ATT Inclusion & Safeguarding

Academy Transformation Trust

ATT Guidance on Protecting Images

from AI Manipulation, Misuse and Blackmail

Contents

Purpose

This guidance supports ATT academies to continue celebrating children and young people, showcasing academy life and strengthening community connection, while reducing emerging risks linked to AI-enabled image manipulation, misuse and blackmail.

ATT Position

Images are an important part of how ATT academies communicate, celebrate and build community. This should continue. ATT's approach is to retain the benefits of visibility, celebration and connection while ensuring that practice reflects the realities of the evolving digital landscape. The emphasis is on safe, informed use, not restriction for its own sake. Our response should be proportionate, evidence-based and focused on helping families make informed decisions, while ensuring the Trust continues to meet its safeguarding and data protection responsibilities.

Understanding the Risk

AI manipulation and misuse

Images of children, young people and adults shared on publicly accessible platforms, including academy websites and social media, can be downloaded, copied or scraped and manipulated using AI tools. This represents a significant shift in safeguarding risk compared with previous years and should now be factored into decision-making about image use.

What are Deepfakes?

Deepfakes are images, videos or audio that have been digitally altered using artificial intelligence to make them appear real. In a school context, this could include a genuine photograph being changed (e.g. a pupil's face placed onto another image) or a completely fabricated image appearing authentic. While deepfakes may sometimes be used in attempts to blackmail or coerce, they do not need to involve these elements to cause harm. Manipulated images can still lead to humiliation, distress and reputational damage for children, staff or the wider school community.

What Is Sextortion?

Sextortion is a type of blackmail where an individual threatens to share sexual images or content—either real or manipulated—unless certain demands are met. In the context of AI image misuse, this may involve a perpetrator claiming to have created or obtained altered images of a child or adult and using this to seek money, information, or other actions from the school, family, or individual. Contact may be made directly with schools, families, or individuals via email, social media, or messaging platforms. Importantly, in some cases no images actually exist, and the claim itself is used to create pressure or distress.

Identification through context

Even where names are not published, children can still be identifiable through contextual or repeated information. Risk can be increased by:

- school uniforms, logos or signage
- locations, entrances or local landmarks

- event details, timings or routines that narrow down place and time
- repeated appearances across posts or over time
- community familiarity or links with other publicly available information

Heightened vulnerability
Some children or adults face greater risk due to their individual circumstances, including domestic abuse situations, care status, court orders, family estrangement or other active safeguarding concerns. Even a single publication decision can have serious consequences.

Risks to staff and to the academy
Misuse, manipulation or blackmail may also affect staff. This is both a safeguarding, staff wellbeing, reputational and data protection issue. Academies should therefore consider image use within wider incident response, business continuity and leadership escalation arrangements.

Statutory and Organisational Responsibilities

Safeguarding
Academies must have regard to Keeping Children Safe in Education and should ensure that online risks and emerging technologies are reflected in safeguarding practice, staff awareness and local decision-making.

Data protection
Where students can be identified, images are personal data. Academies must process images lawfully, fairly and securely, be clear about how images are used, and ensure appropriate data protection arrangements are in place.

Data security and breaches
Academies must have processes to respond to data breaches, including where images are misused, altered or accessed without permission.

Consent and safeguarding responsibility
Parental consent remains an important part of decision-making. However, consent alone does not remove the Trust's safeguarding or data protection responsibilities. The key question is not simply whether consent has been obtained, but whether the proposed use remains necessary, proportionate and safe in the current safeguarding environment, and whether families have been given enough information to make consent genuinely informed.

What Academies Should Put in Place

(See also Appendix 1, Immediate Actions, and Appendix 2, Academy Checklist)

A clear and considered approach to image use
Academies should be clear about the purpose of using images, and whether it is necessary for that purpose, and consider whether a safer alternative could achieve the same aim. Academies should avoid using 'high risk' content. High-risk content or images include close-up or portrait-style images of individuals, images

showing academy logos or signage alongside close up portrait style images, images that could narrow down a child's location or routine or images of children who have active safeguarding concerns.

