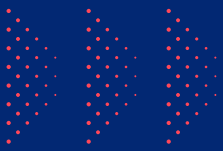
PROTECTING *YOUR CHILDREN'S IMAGES* IN THE AGE OF AI



A short briefing for schools, trusts, and governors

aidos

CONTENTS

01

WHY THIS BRIEFING MATTERS

Recent advances in AI have seen images taken from school websites turned into child sex abuse material. This briefing outlines how schools can respond to this existential threat.

Schools routinely publish pupil images:

- On websites
- In prospectuses
- On social media
- In newsletters and marketing materials

This has always been done responsibly, with consent and safeguarding considerations carefully in place.

However, rapid advances in artificial intelligence (AI) have changed how images can be used once they are public — creating safeguarding risks that did not previously exist.

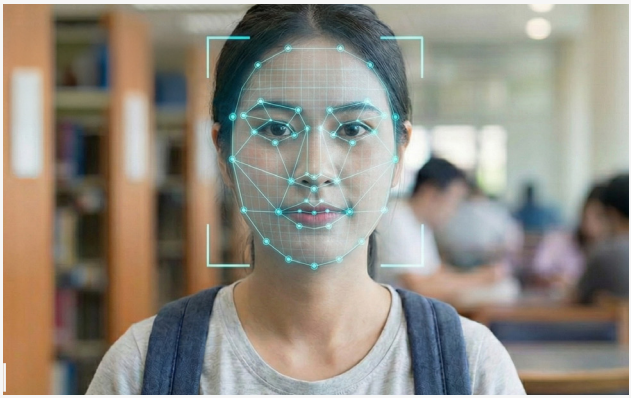
This briefing sets out what has changed, why it matters, and how schools are beginning to respond.

02

WHAT HAS CHANGED?

AI tools can now extract an image of a child and recreate that to produce child sex abuse material. Crucially, this technology is now being used at scale.

2025 was the worst year on record for online child sexual abuse material



With increasing coverage in the press, law enforcement agencies and child protection organisations have reported a rapid rise in AI-generated child sexual abuse material (CSAM).

An AI generated, photorealistic images of a student.

New data released by the Internet Watch Foundation shows 2025 was the worst year on record for online child sexual abuse material found by its analysts, with increasing levels of photo-realistic AI material contributing to the "dangerous" levels.

This does not require hacking, specialist knowledge, or access to school systems.

Any image published publicly — even years ago — can be misused.

Importantly:

- Schools may never be alerted or alternatively blackmailed if misuse occurs
- Harm can happen long after an image is published
- Good intent and consent do not prevent technological misuse in harmful or inappropriate ways

03

WHY CONSENT ALONE IS NO LONGER ENOUGH

Parental consent is a legal requirement under GDPR and remains essential and non-negotiable. However, consent was designed for a pre-AI environment, and parents are not aware of the AI risk and the exponential increase in the number of images that are being created.

Consent:

- Allows publication
- Does not control how images are reused
- Does not prevent data extraction
- Does not remove safeguarding responsibility

In safeguarding terms, this means:

Consent enables use — it does not remove risk.

As with other digital risks, schools have a duty of care to pupils and are expected to take reasonable, proportionate preventative steps wherever foreseeable harm exists.

SAFEGUARDING RESPONSIBILITY HASN'T CHANGED, EXPOSURE HAS

Schools already have a duty to:

- Act in pupils' best interests
- Anticipate and reduce foreseeable harm
- Protect dignity, identity, and welfare
- Maintain trust with parents and communities

Bodies such as Ofsted and the Department for Education increasingly focus on culture, awareness, and prevention, not just response.

As awareness of AI-related image misuse grows, schools may reasonably be asked:

"What steps were taken to reduce this risk?"

05

WHY THIS IS A SAFEGUARDING ISSUE, NOT A TECHNICAL ONE

This is not about:

- Becoming AI experts
- Teaching advanced technology
- Changing how schools communicate

It is about:

- Protecting your children
- Reducing reputational risk
- Acting proportionately and preventatively
- Proactively protecting families from the trauma caused by the exploitation of children's images

WHAT PREVENTATIVE SAFEGUARDING LOOKS LIKE

When new risks have emerged in the past, schools have introduced:

- Filtering and monitoring
- Access controls
- Clear policies
- Proportionate safeguards

In the AI era, image protection is becoming the equivalent control.

Preventative approaches:

- Do not change day-to-day workflows
- Do not remove pupil images
- Do not affect school storytelling or marketing
- Quietly reduce exposure at source

This is about making image use safer by default.

07

AN EMERGING STANDARD, NOT AN EXTREME MEASURE

Protecting pupil images from AI misuse is increasingly seen as:

- Sensible
- Proportionate
- Forward-looking
- Responsible

Much like earlier digital safeguards, it represents the next evolution of good safeguarding practice, rather than a reaction to a specific incident.

Original portrait image
of a student

Aidos protected version
of the same student image

08

HOW SCHOOLS ARE RESPONDING IN PRACTICE

As awareness of AI-related image risk increases, schools are beginning to look for preventative safeguards that are:

- Proportionate
- Low-impact on existing workflows
- Aligned with safeguarding responsibilities
- Reassuring to parents and governors

One emerging approach is the use of image protection technology to anonymise pupils faces before they are published online.

This allows schools to:

- Continue celebrating pupil life and achievement
- Maintain consistent communications and marketing
- Reduce exposure at source rather than reacting after harm
- Demonstrate a proactive safeguarding mindset

Aidos was developed specifically for this purpose — to help schools protect pupil identities in an AI-enabled world without changing how schools work or communicate. It operates in the background, embedding a layer of safeguarding protection into images before they are published, protecting student identities and schools from harm.

09

IF A SCHOOL BELIEVES PUPIL IMAGES HAVE BEEN MISUSED

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

If a school becomes aware of suspected image misuse or blackmail:

- Do not engage with the individual making contact
- Preserve evidence, including messages, emails, 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, including:

- 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.

3. Communicating with parents and carers

Clear, measured communication is essential.

When speaking to parents try and do it face to face:

- Be factual and calm
- Avoid speculation or technical detail
- Reassure families that safeguarding procedures are being followed
- Emphasise that misuse can occur without any fault on the part of the school or child

Key messages may include:

- 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. Supporting and speaking with pupils

Children should never be made to feel responsible for image misuse resulting from criminals stealing images from school online 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 wish to:

- Involve pastoral staff or counsellors
- Monitor wellbeing over time
- Provide reassurance rather than repeated questioning

The focus should always be on emotional safety and stability, not investigation.

10

FINAL REFLECTION

Image misuse involving children is distressing, particularly when it emerges unexpectedly and without warning.

However, schools are not expected to predict every misuse — only to respond thoughtfully, proportionately, and in pupils' best interests.

Safeguarding in the AI era is about combining:

- Clear procedures
- Calm communication
- External support
- And preventative measures like Aidos that reduce future exposure

By doing so, schools can protect pupils, support families, and maintain trust — even in challenging circumstances.

The real identities of all children featured in this booklet have been protected using Aidos technology.

This booklet was produced by the team behind Aidos.

To learn more about our work protecting children's identities online, visit:
www.aidosprotects.com

aidos