



Safe Use of Children's Images and Recordings Policy

**St Matthew's Catholic Primary School
2026–2027**

“Love, Learn and Shine Together with Jesus.”

Policy owner	Mrs Claire Sime, Headteacher
Data Protection Officer	Mrs Louisa Chamberlain
Safeguarding lead	Designated Safeguarding Lead
Approved by	Governing Body
Approval date	September 2026
Review date	September 2027, or sooner following statutory, technological or safeguarding change
Applies to	Staff, governors, volunteers, visitors, contractors, pupils, parents and carers
Scope	Photographs, video, audio, livestreams, screenshots, scanned images, digital artwork and AI-generated or AI-edited media

1 Purpose and key decision

St Matthew's Catholic Primary School celebrates pupils' learning and achievements while placing their safety, dignity and privacy first. Images and recordings can support teaching, assessment, communication and celebration, but once an image is published or shared it may be copied, altered, redistributed or used to create convincing AI-generated material without the child's knowledge or consent.

As an additional safeguarding measure, the school will use only partial, non-identifying or non-facial images of pupils on public-facing channels. The school will not publish or supply a clear, full-face, individually identifiable image of a pupil on its public website, public social-media accounts, public promotional material or external publicity. Suitable images may show hands engaged in learning, work being created, the back or side of a pupil, an over-the-shoulder view, a carefully framed group activity or an image taken from a distance.

This public-publication rule does not prevent the school from holding clear images where they are necessary for internal administration, safeguarding, identification, educational records or another lawful purpose. Such images will not be made public and will be protected under this policy.

2 Legal and statutory framework

This policy has regard to the following legislation and guidance, as amended:

- Keeping Children Safe in Education 2026;
- the Children Acts 1989 and 2004 and section 175 of the Education Act 2002;
- the UK General Data Protection Regulation and Data Protection Act 2018;
- the Online Safety Act 2023;
- the Crime and Policing Act 2026 and relevant offences concerning indecent, intimate and AI-generated images;
- the Protection of Children Act 1978 and Criminal Justice Act 1988;
- the Human Rights Act 1998;
- the Copyright Designs and Patents Act 1988;
- DfE guidance on data protection and generative artificial intelligence in schools;
- DfE guidance on sharing nudes and semi-nudes, including AI-generated and deepfake imagery; and
- Information Commissioner's Office guidance on children's information, photographs and consent.

Images that identify a living person are personal data. Some images may also reveal special-category information, safeguarding status, disability, religion or health. The school will identify and document an appropriate lawful basis for each purpose and will apply the data-protection principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, security and storage limitation.

3 Definitions

Image or recording. Any photograph, video, audio recording, livestream, screenshot, scan, digital artwork or other media from which a child may be identified directly or indirectly.

Public-facing channel. A website, open social-media account, public newsletter, prospectus, advertising, press release, public display or other material available beyond a controlled school audience.

Partial or non-identifying image. An image framed so that a child's face and other distinctive features do not enable identification, for example hands at work, an over-the-shoulder view, the back or side of the child, or a distant group scene.

Deepfake or synthetic media. Image, video or audio created or altered using AI or other technology so that it appears to depict a real person doing or saying something that did not happen.

Personal device. A privately owned phone, camera, tablet, computer, wearable device, storage medium or personal online account.

4 Roles and responsibilities

4.1 Governing Body and Headteacher

- ensure that image use is lawful, proportionate and consistent with safeguarding;
- approve the school's public use of partial and non-identifying images;
- ensure suitable systems, devices, contracts, training and breach procedures;
- ensure that photography does not expose a pupil whose location or identity must be protected; and
- review emerging risks, including generative AI, deepfakes and facial manipulation.

4.2 Data Protection Officer

- advise on lawful basis, privacy information, consent, retention, processors and data-protection impact assessments;
- maintain consent and objection arrangements and advise on rights requests;
- support assessment and reporting of suspected personal-data breaches; and
- review new platforms, photography services or AI-enabled tools before use.

4.3 Designated Safeguarding Lead

- identify children for whom publication or photography creates an increased risk;
- advise staff without revealing unnecessary safeguarding information;
- lead the response to image misuse, sexualised imagery, deepfakes, harassment or exploitation;
- make referrals to Children's Social Care, police or specialist services where required; and
- ensure that online-safety education and staff training address emerging image-based harm.

4.4 All staff and volunteers

- use only authorised school equipment, accounts and platforms;
- check the purpose, permissions and safeguarding restrictions before capturing or sharing an image;
- apply the public rule on partial and non-identifying images;
- respect a child who does not wish to be photographed or recorded;
- never upload a pupil image, recording or identifying information to a generative AI tool;
- store, transfer and delete images in accordance with this policy; and
- report any loss, accidental disclosure, misuse, suspicious request or harmful image immediately.