Consent and communication (see also appendix 3)
Academies should review and update consent for photographs and video at least annually. Parents and carers should understand how images will be used, where they may appear, including on websites and social media, and the potential risks associated with online sharing. Academies should provide opportunities for questions and should make clear that consent can be reviewed or withdrawn. Families should receive sufficient information to make an informed decision.

Involvement of students in image decisions
Academies should involve students in decisions about the use of their image in a way that reflects their age, understanding and maturity. Students, particularly those in Key Stage 3 and above, should be given clear, age-appropriate explanations of how their images may be used. If a student expresses discomfort, academies should ordinarily avoid using the image. Where parental consent and student views differ, academies should take a proportionate safeguarding-led decision, giving appropriate weight to the student's voice.

Selecting safer images and avoiding 'high risk' imagery
Academies should consider using wider shots or group images instead of close-up portraits, avoiding clear front-facing images where possible, and using angles that make images less easily reused or manipulated. The aim is not to avoid imagery, but to reduce identifiability where appropriate.

Avoiding unnecessary identification
Academies should avoid routinely publishing full names alongside public images and should consider carefully whether contextual detail such as event information, location, class group or routine is necessary. Published content should not unintentionally identify or place anyone at greater risk.

Removing metadata and improving technical image hygiene
Academies should remove image metadata, such as location and timestamp information, before publishing and should ensure this forms part of standard image upload processes (see Appendix 5). They should also apply appropriate privacy settings to websites and social media accounts and involve IT colleagues in the technical implementation of these steps.

Reviewing publication platforms
Academies should regularly review what content is publicly accessible, whether all content needs to be fully open, and whether some material could be shared instead through more controlled environments such as secure parent apps or portals.

Auditing images
Academies should review website and social media imagery regularly, for example termly, remove images that are outdated or no longer appropriate, and ensure images remain aligned to current consent arrangements. If images are used by Central Trust and consent to use those images is withdrawn, the Principal should notify the marketing department.

Staff awareness and oversight
Academies should include safer image use within safeguarding and online safety training and should ensure staff understand what safer image practice looks like, who approves publication, and how to escalate concerns. There should be clear leadership oversight of externally shared content.

Social Media Image Sharing

Managing public visibility
Academies should assume that all images posted on public-facing platforms can be downloaded, screenshot or reshared. They should regularly review whether content needs to be fully public and consider limiting visibility where risk is higher or where a more controlled platform could be used.

Facebook and similar platforms
Where academies use Facebook or equivalent platforms, they should review page settings regularly to manage who can view, comment on or share content. Consideration should be given to restricting public commenting where appropriate, alongside active monitoring of interactions. High-resolution, close-up images of individual students should be avoided, particularly where combined with identifying details such as full names, class groups or precise locations.

Sharing practices
Academies should take a measured approach to posting, avoiding large volumes of images in a single post and using caution when tagging individuals. Clear expectations should be in place to ensure that external organisations, photographers or partner agencies do not re-share academy images without agreement.

Ongoing monitoring
Academies should routinely monitor social media platforms for misuse, inappropriate comments or unauthorised sharing. Where concerns arise, content should be removed promptly and escalated in line with safeguarding procedures.

Key Questions for Leaders Before Publishing Images

- Is this image necessary for the purpose we are trying to achieve, or could we communicate the same message another way?
- Could a student be identified from this image alone, or in combination with other information available online?
- Does the student have any active safeguarding considerations that heighten the risk?
- Have parents and carers been informed about evolving risks, including AI image manipulation, so that consent is genuinely informed?
- Would a less identifiable image serve the same purpose?
- Does the image include school signage, identifiable locations, event detail, timings or routines that increase risk?
- Has metadata been removed and have platform privacy settings been checked?

Incident Response

(See also Appendix 3, Incident Response Step by Step)

Immediate actions

If image misuse, manipulation or blackmail is identified or suspected, academies should preserve evidence, avoid deleting or forwarding images unnecessarily, remove original images from public platforms where appropriate, inform the DSL and senior leaders, and record the concern in line with safeguarding procedures on CPOMS where appropriate or as a separate log if it is unclear which students are involved.

