Image Use and Image Security Policy

The Vyne Community School

Approved at:	FGB	Date: 20th October 2026
Last reviewed on:	October 2026	
Next review due by:	October 2027	

Contents

1. Purpose Page 2
2. Scope Page 2
3. Core Principles Page 2
4. Consent Page 3
5. Taking Photographs and Video Page 3
6. Publication of Images Page 3
7. High-Profile Individual Achievement Page 4
8. Students Requiring Additional Protection Page 4
9. Website and Social Media Management Page 4
10. Storage and Retention Page 4
11. Image Audit Page 4
12. Artificial Intelligence and Image Manipulation Page 5
13. Responding to Image Misuse or Manipulation Page 5
14. Blackmail or Threats Page 5
15. Staff Training Page 5
16. Parents and Carers Taking Photographs Page 6
17. Students Taking and Sharing Images Page 6
18. Roles and Responsibilities Page 6
19. Monitoring and Review Page 6
20. Related School Policies Page 6
21. Basis of this Policy Page 7

Appendix 1 -Staff Protocol Page 8

1. Purpose

The Vyne Community School is proud to celebrate the achievements, experiences and contributions of its students. Photographs and video can provide an important record of school life and help communicate the character and values of our school to parents, carers and the wider community.

Digital images of children and young people can, however, be copied, downloaded, scraped from websites and social media, shared without consent or manipulated using artificial intelligence. Manipulation can include the creation of sexualised or abusive imagery. Poor image security may also expose personal information or location data and create safeguarding, privacy and blackmail risks.

The school therefore adopts a safeguarding-first approach to the creation, storage and publication of images of students. Safeguarding children and young people is the highest priority when deciding whether and how images should be used.

This policy enables the school to continue celebrating school life while reducing unnecessary exposure of identifiable images of children and young people.

This policy applies to school staff by recognising that staff have the right to request the removal of their photo from public facing sites if they are not happy with the risks.

2. Scope

For the purposes of this policy, an image includes photographs, video recordings, screenshots and other visual recordings from which an individual may be identifiable.

The policy applies to images created, commissioned, stored or published by the school, including those used on the school website, official social media accounts, newsletters, prospectuses, displays, presentations, press releases, promotional material and other digital platforms. It also applies to staff taking photographs or recordings as part of their professional role.

It does not replace the school's safeguarding procedures relating to children sharing nude or semi-nude images, although an incident may fall within both sets of procedures.

3. Core Principles

Before creating or publishing an image of a student, staff should ask: ***Is an identifiable image of the student actually necessary?***

The school will apply the following principles:

- safeguarding takes precedence over publicity or promotional considerations;
- the minimum amount of identifiable information necessary will be published;
- an identifiable photograph will only be used where there is a legitimate purpose for doing so;
- alternatives such as photographs from behind, over the shoulder, at a distance, group/action photographs or images focused on activities and work should be considered;
- student images and full names will not normally be published together;
- consent does not remove the school's responsibility to assess whether publication is safe and appropriate;
- if consent is uncertain the image will not be used;
- images will not be retained or published for longer than permitted under Data Protection Policy; and
- particular care will be taken where a student has additional safeguarding or privacy considerations.

4. Consent

The school will maintain an appropriate system for recording parental/carer consent for the use of student photographs and video.

Consent arrangements will explain the purposes for which images may be used; the types of platform on which images may appear; that online images can potentially be copied or manipulated by others; the measures the school takes to reduce these risks; and how consent can be withdrawn.

Consent will be reviewed periodically and particularly at appropriate transition points.

Where a student is sufficiently mature to understand the decision, their wishes will also be respected. A student should not be required to participate in a photograph or video where they make clear that they do not wish to do so, even where parental consent exists.

Withdrawal of consent will apply to future use and, where reasonably practicable, existing school-controlled online material will be reviewed and removed.

5. Taking Photographs and Video

Images of students for school purposes should normally be taken using school-authorised equipment or systems. Staff must not routinely use personal devices to photograph or record students. Where exceptional circumstances make this necessary, this must be authorised by an appropriate senior leader and the image must be transferred promptly to an approved school system and removed from the personal device.

Staff must not:

- take photographs in circumstances where students have a reasonable expectation of privacy;
- take images which could reasonably cause embarrassment or compromise a student's dignity;
- stage or request photographs that unnecessarily expose personal information;
- photograph a student where safeguarding information indicates that doing so presents a risk; or
- retain school photographs of students within personal photograph libraries, personal cloud storage or personal social media accounts.

