested. School after school described a growing sense of unease – an awareness that the images they were sharing in good faith were becoming a source of vulnerability they had no solution for. The picture that emerged from those conversations was of a problem not in its early stages, but already well advanced and accelerating.

What I have since also come to understand is the full weight of what this means for the children whose images are misused. Deepfake sexual images can be devastating. Survivors often describe feeling violated, humiliated and powerless. Unlike other forms of online abuse, deepfakes feel intensely personal, because the image looks exactly like you.

For children and young people, this can be especially difficult to process, particularly where images are shared within peer groups. Victims can face severe bullying, public ridicule and harassment, and the trauma is often amplified each time the material is viewed or shared. Many children wrongly blame themselves, fearing they will be judged or disbelieved by their family and peers, and the psychological impact can be truly profound resulting in lasting mental health challenges. These are not abstract consequences, they are the reality for children whose images have been stolen from the websites of schools that shared them in good faith.

The scale of this crime’s acceleration became undeniable earlier this year, when the *Internet Watch Foundation*, the *National Crime Agency* and the *Early Warning Working Group* issued a formal warning to schools following a confirmed blackmail attempt against a UK secondary school – in which criminals scraped photographs of pupils from the school’s website, used AI to generate child sexual abuse material, and threatened to publish the images unless payment was made. The IWF confirmed the school was not the only institution to have been targeted in this way, something we were already acutely aware of.

Continued...



As adults – as school leaders, governors, parents, carers, guardians, professionals and policymakers – we have a duty of care to the children whose images we use in school communications. And that duty of care must reflect the reality of what AI makes possible.

The findings of this report point to a clear set of actions for school leaders, and I would urge every headteacher reading this to consider five things:

Key takeaways for school leaders:

- 1. Don't stop showcasing your school culture, it is an important part of telling your school's story.
- 2. Do acknowledge that the risk to children has changed. The threat posed by AI to children's images is fundamentally different to anything schools have faced before.
- 3. Make sure consent is genuinely informed and reflects today's AI landscape. Consent forms were designed way before criminals began to create CSAM to extort schools, and do not address the risks that now exist.
- 4. Risk assess every image before it is published. The question is no longer just 'do we have permission?' But 'could this image be used to harm this child?'
- 5. Anonymise children's identities in publicly accessible images. This is the single most effective step a school can take to prevent misuse and reduce the risk of harm.

- 6. Should you choose to take none of the preventative actions above, be familiar with, and ready to, implement our plan, on page 5, outlining how to respond should your school be directly targeted.

This is not a tomorrow problem and the following findings in this report makes that impossible to ignore. I hope they prompt every school leader who reads it to act – not next term, but now.

Carole Osborne
Founder and CEO at Aidos

EXECUTIVE SUMMARY

01

01

Executive summary

The threat is
real documented
and growing

49%

of headteachers say
their school has
experienced an incident
involving pupil image
misuse, manipulation
or an extortion attempt.

For the very first time, our national research carried among UK primary and secondary school headteachers, gives us a direct picture of how image exploitation in the age of AI is already affecting UK schools – not as a projected risk, but as a present reality.

While AI-driven image exploitation is an emerging safeguarding concern, our findings show that image misuse is already a significant issue for many schools. Almost one in two headteachers (49%) say their school has experienced an incident involving pupil image misuse, manipulation or an extortion attempt. Nearly half have personal concerns about their school’s published images, and almost half have received a direct complaint from a parent about image misuse. This is not a future safeguarding challenge, it is today’s.

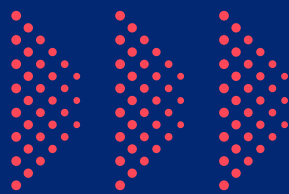
What makes these findings so significant is the context in which they also sit. Latest data from the *Internet Watch Foundation* published earlier this year, confirmed that more than 8,000 AI-generated images and videos of realistic child sexual abuse in 2025 alone were identified, a 14 per cent rise on the previous year.



METHODOLOGY

We commissioned market research consultancy Censuswide, to survey a UK-wide representative sample of 500 headteachers across primary and secondary schools. The fieldwork was carried out between the 5th and 11th June 2026.

The research explores how headteachers across the UK think, feel and respond when it comes to sharing photographs of their pupils online, and how the rapid emergence of AI-driven image exploitation is reshaping the risks associated with that practice. It examines the gap between schools’ existing safeguarding frameworks and the realities of the AI threat landscape, and investigates the degree to which headteachers feel equipped – in terms of policy, confidence and practical tools – to protect the children in their care from image-based misuse and extortion. It also considers what schools are prepared to do in response to the growing threat, and what support, guidance and solutions would help them continue to share school life publicly and with confidence, without compromising the safety of the children whose images they publish.



01 Continued...

What headteachers told us

93%

of headteachers say they are aware that AI tools are being used by criminals to generate deepfake imagery from school websites and social media.