Police involvement

Where there is blackmail, coercion or manipulated imagery that that is illegal, academies should contact the police immediately and should not engage with or respond to demands. If there is immediate risk of harm, this must be treated as an emergency and 999 should be called. Illegal imagery is likely to meet the threshold for police

Illegal Imagery

An image is likely to be illegal where it depicts, or appears to depict, sexual imagery of a child, is being distributed, requested, or stored unlawfully, or is used for coercion or blackmail. This includes AI-generated or manipulated images (e.g. deepfakes) and may also apply to images involving staff if these thresholds are met, even where blackmail is not present. Staff should not view such images, particularly where children are involved, and should not attempt to determine legality or manage incidents alone. Any concern must be reported immediately to the DSL, who will liaise with external agencies, including the police.

Preventing further sharing

Academies should report harmful content to hosting platforms for removal, support access to appropriate reporting tools such as Report Remove for under-18s, and work with police and relevant agencies where further upload prevention or wider disruption activity is required.

Supporting those affected

Academies should prioritise the safety and wellbeing of the child or young person, communicate with parents and carers sensitively, and provide appropriate safeguarding and pastoral support. Staff affected by distressing image abuse incidents should also be offered support.

Leadership escalation and business continuity

Academies should activate relevant business continuity or incident management arrangements and notify appropriate Trust leaders without delay, including the CEO and the Director of Safeguarding and Inclusion through established escalation routes.

Responding Where Staff are Affected

Misuse, manipulation or blackmail involving staff

Where misuse, manipulation or blackmail involves staff, academies should respond promptly and in line with safeguarding and staff well-being responsibilities. Where there is blackmail, coercion or credible threat, academies should support reporting to the police without delay.

Immediate actions
Staff should not engage with, respond to, or comply with any demands. The concern should be reported immediately to the Principal and DSL and recorded in line with academy procedures. Evidence should be preserved, for example screenshots, URLs or usernames, without further sharing.

Reporting and removal
Academies should support staff to report content to the relevant platform using reporting routes for harassment, impersonation or image-based abuse. Academies should continue to pursue removal requests, recognising this may take time where content has been shared more widely. Professionals Online Safety Helpline | SWGfL is a helpful source of support in these cases.

Supporting staff
Academies should provide appropriate pastoral and professional support, including access to supervision or employee support where available. Senior leaders should maintain regular, supportive contact and consider any reasonable adjustments where needed.

Recording and Governance

- All incidents must be recorded fully on CPOMS or the academy's designated safeguarding information system
- A summary of the incident and the response taken must be shared with the Trust's National Attendance, Safeguarding and Inclusion Lead
- The Principal must ensure that the Designated Safeguarding Lead is fully supported throughout the response
- Serious incidents may require notification to Ofsted and/or the Regional Schools Director under the Trust's statutory reporting obligations
- Trust safeguarding leadership will review whether the incident has implications for Trust-wide guidance on image use or online communications

Frequently Asked Questions

Are we being asked to remove all images? No. This guidance asks academies to review current practice and adapt accordingly. The Trust values the use of images to celebrate students and promote academy life. The aim is to ensure that practice is intentional, proportionate and safe. Academies should consider checking websites for any existing 'high risk' images they may have added and removing these if added locally (for example local academy photo galleries).

If parents have consented, is that sufficient? Consent remains important, but it does not remove our safeguarding responsibility. Our role is to ensure that consent is genuinely informed, not simply recorded. consent communications should now include clear information about AI-related risks so that families can make genuinely informed decisions. Consent should be updated at least annually.

Should students be asked for their views? Yes, where appropriate. Students particularly those in Key Stage 3 and above, should be given clear, age-appropriate explanations of how their images may be used. in a

way that reflects their age, understanding and maturity, and academies should ordinarily avoid using an image if a student expresses discomfort.

Can we still use social media? Yes. Social media continues to be a valuable way to share good news and promote our academies. The guidance asks that we are thoughtful about the imagery we use, preferring activity-based and group shots over close-up identifiable images of individual students.

