BRUERN ABBEY SCHOOL

PROTECTING PUPIL AND STAFF IMAGES

Bruern Abbey version prepared 19 November 2026

Next review by August 2027, or sooner following an incident or regulatory change

Purpose and Scope

This policy applies to Bruern Abbey Prep School and Bruern Abbey Senior School. It covers how the school and third parties acting on its behalf take, use, store and publish photographs and videos of pupils and staff. It applies to school websites, social media, prospectuses, newsletters and other school communications and promotional material.

This policy draws on Keeping Children Safe in Education 2026 and the UK Safer Internet Centre's guidance on protecting education settings' images from AI manipulation and abuse. Read it alongside the Prep and Senior Safeguarding Policies, Mobile Phone and Camera Policy, Appropriate and Safe Use of Technology Policy, AI Policy, Behaviour Policy, Anti-Bullying Policy, Data Protection Policy and Information Security Policy.

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 to create sexualised or abusive imagery. Follow the school's safeguarding procedures and the guidance in Keeping Children Safe in Education 2026.
- 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

Bruern Abbey School is committed to the following principles.

- 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- Auditing published imagery on a regular, documented basis and removing or updating content that is out of date, unnecessary or no longer consented to.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 this policy.

The Designated Safeguarding Lead (DSL) at each school is the first point of contact for suspected image misuse. The DSL follows the relevant Prep or Senior Safeguarding Policy, including referrals to the police or other agencies where appropriate. Current contact details are in each school's Safeguarding Policy.

The Head of Prep and Head of Senior oversee implementation, training and incident reporting at their respective schools.

Marketing, Communications and Admissions staff apply this policy to school websites, social media, prospectuses and other promotional material. Marketing coordinates the termly audit with the DSLs.

Staff, volunteers and contractors report any concern about image misuse immediately to the relevant DSL or deputy.
Pupils, parents and carers receive clear information about how images are used and protected, how to raise concerns and how to withdraw consent.

Consent

Before publishing identifiable staff imagery, explain the intended use to the staff member and follow the school's Data Protection Policy. Apply the following consent requirements to identifiable pupil imagery.

- Obtain written consent from parents or carers before using identifiable pupil imagery on the website, social media or in promotional materials. Record consent on enrolment and review it at least annually and at the transition from Prep to Senior.
- Seek the pupil's own agreement alongside parent or carer consent when the pupil has sufficient understanding. For pupils in Years 8 to 11, seek consent from both the pupil and their parent or carer in line with the Mobile Phone and Camera Policy.
- 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.
- Parents, carers and pupils can withdraw consent at any time by contacting the Prep or Senior School office. The office will update the school's consent record and inform staff responsible for published material.
- Record pupil consent and any safeguarding restrictions in the school's designated system. Marketing and Communications staff must check the record before publishing an identifiable image or video.
- Obtain consent for the new use if the purpose of publication changes materially, for example when moving an image from a printed prospectus to public 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?

These principles apply to identifiable pupil imagery at both Bruern Abbey Prep and Senior.

a) Reducing identifiability

- Keep pupils' full names off photos, videos and accompanying captions.
- 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 metadata, such as location, device and time information, before publishing where technically practicable.
- Where technically practicable, use website controls such as disabling right-click and image hotlinking to discourage unauthorised copying or reuse. Treat anything published online as capable of being copied.
- 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 publishing access to authorised staff.
- Store original image and video files in approved school storage.
- Retain imagery only for as long as necessary in line with the school's retention arrangements.

d) Working with external photographers and agencies
- Brief external photographers, agencies and other providers engaged by Bruern Abbey School on this policy. Include compliance with it in their contract or written instructions.
- Carry out appropriate safeguarding checks (e.g. DBS) on any photographer with unsupervised access to pupils.

Content Audits and Ongoing Review
- Marketing, working with the Prep and Senior DSLs, will document an audit of published pupil imagery on the website, social media and key promotional materials at least once a term. The Heads will report the findings through pastoral governance.
- Check that consent remains current, that imagery of pupils who have left or withdrawn consent has been removed from school channels, and that published images follow the security principles and avoid disclosing 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.
- Delay posts that could reveal a pupil's real-time location, such as photos or video from an away fixture or school trip in progress.
- Monitor comments and shares on official accounts. Refer suspected unauthorised reuse, alteration or other misuse to the relevant DSL under 'Responding to Misuse, Alteration or Abuse of Images'.
- Read this policy alongside the Mobile Phone and Camera Policy and the Appropriate and Safe Use of Technology Policy. Follow this policy's official-accounts rule whenever publishing pupil imagery. Follow the Mobile Phone and Camera Policy for device use and photography at school events.
- When selecting pupil imagery for social media, staff should avoid close-up, face-on individual portrait photographs wherever practicable and instead favour natural action shots, group photographs, wider-angle images, side-on or over-the-shoulder photography. An identifiable individual portrait should only be used where there is a clear communications purpose and the appropriate consent is in place.

Responding to Misuse, Alteration or Abuse of Images

Report suspected unauthorised capture, use or alteration of a pupil's or staff member's image immediately to the relevant DSL or deputy. Treat suspected AI-generated sexualised imagery and attempted blackmail as urgent safeguarding incidents.

The DSL will follow the relevant Prep or Senior Safeguarding Policy and national guidance, involving the police or other agencies as appropriate. For suspected nude or semi-nude imagery of a child, staff must follow the safeguarding guidance on handling it and seek direction from the DSL before taking further action. The school will also take the following steps.

- Remove the original image from school-controlled public channels promptly, following any advice from the DSL or police about preserving evidence.
- Leave any response to attempted blackmail to the DSL and police.
- Ask the hosting website or social media platform to remove the misused image, following advice from the DSL or police.
- Offer affected pupils and staff appropriate safeguarding, pastoral or HR support.
- Review the school's published imagery and this policy after an incident.

- 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) helps people request removal of nude, partially nude or sexually explicit images taken when they were under 18.
- Stop NCII helps adults seek removal of non-consensual intimate images from participating platforms.
- Internet Watch Foundation (IWF): Anonymous reporting route for suspected child sexual abuse imagery.

Support for Adults

Staff and other adults affected by the sharing or threatened sharing of intimate or manipulated images can contact Stop NCII or the Revenge Porn Helpline, alongside the school's safeguarding and HR support routes.

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) offers help with images taken when the person was under 18. Visit takeitdown.ncmec.org.
- 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 and UK Safer Internet Centre guidance on protecting school images from AI manipulation and abuse. Visit 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)