



Signhills Academy

Image Use and Security Policy

Approved by:

Date: July 2026

**Next review
due by:**

Summer 2027 Full Gvs

1. Purpose and Scope

This policy sets out how Signhills Academy manages the use, storage, publication and protection of photographs, videos and other imagery featuring pupils, staff and visitors. It addresses the safeguarding risks arising from AI-enabled image manipulation, including the creation of deepfake content and AI-generated child sexual abuse material (AI CSAM).

The policy applies to all imagery used across the school's digital platforms (including ClassDojo, the school website and Facebook page), printed publications, displays, and any other public-facing materials. It covers images taken by staff, contracted photographers, parents and carers (at school events), and any third parties.

2. Legal and Regulatory Framework

This policy is informed by and supports compliance with:

- UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018
- Keeping Children Safe in Education (KCSIE) 2025 (and forthcoming 2026 revisions)
- The Children Act 1989 and 2004
- DfE guidance: Generative Artificial Intelligence (AI) in Education (updated May 2026)
- EWWG guidance: Protecting Your Setting's Images from AI Manipulation and Abuse (June 2026)
- ICO guidance on the use of photographs by schools

3. Key Principles

- **Safeguarding first:** the protection of children is the overriding priority in any decision about image use.
- **Proportionality:** measures should reduce risk without unnecessarily curtailing the school's ability to celebrate pupil achievement and share its life with the community.
- **Authenticated sharing:** identifiable pupil imagery is shared with families through ClassDojo (an authenticated, non-public platform) rather than on the open web or public social media.
- **Data minimisation:** we collect and publish only the imagery that is necessary, retain it only for as long as needed, and remove it when it is no longer current.
- **Informed consent:** parents, carers and (where age-appropriate) pupils must understand the risks as well as the benefits of image publication and give meaningful consent.
- **Staff awareness:** all staff understand the risks of AI image manipulation and follow the image security practices set out in this policy.

4. Image Capture Guidelines

When taking photographs or video of pupils for any school purpose, staff should follow these principles:

4.1 Preferred image types

- Activity-focused shots (e.g. hands working on a task, a science experiment from above, artwork in progress) where the learning is the subject rather than an individual child.
- Group and distance shots where individual faces are not the primary focus.
- Over-the-shoulder and angled shots that show what the child is doing without a clear, close-up, face-on portrait.
- Images of the school environment, resources and displays that do not feature identifiable children.

4.2 Images requiring additional care

- Close-up, face-on portraits of individual children should only be taken where there is a specific and justified reason and explicit parental consent for the intended use. Where such images are shared, they must be shared via ClassDojo only, not on the website or public social media.
- Images of children in situations that could be considered sensitive if taken out of context (e.g. swimming) must not be taken or published.
- Images of Looked After Children, children subject to court orders, or any child whose parents have withdrawn consent must not be taken or published under any circumstances.

4.3 Names and identifying information

The school does not pair children's full names with recognisable photographs on any platform. Where a child is named in text (e.g. an achievement announcement), any accompanying image should be a group or activity shot rather than an identifiable individual portrait. This is a longstanding practice and applies across all channels including ClassDojo.

5. Image Sharing and Publication

The school uses a tiered approach to image sharing, with the most identifiable imagery restricted to authenticated platforms and only generic, low-risk imagery used on public-facing channels.

5.1 ClassDojo (primary channel for pupil imagery)

ClassDojo Class Story and School Story are the school's primary channels for sharing photographs and videos of pupils with families. **All identifiable pupil imagery should be shared via ClassDojo rather than on the school website or Facebook page.**

ClassDojo is appropriate for this purpose because:

- Content is visible only to authenticated parents and carers who are connected to the school or class. It is not publicly accessible, not indexable by search engines, and cannot be scraped at scale.
- ClassDojo automatically strips EXIF metadata (including location data, device information and timestamps) from all images before they are viewed by other users.
- Teachers and school leaders control what is posted and can remove content at any time.

Staff should use Class Story for class-specific content (e.g. photos from a lesson, a trip, a class activity) and School Story for whole-school / cross-class content (e.g. sports teams, performances, assemblies).

5.2 School website

The school website should be used for generic, low-risk imagery only. This includes:

- Images of the school environment, buildings and grounds.
- Activity shots and group photographs taken from a distance where individual children are not readily identifiable.
- Stock or illustrative images that support page content.