5 Lawful basis consent and pupil voice

Consent is not the lawful basis for every school image. The school may use images without consent where this is necessary for a legal obligation, public task, vital interests, safeguarding, identification or another documented lawful purpose. Images used for optional publicity, promotion or media activity will normally rely on specific, informed and freely given consent.

Publicity consent will be separate from admissions and other terms, use clear choices for different channels where appropriate, and explain that consent may be withdrawn. Withdrawal will apply to future use and to material the school controls; it may not be possible to retrieve printed material already distributed or copies made by others after lawful publication.

The child's views will be taken into account according to age and understanding. A pupil will not be forced, pressured or disadvantaged for declining. Even where a parent or carer has consented, staff will normally respect a child who does not want an image taken or used. Consent will be reviewed at least annually and whenever circumstances or the intended use change.

6 Safeguarding and risk assessment

Before taking or publishing images, staff will consider whether the image could reveal a pupil's identity, location, routine, school journey, home, medical condition, SEND, religion, family circumstances or safeguarding status. Particular care is required for children subject to court orders, care arrangements, adoption, domestic-abuse risks, witness protection, child-protection plans or other restrictions.

The DSL will maintain a secure method of alerting relevant staff to restrictions without making the reason visible to other pupils or families. Staff will plan activities sensitively so that a child who cannot be photographed is included and is not singled out or identified by their absence from an image.

Images will never be taken when a child is distressed, receiving first aid or medical care, using a toilet or changing area, in a state of undress, or in a situation that could be embarrassing, degrading, intrusive or open to sexualisation. Images used for swimming or sport must protect dignity and will not show children in changing areas.

7 Public website social media and publicity

- Only partial, non-identifying or non-facial pupil images may be placed on public school channels.
- The school will not publish a clear, close-up, full-face image from which an individual pupil can be identified.
- A pupil's full name will not be published with an image. Captions will not reveal unnecessary personal information, precise routines or live location.
- Staff will check backgrounds for names, labels, screens, medical information, addresses, vehicle registrations or other identifying detail.
- Location and camera metadata will be removed where practicable before publication.
- Images will be uploaded only through authorised school accounts by authorised staff.
- Public posts will not enable facial tagging, public comments, downloads or location sharing where the platform permits these controls.
- Live posting from a visit or event will be avoided where it could reveal children's real-time location or routine.
- Public images will be reviewed and removed when no longer needed or when consent or risk changes.

The partial-image approach reduces risk but cannot guarantee anonymity. Uniform, context, work, voice or other features may still identify a pupil. Staff must therefore continue to check lawful basis, consent where applicable and individual safeguarding restrictions.

8 Internal educational and administrative use

The school may take and retain identifiable images for legitimate internal purposes, including pupil records, safeguarding, assessment, evidence of learning, access arrangements, displays within controlled areas and secure communication with parents. Only the minimum necessary image will be captured and access will be limited to staff and recipients who need it.

Internal display does not automatically permit online publication. Images from learning platforms, school information systems or closed parent communications must not be copied to personal devices, personal accounts, messaging groups or public social media. Screenshots are subject to the same rules as the original image.

9 Staff devices storage and transfer

- Pupil images and recordings must be captured only on authorised school devices unless the Headteacher has approved a documented exceptional arrangement.

- Personal phones, personal cameras, private email, WhatsApp, personal cloud storage, memory sticks and personal social-media accounts must not be used to capture, store, transfer or share pupil images.
- Images must be transferred promptly to the approved school system and removed from the device, local downloads, recently deleted folder and temporary storage when no longer required.
- Access will be role-based and protected by passwords, multi-factor authentication where available, encryption and current security controls.
- Images will not be copied or retained simply because storage is available. Duplicate and poor-quality images will be deleted securely.
- Any lost device, misdirected message, unauthorised access or accidental upload must be reported immediately to the Headteacher, DPO and DSL.

10 Generative AI deepfakes and image manipulation

A real pupil's image, video, voice, name, work or identifying information must not be entered into, uploaded to or processed by a generative AI service. This prohibition includes tools used to generate, edit, enhance, animate, restyle, crop, remove backgrounds, clone voices, create avatars, train models or produce synthetic media, unless the Headteacher and DPO have approved a specific system following a documented data-protection and safeguarding assessment. Consumer AI tools will not be approved for this purpose.

Staff and pupils must not create, request, possess or share a deepfake, manipulated image, synthetic voice or AI-generated media that purports to depict a pupil or member of the school community without explicit authority and a lawful, safe purpose. Sexualised, intimate, humiliating, threatening or abusive material will be treated as a safeguarding concern and may constitute a criminal offence.