6. Publication of Images

The school will adopt a principle of minimum necessary identification when publishing images. For public-facing platforms such as the school website and open social media accounts, the school should normally:

- favour photographs showing students engaged in activities rather than formal face-on portraits;
- use group, distance, side-on, over-the-shoulder or similar images where these achieve the purpose;
- avoid publishing a student's full name alongside an identifiable photograph;
- consider whether an image needs to show a student's face at all;
- use appropriately reduced-resolution images for online publication;
- ensure unnecessary metadata, including EXIF location, device and timestamp information, is removed;
- avoid imagery that unnecessarily reveals a student's routine, location or other personal information; and
- use appropriate privacy settings where content does not need to be publicly accessible.

7. High-Profile Individual Achievement

There will be occasions where celebrating an individual student's achievement - for example examination success, sporting achievement, an award or representation of the school - reasonably involves publishing their name and photograph.

This may take place where appropriate consent has been obtained and the school considers publication proportionate and safe. The existence of consent will not automatically mean that publication should occur. Staff should consider the student's age, the nature of the achievement, the intended audience, the platform being used and any known safeguarding circumstances.

8. Students Requiring Additional Protection

Some students may face particular risks if their photograph, identity or location becomes publicly available. This may include, but is not limited to, children in care, students subject to particular safeguarding arrangements, children involved in family proceedings or students whose location needs to remain confidential.

The DSL may direct that photographs of an individual student must not be taken or published regardless of general parental consent. Staff must follow safeguarding information provided to them and must not attempt to determine independently whether publication is safe.

9. Website and Social Media Management

Only authorised staff may publish images through official school channels. Images must not be published through personal staff social media accounts or unofficial school-related accounts.

Privacy settings should be used where appropriate to restrict unnecessary access to content.

The school recognises that once an image is published openly online it may be copied or downloaded by third parties and the school cannot guarantee that it will remain under the school's control. Decisions about publication must therefore be based upon the potential consequences of public availability, rather than an assumption that an image will remain only on the original platform.

10. Storage and Retention

Images containing identifiable students constitute personal information and must be handled securely. Images will:

- be stored only within authorised school systems;
- be accessible only to those who have a legitimate reason to access them;
- not normally be retained indefinitely;
- be deleted when there is no longer a legitimate purpose for retaining them; and
- be included within the school's normal data protection and retention arrangements.

11. Image Audit

The school will undertake a termly review of publicly available student imagery, including the school website and official social media platforms. The review will consider whether:

- images remain necessary and appropriate;
- consent remains valid;
- students pictured are still members of the school community;
- images reveal unnecessary identifying information;
- older photographs should be removed or replaced; and
- changes in technology or safeguarding risks require different controls.

Images of students who have left the school should normally be removed from prominent/current website and promotional content as materials are refreshed.

12. Artificial Intelligence and Image Manipulation

No member of staff or student may use an image of another identifiable member of the school community within an AI image-generation, image-editing or face-manipulation service without an authorised educational purpose and appropriate permission.

Creating, requesting, possessing or sharing manipulated imagery intended to sexualise, humiliate, threaten, impersonate, bully or otherwise harm another person will be treated as a serious safeguarding matter. Where students are involved, the school's behaviour, safeguarding and online safety procedures will apply.

Where an image is sexual or abusive, staff must not investigate by asking for the image to be forwarded or shared further. The matter must immediately be referred to the DSL.

13. Responding to Image Misuse or Manipulation

Any suspected misuse, unauthorised sharing, AI manipulation, sexualisation or threatened publication of an image of a student must be reported immediately to the DSL or, where appropriate, the Headteacher. The immediate response will prioritise the student's safety, dignity and emotional wellbeing.

The school will, as appropriate:

- safeguard the student and assess immediate risk;
- notify the DSL and appropriate senior staff;
- preserve relevant evidence securely without unnecessarily copying, downloading or further distributing illegal material;
- remove the school's original publicly accessible image where appropriate;
- record the incident and undertake a safeguarding/data protection risk assessment;
- inform parents/carers where appropriate;
- seek advice from or make referrals to relevant safeguarding, police or specialist agencies;
- request removal from websites or platforms where appropriate; and
- consider whether a personal data breach has occurred and follow the school's data protection procedures.

14. Blackmail or Threats

If the school, a student or member of staff receives a threat or demand connected with manipulated or intimate imagery, the matter must immediately be escalated to the Headteacher and DSL.