What is high-risk content? High-risk content or images include close-up or portrait-style images of individual students, images showing school logos or signage alongside close up portrait style images, images that could narrow down a child's location or routine or images of students who have active safeguarding concerns.

Appendix 1:

Academy Checklist

Leadership and oversight

☐ There is a clear local approach to using images which aligns with ATT guidance.

☐ A senior leader, DSL, communications lead and IT contact know their respective roles in safer image use.

☐ Image use is considered as both a safeguarding issue and a data protection issue.

Consent and communication

☐ Photo and video parental consent is reviewed and updated at least annually.

☐ Parents and carers are given clear information about how images may be used and the risks of online sharing.

☐ Students are given clear, age-appropriate explanations of how their images may be used. If a student expresses discomfort, use of the image is avoided.

☐ Processes are in place for questions, changes or withdrawal of consent.

Safer image selection

☐ Images are selected carefully with safeguarding in mind, with wider shots or less identifiable images used where appropriate.

☐ Full names are not routinely published alongside publicly accessible student images.

☐ Posts do not include unnecessary contextual details that increase identifiability or risk.

Technical controls

☐ Metadata is removed from images before publication.

☐ Public-facing images are proportionate in quality and do not unnecessarily increase risk.

☐ Privacy and sharing settings on websites and social media are reviewed regularly.

Social media

☐ The academy assumes that public posts can be downloaded, screenshot or reshared.

☐ Facebook and other social media page settings are reviewed regularly.

☐ Commenting, tagging and resharing are monitored and managed appropriately.

☐ External partners do not re-share academy images without agreement.

Website review

☐ Website and social media imagery is reviewed regularly, for example termly.

☐ Out-of-date images, 'high risk' content or images no longer aligned to consent are considered for removal.

☐ Any concerns about image use are discussed through safeguarding and leadership routes.

Incident response

☐ Staff know what to do if an image is misused, manipulated or used in a threat.

☐ Evidence would be preserved and escalated immediately to the DSL and senior leaders.

☐ Serious incidents are escalated through Trust and business continuity routes where required.

Appendix 2:

Incident Response Step by Step

The following steps should be followed when a report is received regarding the misuse of a student's image. The DSL leads the response throughout.

IMPORTANT: If a student is in immediate danger

If at any point you believe a student is at risk of immediate or serious harm, call 999 immediately. Do not wait to follow internal procedures before contacting the police where there is immediate risk to a child.

Step 1: Receive and Record the Report

- Record the date, time and source of the report
- Record the exact nature of the concern, including what was alleged, what platform or medium was involved, and whether any content has been viewed
- Do not attempt to view, download or share suspected illegal content
- Secure all communications relating to the incident, including messages received by the school
- Log the incident on CPOMS or your academy's safeguarding recording system immediately

Step 2: Inform Trust Safeguarding Leadership

- The DSL must contact the Trust's National Attendance, Safeguarding and Inclusion Lead immediately
- The Trust's CEO should be informed if the incident involves a direct threat to the school or if media contact appears likely
- Do not manage the incident in isolation; Trust leadership must be involved from the outset

Step 3: Assess Risk to the Student

- Identify the student or students who may be affected
- Establish whether the student is currently aware of the situation
- Assess whether the student is distressed or at risk of self-harm
- Consider whether any other students are affected
- Do not question the student in detail at this stage; focus on immediate welfare
- Ensure the student is not left unsupported or isolated

Step 4: Contact Police

- Contact the police at the earliest opportunity, and before engaging with any demands
- Call 101 to report the incident, or 999 if there is immediate risk to a child
- Provide the police with all communications and information relating to the incident
- Do not pay any demand, respond to threats, or contact the alleged perpetrator without police guidance
- Preserve all evidence: do not delete messages, emails, or any contact received

The police may direct you to the National Crime Agency (NCA) or to specialist units. Follow their guidance regarding next steps.