School-created illustrations using AI must not be based on or resemble a real pupil, must not include personal data, and must be checked for bias, harmful content and misleading presentation. Where necessary, synthetic content will be clearly labelled. AI-generated material will not be presented as a genuine photograph or recording of a school event.

11 Responding to harmful images or deepfakes

If a member of staff becomes aware of a harmful, sexualised, intimate or manipulated image involving or appearing to involve a child, they must not download, print, copy, forward or ask the child to share it. They must preserve only the minimum information necessary, such as the platform, account, URL, time and how the concern came to attention, and report immediately to the DSL.

The DSL will follow KCSIE, the school Child Protection and Safeguarding Policy and current guidance on sharing nudes and semi-nudes, including AI-generated and deepfake imagery. The response may include risk assessment, support for the child, platform reporting, preservation of evidence, parental contact where safe, and referral to police, Children's Social Care or other specialist agencies. Staff must not investigate or search devices beyond their authority.

12 Parents carers and visitors at events

Photographs taken by parents or carers for purely personal or household purposes may fall outside data-protection law. However, the school controls access to its premises and events and may restrict or prohibit photography to protect children, preserve confidentiality or avoid disruption.

- The school will tell families in advance whether personal photography is permitted.
- Where photography is allowed, it must be unobtrusive, must not interfere with the event and must stop immediately if directed by staff.
- Parents and carers must focus on their own child and must not publish, tag or share images containing other children without permission from those children's parents or carers.

- Photography and recording are prohibited in toilets, changing areas, medical spaces and any area identified by the school.
- Livestreaming by parents, carers or visitors is not permitted.
- Where a safeguarding restriction means photography cannot be managed safely, the school may operate a no-photography event or provide an approved image afterwards.

These event rules are safeguarding and premises-management decisions. The school will communicate them positively and apply them consistently.

13 Pupils taking images

Pupils may take images or recordings only as part of an authorised, supervised learning activity using approved school equipment and accounts. Staff will teach consent, respectful framing, privacy, copyright, misinformation, deepfakes and safe reporting in an age-appropriate way. Pupils must not photograph or record another person secretly, in a private setting, against their wishes or for bullying, humiliation or sexualisation.

Unauthorised images will be managed under the Relationships and Behaviour Policy, Online Safety Policy and Child Protection and Safeguarding Policy. Staff will avoid viewing, copying or deleting suspected illegal sexual imagery unless directed under the applicable safeguarding procedure.

14 Media commercial photographers and contractors

- The Headteacher must approve all external photography or filming in advance.
- The purpose, lawful basis, intended audience, retention, ownership, security and deletion arrangements will be documented.
- Parents, carers and pupils will be informed and specific consent obtained where required.
- The photographer or contractor will receive a written brief and contract, display identification and remain supervised.
- There will be no unsupervised access to pupils, private one-to-one sessions, contact outside the agreed activity or use for the contractor's own portfolio, advertising or AI training.
- The school will not provide a clear, full-face, individually identifiable pupil image for public media use. Any press attendance will be subject to the school's partial-image requirement and safeguarding controls.
- Files must be transferred securely and deleted by the contractor at the agreed time, with confirmation where required.

15 Livestreaming video calls and remote participation

Any school-controlled livestream, video call or remote participation will use an approved platform and be risk assessed. Access will be restricted to the intended audience, links and passwords will not be published openly, recording will be disabled unless necessary and authorised, and participants will be told whether recording is taking place. Backgrounds, names, chat, screen sharing and participant lists will be managed to minimise disclosure.

16 Retention deletion and individual rights

Images and recordings will be retained only for as long as needed for the documented purpose and in accordance with the school retention schedule. Publicity images will be reviewed regularly. Secure deletion will include copies held in local folders, devices, cloud storage, editing software, backups where practicable and contractor systems in accordance with agreed retention arrangements.

Children and parents or carers may ask how an image is used, object to processing, withdraw consent or request deletion. The DPO will consider each request under data-protection law. Rights are not absolute; an image may need to be retained for safeguarding, legal claims, statutory records or another compelling lawful reason. The school will explain the outcome.

17 Copyright ownership and reuse

The school will respect copyright and licensing. Images found online will not be copied simply because they are visible. Staff will use school-owned, licensed or appropriately credited material. A person receiving a school image does not automatically gain permission to edit it, use it commercially, upload it to AI or publish it elsewhere.

