



SOCIAL MEDIA POLICY

*Protecting the School's Images from
 AI Manipulation and Abuse*

2026 – 2028

<i>At the time of publishing the following roles were held:</i>	
Head teacher:	Michelle Clark
Designated Safeguarding Lead & Deputies	Michelle Clark, Hayley Fassam, Kerry-Anne Booth, Chrissy Byrne
Social Media Lead:	Michelle Clark
SENDCo	Hayley Fassam

Approved by			
Name:	Alice Vince		
Position:	Chair of Governors		
Signed:			
Version Date:	8 th October 2026	Version No:	1
Review date:	Autumn 2028		

REVIEW SHEET

Version Number	Version Description	Date of Revision/Review
1	Original version	Oct 2026

1. Purpose

The school recognises that photographs and videos shared online can be copied, altered and redistributed using artificial intelligence (AI), including tools capable of creating realistic or misleading images and videos.

This policy establishes clear safeguards for protecting pupils, staff and families from the misuse, manipulation or abuse of school-generated images and video.

The school will take a precautionary approach. Safeguarding, dignity and privacy take priority over publicity, engagement or convenience.

This policy should be read alongside the school's Child Protection and Safeguarding Policy, Data Protection Policy, Social Media Policy, Acceptable Use Policy, Staff Code of Conduct and relevant privacy notices.

2. Scope

This policy applies to:

- all employees, governors, trustees and volunteers;
- agency workers, contractors and visitors who create or handle school images;
- anyone authorised to take, upload, edit, publish or store photographs or video on behalf of the school;
- official school websites, social-media accounts and approved parent or learning platforms;
- photographs, video, audio and other media containing pupils, staff or identifiable members of the school community.

It also applies where school-generated images are supplied to third parties, including photographers, media organisations, event providers and technology suppliers.

3. Core Principles

- Minimise exposure by publishing only images that are necessary and appropriate.
- Avoid unnecessary identification of pupils and other members of the school community.
- Use approved platforms and devices for creating, editing, storing and publishing school images.
- Never knowingly create or publish manipulated images of pupils that could mislead, embarrass, humiliate, sexualise or otherwise cause harm.
- Never use AI tools to manipulate pupil images unless the use has been specifically approved under this policy.
- Treat AI-generated or manipulated sexualised images of children as a safeguarding matter, regardless of whether the original photograph was authentic.
- Respond immediately to suspected misuse, manipulation, impersonation or abusive distribution of school images.
- Preserve evidence appropriately without downloading, copying or redistributing illegal sexual imagery.
- Respect pupil dignity and choice, including a pupil's objection to promotional photography.

- Review this policy regularly as AI capabilities, platforms, risks and relevant guidance develop.

4. Protecting Images Before Publication

4.1 Use the Minimum Necessary Image

The school will consider whether an image needs to be published at all. Where an image is required, staff should consider whether the same communication objective can be achieved using:

- photographs taken from behind;
- photographs from a distance;
- photographs showing hands or work rather than faces;
- photographs where individuals are not readily identifiable;
- photographs of buildings, displays, equipment or completed work;
- illustrations or school-created graphics rather than photographs of pupils.

Publicity must never be the sole reason for exposing a pupil to unnecessary risk.

4.2 Public Identification of Pupils

The school will not normally publish clear, front-facing or otherwise readily identifiable pupil faces on public social media or the public website.

Staff must also consider whether a pupil could be identified through:

- their name;
- voice;
- school uniform;
- class or year group;
- location;
- distinctive clothing or equipment;
- certificates or awards;
- captions;
- background information;
- vehicle registration numbers;
- other pupils or adults appearing in the image.

A face does not need to be visible for an image to constitute identifiable personal data.

4.3 Avoid Providing Material That Facilitates Misuse

Do not unnecessarily publish combinations of information that could make an image easier to misuse, including:

- a pupil's full name alongside their photograph;
- detailed personal information;
- precise locations;
- real-time movements;
- home addresses;
- travel routes;

- accommodation details;
- regular schedules;
- information about a pupil's vulnerability;
- information about safeguarding, health, SEND, behaviour or family circumstances.

School social-media posts must not provide information that could assist someone in locating, identifying or targeting a child.