Step 5: Make a Referral to Children's Social Care if Required

- Where there is reasonable cause to believe a student is suffering or at risk of suffering significant harm, a referral to the local authority children's social care must be made
- This referral should be made by the DSL in accordance with the academy's safeguarding procedures
- The referral should be logged on CPOMS and documented with time and outcome

Step 6: Report to the Internet Watch Foundation (IWF) and other appropriate reporting channels depending on who is affected

- If AI-generated or other abusive imagery of a student is identified online, report it to the Internet Watch Foundation at Report online child sexual abuse imagery or 'child pornography'
- The IWF has the power to work with online platforms to have content removed
- Reporting to the IWF does not replace police reporting; both should happen
- Report to other reporting channels as appropriate. For example the NSPCC/Childline 'Report/Remove' tool is able to have images taken down from the internet to prevent further sharing. Refer to the list in appendix 5 for other reporting routes.

Step 7: Contact the Platform or Hosting Site

- If manipulated imagery or blackmail content appears on a specific platform (social media, messaging app or website), submit a report to that platform's trust and safety team using their official reporting tools
- Provide as much detail as possible including the URL or account involved
- Platform removal may take time; this step is not a substitute for police involvement

Step 8: Communicate with the Student and Family

- The DSL and/or a trusted member of staff should meet with the student and their family as soon as it is safe to do so
- Communicate clearly, calmly and without blame
- Ensure the family understands what is happening, what steps are being taken, and who the lead contact is
- Advise the family not to pay any demands and not to delete any communications they have received
- Signpost the family to appropriate support services, including those listed at the end of this document
- Record all communications with the family

Step 9: Support the Student's Wellbeing

- Ensure the student has access to pastoral and mental health support throughout the process
- Consider whether a referral to CAMHS or an external therapeutic service is appropriate
- Monitor the student's attendance, behaviour and wellbeing during and after the incident
- Maintain confidentiality appropriately, limiting knowledge of the incident to those with a clear need to know
- Keep the student informed about what is happening at each stage in an age-appropriate way

Step 10: Review and Debrief

- Once the immediate response is complete, the DSL and Trust safeguarding lead should review the incident
- Consider whether any changes to the academy's image use practice are needed as a result
- Consider whether any staff training or updated guidance is required

- Record all actions taken and outcomes on CPOMS
- Report the incident through the Trust's governance and safeguarding reporting structure

What Not to Do

Key Principles: Actions to Avoid;

- Do not pay any demand or respond to threats without police guidance.
- Do not attempt to view, download or share suspected illegal content.
- Do not contact or engage with the alleged perpetrator independently.
- Do not delete any communications, messages or evidence.
- Do not manage the incident without involving Trust safeguarding leadership.
- Do not disclose details of the incident to staff or other students beyond those with a clear need to know.
- Do not reassure the family that 'nothing will come of it' or downplay the concern.
- Do not attempt to negotiate with or appease those making demands.

Appendix 3:

Parent and carer communication and informed consent

Parent consent information letter template

Dear Parents and Carers,

Photos and videos are an important part of life at our academy. They help us celebrate children's achievements, share special moments, and show what daily life is like in our schools. Many families enjoy seeing these updates and being part of the community.

At the same time, the online world is changing quickly. There is a new and growing risk that images shared online (for example on school websites or social media) could be copied and misused. Some people may use technology, including AI, to change or manipulate images.

This is rare, but it is important that families understand the risks.

Our approach is not to stop using photos or videos. We believe it is important to keep celebrating children and sharing positive experiences. Instead, we are taking a careful and balanced approach so that images can be used safely.

Across ATT academies, this means we will:

- regularly review and update consent for photos and videos
- think carefully about what types of images we use
- avoid sharing unnecessary details that could identify children
- review how and where images are shared, including websites and social media

We also work to make images safer by:

- removing information such as location data before publishing (this is called metadata)
- checking privacy and sharing settings where possible
- using images in ways that reduce risk but still show school life

Once an image is online, other people may copy or share it. Because of this, we aim to use images in a thoughtful and careful way.

When we ask for your consent, we want it to be fully informed. This means you understand both:

- the benefits of sharing images
- the possible risks of images being shared online

If you would like to:

- ask questions
- check your child's current consent
- change your preferences
- or ask us not to use your child's image in certain ways

please contact the academy. We will always respond carefully and work with you.