18 Breaches complaints and reporting

Any unauthorised capture, disclosure, publication, loss, manipulation or use of an image must be reported immediately to the Headteacher, DPO and DSL. The school will take steps to contain the incident, protect the child, request removal, preserve appropriate evidence, assess data-protection risk and make any required report to the Information Commissioner's Office, police, Children's Social Care, platform or other body within the applicable timescale.

Concerns should be raised with the Headteacher. Formal complaints will be handled under the Complaints Policy. Safeguarding concerns and personal-data breaches will be managed immediately and will not wait for the complaints process.

19 Training monitoring and review

Staff induction and regular safeguarding and data-protection training will include safe image capture, consent, individual restrictions, secure storage, public partial-image requirements, parent photography, generative AI, deepfakes and incident reporting. The Headteacher, DSL and DPO will monitor practice, platforms, consent records, incidents and emerging technology. This policy will be reviewed annually and sooner if law, guidance, technology or risk changes.

Appendix 1 Staff checklist before taking or sharing an image

Check	Decision	Action or initials
Is there a clear educational, administrative or communication purpose?	☐ Yes ☐ No ☐ Not applicable	
What is the documented lawful basis? Is specific consent required and current?	☐ Yes ☐ No ☐ Not applicable	
Has the child's view been sought and respected?	☐ Yes ☐ No ☐ Not applicable	
Are there any safeguarding, court, care, adoption or family restrictions?	☐ Yes ☐ No ☐ Not applicable	
Is the device, account and platform authorised?	☐ Yes ☐ No ☐ Not applicable	
Is the image necessary and limited to what is needed?	☐ Yes ☐ No ☐ Not applicable	
Is the child appropriately dressed, comfortable and treated with dignity?	☐ Yes ☐ No ☐ Not applicable	
Does the background reveal names, screens, addresses, medical information or other personal data?	☐ Yes ☐ No ☐ Not applicable	
For public use, is the image partial, non-identifying and non-facial?	☐ Yes ☐ No ☐ Not applicable	
Have names, precise location, routines and metadata been removed?	☐ Yes ☐ No ☐ Not applicable	
Will the image be stored securely and deleted at the correct time?	☐ Yes ☐ No ☐ Not applicable	
Has any AI-enabled editing or processing been avoided?	☐ Yes ☐ No ☐ Not applicable	

Appendix 2 Image and recording consent record

Use only where consent is the appropriate lawful basis. Provide the accompanying privacy information and allow separate choices.

Field	Entry	Field	Entry
Pupil name and class		Academic year	
Parent or carer name		Date issued	
Pupil's views recorded by		Date reviewed	

Proposed use	Choice
Secure parent communication or learning platform	☐ Yes ☐ No
Internal displays in controlled school areas	☐ Yes ☐ No
Public website using partial non-identifying images only	☐ Yes ☐ No
Public school social media using partial non-identifying images only	☐ Yes ☐ No
Printed publicity using partial non-identifying images only	☐ Yes ☐ No
External media under school supervision and partial-image rules	☐ Yes ☐ No

I understand how images may be used, that consent can be withdrawn for future use, and that the school may be unable to retrieve material already printed or copied by others after lawful publication. The school will continue to apply safeguarding restrictions regardless of consent.

Agreement	Signature or name	Field	Entry
Parent or carer signature		Date	
Pupil signature where appropriate		Date	
School record updated by		Date	

Appendix 3 Response to suspected image misuse or deepfake

1. Do not forward, print, download, copy or ask the child to send the image.
2. Reassure the child, avoid blame and establish only what is necessary for immediate safety.
3. Record how the concern came to attention and the platform, account, URL, date and time without reproducing the image.
4. Report immediately to the DSL. Notify the DPO if school-held personal data may have been involved.
5. Do not conduct an investigation or search a device beyond school authority and current guidance.
6. The DSL completes a safeguarding risk assessment and follows KCSIE and the relevant image-sharing guidance.
7. Consider immediate protection, parental contact where safe, platform removal, police, Children's Social Care and specialist referrals.
8. Record decisions, support, referrals and review actions securely.

Appendix 4 Public image examples

Example	School position
Hands completing artwork or practical work	Suitable if names and identifying details are not visible
Back or side view during a group activity	Suitable after checking distinctive features and context
Over-the-shoulder view of learning	Suitable if the work and screen contain no personal data
Wide group image from a distance	May be suitable if individuals are not identifiable
Close-up full-face portrait of a pupil	Not permitted on public-facing channels
Full name beside any pupil image	Not permitted
Image showing a live location or regular route	Not permitted
Image uploaded to an AI editing or generation tool	Not permitted without exceptional written approval following safeguarding and data-protection assessment

Policy approval

Headteacher signature: _____ Date: _____

Chair of Governors signature: _____ Date: _____