5. AI Manipulation of School Images

5.1 Prohibited Uses

Staff must not use public or unapproved AI services to:

- alter a pupil's face or body;
- place a pupil into a different environment;
- create a synthetic or fictional version of a pupil;
- change a pupil's clothing;
- remove clothing from a person;
- create sexualised or suggestive content;
- create realistic impersonations of pupils, staff or families;
- generate false quotations, speech or actions attributed to a pupil;
- create misleading videos or audio recordings;
- use facial recognition or emotion-analysis tools for social-media purposes;
- create images designed to ridicule, shame, embarrass or humiliate a pupil;
- upload identifiable pupil photographs for the purpose of experimenting with an AI tool.

IMPORTANT: Removing or obscuring a face after uploading an identifiable pupil image to an unapproved AI service does not make the original upload acceptable.

5.2 Approved AI Use

AI may only be used with school content where:

- the school has approved the particular tool;
- the DPO and IT lead have completed appropriate checks;
- the supplier's data-processing arrangements have been assessed;
- a DPIA has been completed where required;
- the proposed use has a clear educational or operational purpose;
- the tool does not use school images for unauthorised training or secondary purposes;
- the content does not create an unacceptable safeguarding, privacy or reputational risk.
- Where there is uncertainty, do not upload the image.

6. Images of Staff and Adults

The same principles apply to photographs and videos of staff, governors, volunteers, parents and visitors.

The school will not knowingly create or publish manipulated content that:

- falsely represents an individual's behaviour;

- damages their reputation;
- depicts them in a sexualised or humiliating manner;
- falsely attributes statements to them;
- impersonates them;
- creates misleading evidence about them.

Suspected malicious manipulation of staff images should be reported to the Headteacher and, where appropriate, the DPO, DSL or police.

7. Closed Parent and Learning Platforms

The fact that a platform is private or restricted does not mean that images are protected from AI misuse.

Approved closed platforms must therefore be treated with the same care as public channels. The school will:

- use the smallest appropriate audience;
- restrict access to authorised users;
- remove access promptly when circumstances change;
- use platform controls that restrict downloads or sharing where reasonably possible;
- remind parents and carers not to copy, manipulate or redistribute photographs of other children;
- explain that technical restrictions cannot guarantee that content will never be copied or altered.

Public social-media permission and closed-platform permission must remain separate decisions.

8. Staff Responsibilities

All staff who create or handle school images must:

- use school-owned or approved devices;
- use approved storage systems;
- follow the school's image and consent procedures;
- check images before publication;
- report concerns immediately;
- never upload pupil images to unapproved AI services;
- never use personal AI accounts to process school images;
- never send pupil images through personal messaging accounts or personal email;
- delete temporary copies in accordance with the school's retention arrangements.

Staff must not assume that a popular, free or commercially available AI service is safe for school use.

9. Parents, Carers and the Wider School Community

The school will communicate clearly with parents and carers about the risks associated with copying and manipulating children's photographs.

Parents and carers will be asked:

- not to copy or redistribute photographs of other children;
- not to upload school photographs containing other children to AI services;
- not to use photographs of pupils to create altered, synthetic or sexualised material;
- to report suspected misuse of school or pupil images to the school immediately.

The school will explain that once an image has been published online, it may be copied, downloaded, screenshotted or altered by others and that the school cannot guarantee the removal of every copy.

10. Responding to Suspected AI Abuse

Examples include:

- a pupil's photograph appearing on an unfamiliar account;
- a pupil appearing in a fabricated photograph or video;
- an image being altered to make a pupil appear to be doing something they did not do;
- a pupil's face being placed onto another person's body;
- sexualised or nude imagery appearing to involve a pupil;
- fake audio or video appearing to show a pupil making statements;
- an account impersonating a pupil or member of staff;
- threats to publish manipulated images;
- requests for money, information or further images connected with manipulated content.

Staff must:

- Tell the DSL immediately where a child may be at risk.
- Inform the Headteacher and relevant safeguarding or data-protection lead.
- Do not confront the suspected perpetrator.
- Do not forward the material to colleagues, parents or other pupils.
- Do not upload the material to another AI service to determine whether it is genuine.
- Do not ask a child to send the material to the school if doing so would expose them to further harm.
- Preserve relevant information and links safely in accordance with safeguarding and data-protection procedures.
- Follow the school's safeguarding and incident-response procedures.

11. Sexualised or Nude AI-Generated Images of Children

The school treats AI-generated, AI-edited or otherwise manipulated sexualised images involving children as a serious safeguarding concern.

Staff must never:

- download the image;
- screenshot it;
- copy it;
- forward it;
- save it to a personal device;
- upload it to another service;
- ask a child to send it to them;
- share it with colleagues except through an authorised safeguarding process.

