Brabyns Nursery School

PROTECTING CHILDREN AND STAFF IMAGES

Date approved - August 2026
Next review date - August 2027, or sooner following an incident or regulatory change

Purpose and Scope

This policy sets out Brabyns Nursery School approach to the safe capture, use, storage and publication of images and video ("imagery") of pupils and staff across school websites, social media channels, prospectuses, newsletters and other promotional or communications materials, as well as third parties the school uses with regard to imagery.

This policy is informed by,'Protecting your setting's images from AI manipulation and abuse: Guidance for education settings and organisations working with children and young people' (UK Online Harms Early Warning Working Group / UK Safer Internet Centre' and KCSIE 2026. Other school policies that it links to include Safeguarding, Behaviour, Anti-Bullying, Mobile Phones, Appropriate Use of Technology and AI.

Safeguarding is the paramount consideration throughout this policy. Image security is treated as a safeguarding matter, not merely a marketing, IT or data protection matter. Photographs and videos of pupils published on websites, social media platforms and other digital spaces can be copied or scraped by third parties without the school's knowledge. Once obtained, such images can be:

- Manipulated using AI tools — including nudification apps — to create sexualised or abusive imagery. It is illegal to create such material regardless of whether it is AI-generated.
- Used to blackmail schools, families or individual pupils and staff with threats to publish manipulated imagery unless a ransom is paid.
- Combined with metadata (e.g. location or timestamp data) to expose an individual's routine, home area, or the school's site layout, creating physical safety risks.
- Shared or reused without consent, causing distress, reputational harm and loss of control over an individual's identity and personal data.

Policy Statement

Brabyns Nursery School is committed to:

- Treating the safeguarding, dignity and wellbeing of every pupil and member of staff as the first consideration in any decision to capture, use or publish imagery.
- Minimising the identifiability, resolution and metadata of published images so that they are harder to misuse or manipulate.
- Auditing published imagery on a regular, documented basis and removing or updating content that is out of date, unnecessary or no longer consented to.
- Responding swiftly, sensitively and in line with statutory safeguarding procedures to any incident of image misuse, manipulation or abuse.

Roles and Responsibilities

Governors - Approve and monitor the policy

Designated Safeguarding Lead (DSL) in each school - Act as the first point of escalation for any actual or suspected incident of image misuse or abuse; ensure any incident is treated as a safeguarding matter and, where appropriate, referred to the police.

Head - Ensure this policy is implemented consistently within their school, that staff are trained, and that image-related incidents are reported.

Marketing, Communications and Admissions staff - Apply the image security principles in to all website, social media, prospectus and promotional content

All staff, volunteers and contractors - Report any concern about image misuse immediately to the DSL.

Pupils, parents and carers - Are provided with clear information about how imagery is used and protected, and are supported to raise concerns or withdraw consent.

Consent

Consent is the foundation of lawful and ethical use of pupil imagery. The Group will:

- Seek written parental/carer consent for the use of pupil imagery on the website, social media and in promotional materials, obtained on enrolment and reviewed at key transition points (e.g. annually, or on moving between prep and senior school).
- As best practice, also seek the pupil's own consent alongside parental/carer consent where the pupil is of sufficient age and understanding to make that decision, recognising their growing autonomy and rights.
- Ensure consent forms are written in plain, accessible language, clearly explain how images may be used, and set out the specific risk of online misuse and AI manipulation so that consent is genuinely informed.
- Make clear that consent can be withdrawn at any time, and provide an easy, named route for parents, carers or pupils to do so.
- Record consent status against each pupil and ensure marketing and communications staff check this record before publishing any identifiable image.
- Never rely on assumed or historic consent where the purpose of use has changed materially (for example, moving from a printed prospectus to open social media).

Image Security Principles (Best Practice)

Before using any image of a pupil, staff should first ask: is an identifiable image of a child actually needed to achieve the communications objective, or would imagery without faces serve the purpose equally well?

Where identifiable pupil imagery is used, the following principles apply across all Group schools:

a) Reducing identifiability

- Avoid publishing full names alongside photographs;
- Prefer images taken from a distance, at an angle, over-the-shoulder, in groups, or otherwise not face-on and fully identifying, where this still meets the communications need.
- Avoid images that reveal a pupil's home area, regular routine, or specific location/time patterns (e.g. always published on the same day as a fixed weekly activity).

b) Technical protection

- Remove EXIF and other metadata (location, device, timestamp) from every image before publication.
- Use appropriately reduced image resolution to reduce the quality available for manipulation, while remaining fit for purpose.
- Apply visible or embedded watermarking where practicable, particularly for images used in open, public-facing contexts.
- Consider protective software solutions

c) Access and platform controls

- Apply the most restrictive privacy and sharing settings appropriate to the purpose
- Limit the number of staff with rights to publish images
- Store master/original image files securely

- Only retain pupil imagery for as long as necessary.

d) Working with external photographers and agencies
- Ensure any external photographer, agency, sports club, theatre company or tour operator engaged by a Group school is briefed and contractually required to follow this policy
- Carry out appropriate safeguarding checks (e.g. DBS) on any photographer with unsupervised access to pupils.