The website should not be used to share close-up, identifiable photographs of individual pupils. Where the website currently contains such images, these should be reviewed and, where appropriate, replaced with lower-risk alternatives.

All images uploaded to the website must have EXIF metadata stripped before upload. The website administrator is responsible for this.

Images of pupils who have left the school are removed at the end of the school year in which they leave.

5.3 Facebook

The school's Facebook page should be used for text-based announcements, community news, reminders and general engagement. It should not be used to share identifiable photographs of individual pupils.

Where images are used on Facebook (e.g. to illustrate an event or announcement), they should follow the same low-risk principles as the website: distance shots, activity-focused images, or images where individual children are not readily identifiable.

- Staff must not share or repost school images of pupils to personal social media accounts.
- Comments on posts are not permitted.

5.4 Printed and display materials

Printed publications (newsletters, prospectus, corridor displays) carry lower risk than online publication as they are not as readily scraped at scale. The same consent requirements apply, and images of children who have left should be replaced at the next print run or display refresh.

5.5 Local media

Where the school is featured in local media coverage, images may be shared with the media outlet only where specific parental consent for media use has been obtained. The school should request that the media outlet does not pair a child's full name with an identifiable photograph.

Channel	Use for	Do not use for
ClassDojo	All pupil photographs and videos shared with families. Class and whole-school celebrations.	N/A – this is the primary and preferred channel for pupil imagery.
Website	Generic/distance shots, environment images, activity-focused photos where individuals are not readily identifiable.	Close-up identifiable pupil portraits. Any image paired with a child's full name.
Facebook	Text announcements, community news, reminders. Generic/distance images only where needed.	Identifiable pupil photographs. Staff reposting to personal accounts.
Print / Display	Newsletters, prospectus, corridor displays (with consent). Lower risk than online channels.	Images of LAC/restricted pupils. Images of leavers (replace at next refresh).

6. Consent

Consent for the use of pupil imagery is obtained via the school's image consent form, which is issued to all families on admission and re-confirmed annually.

The consent form must:

- Clearly explain why the school uses pupil imagery and the channels through which it may be shared (ClassDojo, website, print, local media).
- Explain the risks associated with online publication, including the possibility that images could be downloaded or manipulated by third parties using AI tools.
- Describe the steps the school takes to reduce these risks, including the use of ClassDojo as a non-public, authenticated platform.
- Offer a clear and straightforward opt-out for each channel, with assurance that opting out will not disadvantage the child.
- Explain how consent can be withdrawn at any time.

Where pupils are of sufficient age and maturity to understand, their views should also be sought by parents.

Staff with concerns about their own images being used should speak to the Headteacher. Staff consent is managed separately through the **Staff Code of Conduct** and employment terms.

7. Metadata and Technical Measures

ClassDojo automatically strips all EXIF metadata from images before they are viewed by parents. No manual action is required for content shared via ClassDojo.

For images uploaded to the school website, the following technical steps must be taken before upload:

- **EXIF metadata removal:** all location data, device identifiers and timestamps must be stripped. The UK Safer Internet Centre's guide provides step-by-step instructions.
- **Image resolution:** images should be resized to the minimum resolution required for web display.
- **Watermarking:** the school may choose to apply a watermark to images to deter misuse.

Staff who populate the website and Facebook page are responsible for implementing and maintaining these measures.

8. Content Review and Audit

The school will carry out a documented review of all pupil imagery across its platforms at least termly. The audit should:

- Identify and remove images of pupils who have left the school from the website and any remaining legacy content on Facebook.
- Confirm that the website contains only generic, low-risk imagery in line with this policy.
- Confirm that identifiable pupil imagery is being shared via ClassDojo only.
- Confirm that metadata has been stripped from all website images.
- Check that consent remains in place for all pupils whose images are used.
- Review Facebook content and confirm no identifiable pupil imagery has been posted.
- Review ClassDojo School and Class Story content for appropriateness.

The audit should be recorded using the checklist at Appendix A and retained for at least one year. The DSL and website administrator share responsibility for this process.