- Almost one in two headteachers (**49%**) say their school has experienced an incident in which pupil images were misused, manipulated or used as part of an extortion or blackmail attempt.
- A further **54%** say they have personal concerns that their school’s published images could be vulnerable, and 45% say their school has received a direct complaint from a parent or carer about the misuse or potential misuse of a pupil’s image shared online.
- Awareness of the threat is near-universal – **93%** of headteachers say they are aware that AI tools are being used by criminals to generate deepfake imagery from school websites and social media. Yet fewer than half (**43%**) would feel very confident knowing exactly what steps to take if their school received a ransom demand involving manipulated pupil images tomorrow.
- The risk is compounded by how long pupil images remain online. Just **34%** of schools update their published photographs annually. More than half (**52%**) do so only every two to three years, leaving many schools with years of publicly available pupil photography that could be exploited if left unprotected.
- The research also reveals a significant gap in consent and policy frameworks. While **85%** of schools carry out a risk assessment on the online publication of pupil images, only **43%** say their consent process fully addresses the specific risk of AI exploitation or deepfake generation, and **16%** have no AI or deepfake-specific policy at all.

What schools are considering doing about it

- More than half of headteachers (**54%**) say they are already actively considering removing identifiable photographs of pupils from their school’s website and social media, a step the NCA and IWF have themselves recommended.
- But **94%** say school photographs are important to their school’s culture, identity and reputation. The tension between protection and celebration is real and many schools are still looking for practical solutions
- Using a safeguarding platform such as Aidos, could be one of the solutions. By permanently replacing every child’s face in a school photograph with a realistic, synthetic substitute before the image is shared – irreversibly, with no recoverable original, not sourced from any real person or existing image database, Aidos means schools can keep sharing everything they have always shared. The difference is that those images are no longer capable of revealing the identities of the children within them, fundamentally changing the risk they present if shared publicly.
- Schools should not have to choose between celebrating their children and protecting them. The risk to children’s identities online is growing rapidly, and safeguarding approaches must reflect that. The technology to close this gap exists today.
- This report is our call on every school leader, safeguarding professional and policymaker to act, before a case hits closer to home.

Our call to action

KEY FINDINGS

02

02

Key findings



49%

of headteachers say their school has experienced pupil image misuse, manipulation or an extortion attempt

54%

say they have personal concerns that their school's published images are vulnerable to AI misuse

45%

say their school has received a direct complaint from a parent about the misuse of a pupil's image

93%

of headteachers are aware that AI criminals are targeting school photographs

43%

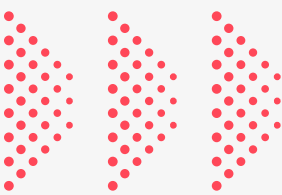
Fewer than half feel very confident knowing what to do if their school received a ransom demand tomorrow

52%

of schools update their published pupil photographs only every two to three years

02

Continued...



43%

Less than half say their consent process fully addresses the risk of AI exploitation of school photography



16%

One in six schools has no AI or deepfake-specific policy in place at all

54%

are already actively considering removing identifiable photographs of pupils from their school's website and social media

94%

Yet, the majority say school photography is important to their school's culture, identity and reputation



EXPERT VOICES



The findings of this report are not numbers in isolation, they represent the experiences of real school leaders, facing a threat that existing safeguarding frameworks were never designed to address. Two of the most authoritative voices in child protection and safeguarding in the UK, as well as a Director of Safeguarding for Trust representing a collection of secondary schools, put the findings in context.

03

03

Expert voices

“

I have spent 35 years in policing, and I have never seen a threat to children escalate as fast as this one. The online sexual abuse of children is reaching pandemic levels, and the emergence of AI is fuelling the demand in ways that existing safeguarding frameworks were simply never designed to address. These findings show that school leaders know this is happening – and that fewer than half do not yet feel equipped to respond to it. That gap needs to close.

I would urge every headteacher in the country to ask themselves one question: if a parent came to me tomorrow and asked what I have in place to protect their child's image, what would my answer be? If the answer is not a confident one, it is time to act.

”

Simon Bailey CBE, QPM, DL

Former National Policing Lead for Child Protection and Advisor, Aidos

03

Expert voices

“

As a Director of Safeguarding, my job is to anticipate risk, not just respond to it. We haven't seen our schools targeted, and I hope we never will be. But hope is not a safeguarding strategy, and neither is waiting for a case closer to home before we act. What is clear is that AI has made this risk real, fast-moving, and increasingly hard to ignore.

Do we as schools have all the answers? No. But we know enough to take it seriously and keep asking what more we can do. Across our trust, we run regular safeguarding quality assurance to keep our policies and practice under constant review, because the images our schools share every day are being used in ways nobody anticipated when those consent forms were first written. That has changed, and our response has to change with it.

”

**Charlie O'Sullivan**

Director of Safeguarding, The Collegiate Trust

03

Expert voices

“

In my 30-year career working with victims and survivors of sexual abuse, I have learned that the psychological harm caused by sexual exploitation is real, regardless of the form that exploitation takes. AI-generated child sexual abuse material may be artificial, but the fear, shame and loss of control experienced by children and young people are not.