Content Audits and Ongoing Review
- Each school will carry out a documented audit of pupil imagery on its website, social media channels and key promotional materials at least termly, reported at pastoral governance
- Audits will check that: consent remains current and valid; imagery of pupils who have left the school or withdrawn consent has been removed; images comply with the security principles; and no image inadvertently discloses sensitive information
- Outdated, unnecessary or non-compliant images will be removed or replaced without delay

Social Media Specific Guidance
- Only approved, officially managed social media accounts may be used to publish pupil imagery; personal staff accounts must never be used to post images of pupils.
- Before posting, staff must check the platform's current privacy and audience settings and apply the most restrictive setting consistent with the purpose of the post.
- Live-posting of imagery that could reveal a pupil's real-time location (e.g. an away fixture in progress) should be avoided or delayed.
- Comments and shares on official accounts should be monitored, and any resharing, screenshotting or manipulation of posted imagery identified through monitoring should be treated as a potential incident under Section 9.
- Staff should follow the Group's Acceptable Use Policy alongside this document; where the two differ on imagery specifically, this policy takes precedence.

Responding to Misuse, Alteration or Abuse of Images
Any suspicion that a pupil's or staff member's image has been taken, manipulated (including by AI) or used without consent — including AI-generated sexualised imagery or blackmail attempts — must be treated as an urgent safeguarding incident and escalated immediately to the DSL.

The response will be in line with the Safeguarding Policy including guidance on sharing of images, including contacting the police where the use of the image is illegal. In addition the school will
- Take immediate steps to ensure the original, compromised image is no longer publicly available, including removing it from the school website or social media.
- not engage with individuals attempting blackmail or respond to any demand.
- Request direct removal from the hosting website or social media platform where the image has been shared
- Support pupils inline with the safeguarding policy
- Audit imagery on sites and platforms, and review this policy

- Report Remove (Childline/IWF): Supports under-18s to confidentially report sexual images or videos of themselves, including AI-generated images, for potential removal from the internet.
- Take It Down (NCMEC): An image take-down service, including for AI-generated images.
- Stop NCII: For removal of non-consensual intimate images of those aged 18 and over — relevant to sixth-form pupils and staff.
- Internet Watch Foundation (IWF): Anonymous reporting route for suspected child sexual abuse imagery.
-

Training

- All staff will receive this policy on induction
- Marketing, communications, admissions and IT staff will receive additional, role-specific training on the technical measures
- Designated Safeguarding Leads will ensure this topic is included in whole-school safeguarding briefings and in curriculum-based online safety education for pupils, age-appropriately.

Appendix: Useful Contacts and Resources

Reporting and support routes

- Police (non-emergency 101 / emergency 999): Report threats to publish sexual imagery of a child; call 999 for immediate risk of significant harm.
- Internet Watch Foundation (IWF): report.iwf.org.uk — anonymous reporting of suspected child sexual abuse imagery.
- Report Remove (Childline / IWF): childline.org.uk — confidential support for under-18s to report and seek removal of sexual images of themselves, including AI-generated images.
- Take It Down (NCMEC): takeitdown.ncmec.org — image take-down service, including AI-generated images.
- Stop NCII: stopncii.org — removal of non-consensual intimate images of those aged 18 and over.
- Revenge Porn Helpline: support for adults (18+), including staff, threatened with the release of intimate images.
- Professionals Online Safety Helpline (SWGfL): support for professionals working with children on any online safety issue.
- Stop It Now: helpline and support, including for staff affected by exposure to distressing material.
- Marie Collins Foundation: support for children impacted by technology-assisted child sexual abuse and image-based abuse.

Guidance and templates

- UK Online Harms Early Warning Working Group / UK Safer Internet Centre: Protecting your setting's images from AI manipulation and abuse — saferinternet.org.uk/education-images
- IWF and NCA CEOP Education: Understanding and responding to AI-generated child sexual abuse material
- ICO: Taking photographs — data protection advice for schools
- ICO: A guide to data security (UK GDPR)
- ICO: Data sharing code of practice
- SWGfL: Online Safety Policy template and Social Media checklists
- UKCIS: How to respond to an incident (overview)
- Hwb: Practices and principles for schools' use of social media
- Guide to removing EXIF metadata (UK Online Harms Early Warning Working Group)