If such material is encountered accidentally, staff should stop viewing it and report the matter immediately to the DSL.

The DSL will determine the appropriate safeguarding response in accordance with current national guidance and local procedures.

12. Data Protection and Privacy

Photographs and videos may constitute personal data even where a person's name is not included.

The school will:

- identify the appropriate lawful basis for processing;
- provide appropriate privacy information;
- maintain current permission and objection records;
- respect safeguarding restrictions and do-not-publish decisions;
- minimise the information published;
- retain images only for as long as there is a legitimate purpose;
- use appropriate technical and organisational security measures;
- investigate suspected personal-data breaches promptly.

The school recognises that publishing an image creates risks beyond the school's direct control. Copies may remain on other systems after the school removes the original.

13. Copyright and Ownership

The school must have the appropriate rights to use every photograph, video, graphic, illustration, piece of music or other media that it publishes.

Staff must not assume that:

- an image found online is free to use;
- an image generated by an AI service automatically belongs to the school;
- credit alone provides permission;
- a platform's music library automatically permits organisational or advertising use.

Copyright and licensing must be checked before publication.

14. Social Media Moderation

The Social Media Lead will monitor official accounts on active working days and ensure appropriate cover arrangements are in place.

Content should be removed, restricted or reported where it:

- targets a child;
- shares personal information;
- threatens or harasses an individual;
- contains abusive or discriminatory material;
- appears to involve manipulated or fabricated safeguarding material;
- impersonates a pupil, staff member or the school;

- breaches platform rules or the law.

Fair criticism must not be removed simply because it is negative.

15. Security of School Accounts

Official social-media accounts must:

- use an official school email address;
- have at least two trained administrators;
- use multi-factor authentication;
- use unique passwords held in an approved password manager;
- have managed recovery details;
- have access reviewed at least termly;
- have departing staff removed promptly;
- have connected applications and third-party tools reviewed regularly.

No official account should depend on an individual's personal social-media profile or personal recovery details.

16. Incident Management

Where an image has been published incorrectly, manipulated, misused or obtained through unauthorised access, the school will:

- Contain the incident where possible.
- Remove or restrict school-controlled content where appropriate.
- Secure compromised accounts.
- Notify the Headteacher, DSL, DPO, Social Media Lead and IT as appropriate.
- Record what happened and when it was identified.
- Identify who may have been affected.
- Assess whether the incident constitutes a safeguarding concern or personal-data breach.
- Consider whether external reporting or notification is required.
- Support affected pupils or staff.
- Review controls and training to reduce the risk of recurrence.
- Staff must not delay reporting because they are uncertain whether an image is genuine.

17. Training

Relevant staff will receive appropriate guidance on:

- safe school photography;
- image permissions and restrictions;
- AI manipulation risks;
- identifying potentially manipulated content;
- social-media security;
- safeguarding escalation;
- data-protection requirements;

- copyright and licensing;
- appropriate use of AI tools.

Training will be refreshed when there are significant changes to technology, guidance, legislation or the school's procedures.

18. Pre-Publication AI Safety Check

Before publishing any image, the publisher must confirm every applicable item below. If any answer is NO or UNCLEAR, do not publish.

- ☐ The image has a clear and legitimate school purpose.
- ☐ The correct permission and restriction checks have been completed.
- ☐ No pupil is unnecessarily identifiable.
- ☐ The image does not reveal sensitive information.
- ☐ The image does not reveal a live location or security information.
- ☐ The image has not been processed through an unapproved AI service.
- ☐ No AI manipulation creates a misleading or harmful representation of a person.
- ☐ The school has the necessary copyright or licence.
- ☐ The image is stored securely.
- ☐ The correct person has approved the content where approval is required.
- ☐ The post is respectful, inclusive and appropriate for a public audience.

19. Review and Monitoring

The Headteacher and Social Media Lead will monitor compliance with this policy.

The DPO and DSL will review relevant controls following significant incidents or emerging risks. The policy will be reviewed at least annually and sooner where there is:

- a significant development in AI technology;
- new safeguarding guidance;
- a material legal or regulatory change;
- a serious incident;
- a data breach;
- evidence of misuse of school images;
- introduction of a new social-media or AI platform.

20. Final Principle

FINAL PRINCIPLE: A photograph does not stop being sensitive simply because it has been published.

Before sharing an image, the school must consider not only how it looks today, but also how it could be copied, altered, combined with other information or misused in the future.

Where there is doubt, the school will choose the safer option: do not publish until the risk has been assessed and the appropriate person has approved the content.