”

Nina Vaaranen-Valkonen

Executive Director, Protect Children and Member
of the Safeguarding Advisory Group, Interpol CAC

WHAT TO DO IF YOUR SCHOOL IS TARGETED? (OUR ADVICE)

04

04

What to do if your school is targeted? (Our advice)

While preventative safeguarding is always preferable, schools may find themselves dealing with concerns about image misuse, including attempts at extortion or blackmail. In these situations, how a school responds matters as much as the incident itself.

1. Immediate steps

- Do not engage with the individual making contact
- Preserve evidence, including messages, email URLs and timestamps
- Inform the Designated Safeguarding Lead (DSL) immediately
- Follow existing safeguarding and data protection procedures
- Call the Police (via 101 or 999 if there is immediate risk)
- Schools should treat image-based blackmail as a serious safeguarding concern, regardless of whether the images were altered or entirely fabricated

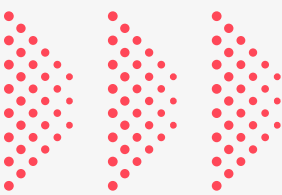


2. External support

- Incidents involving image misuse or blackmail should be reported through established channels
- UK Safer Internet Centre – for advice on image misuse and takedown support
- Local authority safeguarding teams, where appropriate
- Schools should also follow internal incident reporting and record-keeping procedures in line with data protection requirements



04 Continued...



3. Communicating with parents and carers



Clear, measured communication is essential. When speaking to parents, try to do so face to face. Be factual and calm, avoid speculation or technical detail, reassure families that safeguarding procedures are being followed, and emphasise that misuse can occur without any fault on the part of the school or child.

Key messages to convey:

- The school is aware of the concern
- Appropriate authorities have been informed
- Support is in place for affected pupils
- Preventative steps are being reviewed or strengthened

Transparency, without alarm, helps maintain trust.

4. Communicating with pupils

Children should never be made to feel responsible for image misuse resulting from criminals stealing images from school materials. When speaking with pupils:

- Use age-appropriate language
- Reassure them that they have done nothing wrong
- Avoid showing or describing harmful content
- Emphasise that adults are handling the situation

Schools may also wish to involve pastoral staff or counsellors, monitor wellbeing over time and provide reassurance rather than repeated questioning. The focus should always be on emotional safety and stability, not investigation.



For guidance on image takedown support visit:
www.saferinternet.org.uk

SAFEGUARDING & IMAGE ANONYMISATION

05

05

Safeguarding & image anonymisation

12 questions every school should ask

Protecting children’s identities online is no longer optional. But not all image anonymisation solutions are built the same way. Before selecting a provider, schools, trusts and safeguarding teams should ask the following questions — and expect documented answers rather than marketing claims.



01

Will our images be used to train AI models?

- What to look out for
“No” to training on your images. Guaranteed in the contract.

02

Where are children’s images processed?

- What to look out for
Transparent answers and documented data-processing arrangements.

03

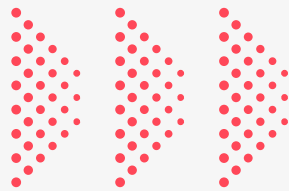
Who can access our images?

- What to look out for
Strict access controls and minimal third-party involvement.

04

Do schools retain ownership of their images?

- What to look out for
Full ownership remains with the school.



05 Continued...

05

What information is changed within the image?

- 👁️ **What to look out for**
Protection of identity while preserving the authenticity of the image.

06

Can we continue using our images for marketing?

- 👁️ **What to look out for**
Images that remain authentic and suitable for all school communications.

07

How consistent are the results?

- 👁️ **What to look out for**
Reliable, predictable outputs at scale — not just on one image.

08

How easy is your solution to implement?

- 👁️ **What to look out for**
A straightforward implementation with clear onboarding and ongoing

09

What security standards do you follow?

- 👁️ **What to look out for**
Encryption in transit and at rest, documented retention, secure deletion.

10

Was this solution built specifically for schools?

- 👁️ **What to look out for**
A provider with deep understanding of education and safeguarding.

11

Can you provide GDPR documentation?

- 👁️ **What to look out for**
Clear, documented evidence — ICO registration, a DPA, a stated lawful basis.

12

Why should we trust your solution?

- 👁️ **What to look out for**
Technical excellence plus recognised safeguarding expertise and transparency.



Every question above comes with the specific things to ask a supplier and what a good answer sounds like. Download the full guide at aidosprotects.com.



Aidos is the UK's first and only AI safeguarding platform built solely to protect children's identities in school photography. It makes pupils and teachers in school photographs permanently unidentifiable before they are shared online — protecting children from deepfake exploitation, sextortion and AI-generated image abuse without disrupting the way schools communicate and celebrate their communities. Founded by Carole Osborne — a former branding agency owner, entrepreneur and mother of two, the platform is built on a simple belief: that schools should not have to choose between celebrating their children and protecting them.

It was during her time running a branding agency, that she first encountered the consequences of school image vulnerability — witnessing the distress caused when a school's pupil images were compromised, an experience that became the founding purpose of Aidos.

Aidos is also advised by a team of leaders in safeguarding, technology and education, and is registered in England and Wales.

aidosprotects.com | aidos@aidosprotects.com