15. Staff Training

Relevant staff will receive information and training on:

- safe creation and publication of student images;
- consent;
- image security and metadata;
- risks associated with AI image manipulation;
- recognising image-based abuse; and
- reporting and safeguarding procedures.

16. Parents and Carers Taking Photographs

The school recognises that parents and carers may wish to photograph their own children at appropriate school events, however due to safeguarding considerations the school will restrict or prohibit photography and recording. Parents and carers will be reminded that they should not post photographs taken at school events onto their social media.

17. Students Taking and Sharing Images

Students must not photograph, video or record another person in school.

Students must not upload, manipulate, alter or distribute an image of another student or member of staff in a manner that is abusive, sexualised, discriminatory, threatening, humiliating or likely to cause harm.

The use of AI does not reduce responsibility for the resulting content. AI-generated or AI-manipulated content will be addressed according to its nature and impact in the same way as other harmful digital content. Serious incidents will be managed through safeguarding procedures and may be referred to the police or other agencies.

18. Roles and Responsibilities

- The Headteacher has overall responsibility for ensuring appropriate arrangements are in place for the safe use of images.
- The Designated Safeguarding Lead is responsible for safeguarding responses to image misuse, manipulation and image-based abuse.
- The Data Protection Officer will advise on data protection, personal data breaches, retention and information governance where required.
- Staff responsible for communications, website and social media must ensure that published imagery complies with this policy.
- All staff are responsible for following this policy and immediately reporting concerns.

19. Monitoring and Review

This policy will be reviewed annually, or sooner where:

- there is a significant image-security or safeguarding incident;
- relevant legislation or statutory guidance changes;
- emerging AI technology creates materially different risks; or
- an audit identifies weaknesses in existing practice.

Following any significant incident, the school will consider whether imagery, consent arrangements, technical controls, staff training or associated policies require amendment.

20. Related School Policies

- Child Protection and Safeguarding Policy
- Online Safety Policy
- Data Protection Policy
- Behaviour Policy
- Staff Code of Conduct
- Acceptable Use / ICT Policy
- Social Media Policy
- Privacy Notices

21. Basis of this Policy

This policy has been developed with reference to Protecting your setting's images from AI manipulation and abuse: Guidance for education settings and organisations working with children and young people, produced by the UK Online Harms Early Warning Working Group. The guidance emphasises safeguarding-first image use, data minimisation, consent, secure publication and storage, regular image audits, staff training and clear procedures for responding to image-based abuse and AI manipulation.

Appendix 1: Staff Protocol

Taking, storing and publishing images of students

5 CHECKS BEFORE YOU PUBLISH
Do we need this image? | Do we have consent? | Does it identify more than necessary?
Could we use a safer image or angle? | Has metadata been removed?

Before taking an image

- Check that there is a legitimate school purpose and that an identifiable image is necessary.
- Check the student's image consent status and any safeguarding restrictions.
- Respect the student's own wishes: do not require a student to be photographed if they object.
- Use school-authorised equipment or systems. Personal devices must not routinely be used.

When taking an image

- Prefer activity, group, distance, side-on or over-the-shoulder images where these meet the purpose.
- Avoid unnecessary close-up, face-on portraits for public use.
- Protect dignity and privacy; never photograph in circumstances where a student has a reasonable expectation of privacy.
- Avoid capturing personal information, timetables, addresses, location clues or other sensitive material in the background.

Before publishing

- Do not normally publish a full student name alongside an identifiable photograph.
- Use the minimum necessary identification and consider whether the face needs to be visible at all.
- Use reduced-resolution imagery where appropriate and ensure EXIF/location/device/timestamp metadata is removed.
- Use privacy controls where content does not need to be public.
- Only authorised staff may publish through official school channels.

Storage and deletion

- Store images only on authorised school systems and only for as long as needed.
- Do not retain student images in personal photo libraries, personal cloud storage or personal social media.
- Delete or replace outdated images as school content is refreshed.

If an image is misused, manipulated or sexualised

- Report immediately to the DSL / Headteacher.
- Prioritise the student's safety, dignity and emotional wellbeing.
- Do not ask anyone to forward or further share sexual or illegal imagery.
- Preserve relevant evidence securely and seek safeguarding/police advice as appropriate.
- Do not engage with blackmail demands or make payment.
- Where a child is at immediate risk of significant harm, call 999.

If in doubt: do not publish. Ask the DSL or an authorised senior leader.