If you ever become aware that an image of a child from the academy has been misused or shared in a way that worries you, please tell us straight away so we can take action to keep children safe.
Thank you for working with us to keep children safe while continuing to celebrate their success and experiences.

Yours sincerely,

Supporting families – What to Say

Helpful Framing	Avoid
• Your child has not done anything wrong • We are taking this very seriously and have already contacted the police • Please do not pay any demands or respond to any contact from whoever sent this • Please keep all messages and do not delete anything • We will keep you informed at every step	• Suggesting the family or student could have done more to prevent it • Downplaying the concern or suggesting it will resolve itself • Sharing details of the incident with other parents • Making promises about outcomes or timescales that cannot be kept

Appendix 4:

References, reporting routes and further guidance

Contacts

- **Police** 999 for emergency - 101 for non emergency report
- **Trust Safeguarding Lead** - via direct contact Details held by DSL
- **Children's Social Care** – Local Authority for the academy's area – details held by DSL

Recognised reporting and removal tools

- **Report Remove (Childline / IWF)** For under-18s to confidentially report and remove sexual or AI-generated images of themselves:
  https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/report-remove/

- **Internet Watch Foundation (IWF) reporting portal** For reporting illegal images of children, including AI-generated content:
  https://www.iwf.org.uk/en/uk-report/

- **CEOP Safety Centre** For reporting online sexual exploitation, coercion or abuse:
  https://www.ceop.police.uk/ceop-reporting/

- **StopNCII.org (Revenge Porn Helpline)** Helps prevent further sharing of non-consensual intimate images using digital fingerprinting. Only suitable for images of adults held on the adults own device:
  https://stopncii.org/

- **Google image removal requests** Request removal of explicit or non-consensual images from Google search results:
  https://support.google.com/websearch/answer/16854698

- **Professionals Online Safety Helpline** - A free helpline supporting professionals working with children and young people with any online safety issues they face. Professionals Online Safety Helpline | SWGfL

Further Guidance

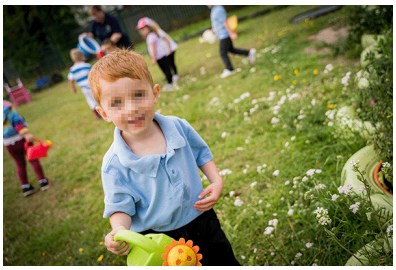
- **UK Safer Internet Centre**: image guidance for education settings.
- **Department for Education:** data protection in schools, including taking and using photos and videos.
- **Internet Watch Foundation:** guidance on AI-generated imagery and child protection.

This guidance should be read alongside the Trust's Safeguarding and Child Protection Policy, Data Protection Policy and Acceptable Use Policy.

Appendix 5:

Understanding and Addressing Image Risk

Example: High Risk Imagery


High resolution, portrait-style images show more of the subject's face, giving AI manipulation tools more data to work with, especially where academy details are visible such as logos or badges. The images above are deliberately censored but would otherwise be considered high-risk images. Be mindful of publicly sharing staged images where pupils are asked to look directly at the camera, such as at award presentations, where students' names may also be visible on certificates, in presentations, etc.

Example: Lower Risk Imagery



Photos where the subjects are not fully facing the camera present a lower risk. Using lower resolution images and wider framed compositions where subjects are further away from the camera is also helpful.

Removing Metadata

Photo metadata is hidden information embedded inside an image file. It can reveal exactly when, where, and how a picture was taken, who owns it, and the technical settings used by the camera. Removing location and timestamp information from an image before it is shared publicly can help avoid revealing academy routines. There are various ways to remove image metadata. Below is a method that will work on windows devices:

- Navigate to the image file in your file viewer. Right-click on the file and select '*properties*'
- In the window that opens, select the '*details*' tab at the top
- Click the link '*Remove Properties and Personal Information*' at the bottom
- Press '*Okay*' in the new window to create a copy of the file with all possible metadata removed

The copied file is safe to use online. On any device, including phones and tablets, **screenshotting** a photo creates a version without the location data and original timestamp.