9. Incident Response: Misuse, Manipulation or Blackmail

If the school becomes aware that pupil or staff imagery has been misused, manipulated, or used in an attempt at blackmail, the following steps must be taken **immediately**:

9.1 Contain and escalate

- Do not delete any communication, threat or imagery received. Retain and store securely for the police.
- Immediately remove the original (unaltered) versions of the compromised images from all school platforms.
- Notify the Designated Safeguarding Lead (or deputy) and the Headteacher.
- **Do not engage with the individual making threats. Do not respond to demands. Do not make any payment.** The paying of ransom can be illegal in certain circumstances.

9.2 Report

- **Police:** Report to local police. If a child is at immediate risk, call 999.
- **Report Remove (Childline/IWF):** Supports under-18s to report sexual images of themselves, including AI-generated images.
- **Take It Down (NCMEC):** Removal of under-18 intimate imagery including AI-generated.
- **Stop NCII:** For removal of non-consensual intimate images of adults (18+), including AI-generated.
- **Platform reporting:** Request removal from any hosting site or social media platform.

9.3 Support

- Prioritise the safety and emotional wellbeing of affected pupils.
- Inform parents and carers of affected children with clear next steps.
- Ensure affected staff have access to wellbeing support. The Professionals Online Safety Helpline (SWGfL) is available for advice.
- Record the incident in line with safeguarding and incident reporting procedures.

9.4 Prevent recurrence

- Carry out an immediate audit of all remaining imagery across all platforms.
- Review and tighten publication practices.
- Update staff training to reflect lessons learned.
- Report the incident and outcomes to the Governing Body.

10. Staff Training

All staff will receive training on image security as part of the school's annual safeguarding update. This training will cover:

- The risks posed by AI image manipulation and deepfake technology.
- The school's tiered approach to image sharing (ClassDojo for identifiable imagery; website and Facebook for generic content only).
- The school's image capture guidelines and the types of photographs to prioritise.
- How to recognise and respond to incidents of image-based abuse, blackmail or threats.
- Staff responsibilities regarding their own use of school imagery (including not sharing to personal social media accounts).

The DSL is responsible for ensuring this training is delivered and recorded.

11. Photography by Parents and Visitors at School Events

Parents and carers are permitted to take photographs and videos of their own children at school events (e.g. performances, sports day) for personal, family use. However:

- Parents must not publish images of other people's children on social media without the consent of those children's parents.
- The school will include a reminder about responsible image sharing in communications ahead of events.
- The school reserves the right to restrict photography at specific events where safeguarding concerns arise.

12. Policy Review

This policy will be reviewed annually, or sooner if there is a significant change in guidance, legislation, technology or incident. Given the pace of change in AI technology, the school will monitor developments throughout the year and update practice as necessary between formal review cycles.

Appendix A: Image Security Checklist

Use this checklist to carry out the image audit. Complete and retain for records.

✓	Action	Notes / Owner
☐	All images of leavers removed from school website	Check leavers list against published content
☐	Website contains only generic/low-risk imagery	No close-up identifiable pupil portraits
☐	No identifiable pupil imagery on Facebook page	Review all posts since last audit
☐	EXIF metadata stripped from all website images	Spot-check ~5 images using metadata viewer
☐	ClassDojo being used as primary image sharing channel	Confirm Class Story active across all year groups
☐	Consent records checked against published imagery	Cross-reference Arbor consent data
☐	Image guidelines shared with staff this term	Note date of last briefing or training
☐	No images of LAC or restricted pupils on any platform	Check against DSL restricted list
☐	Incident response plan accessible to DSL and HT	Confirm document location and currency

Audit date:	
Completed by:	
Actions arising:	

Appendix B: Key Contacts and Reporting Routes

Organisation / Service	Details
Police (non-emergency)	101 (or 999 if immediate risk of harm)
Report Remove (Childline / IWF)	childline.org.uk – for under-18s to report sexual images of themselves
Internet Watch Foundation	iwf.org.uk – anonymous reporting of suspected CSAM
Take It Down (NCMEC)	takeitdown.ncmec.org – removal of under-18 intimate imagery
Stop NCII (adults 18+)	stopncii.org – removal of non-consensual intimate images of adults
Professionals Online Safety Helpline	saferinternet.org.uk/helpline – advice for education professionals
UK Safer Internet Centre – Image Guidance	saferinternet.org.uk/guide-and-resource/image-guidance-for-education-settings