Vernham Dean Gillum's C of E Primary School

Policy on Using Photos and Videos

(Statutory Safeguarding, Image Security & Zero-Online Pupil Image Policy)

Approval Date: September 2026

Review Date: September 2027 (Termly/Biannual)

Status: Statutory Policy

1. Purpose and Scope

This policy outlines the responsible management, sharing, and protection of photographs and videos featuring children and young people across Vernham Dean Gillum's C of E Primary School's online platforms, including the school website, public social media channels, digital marketing materials, and internal learning spaces.

Ensuring the security of student imagery is a core component of our statutory safeguarding duty under Keeping Children Safe in Education (KCSIE 2026), Working Together to Safeguard Children, and UK GDPR / Data Protection Act 2018. This policy aims to protect our school community from modern digital threats, including automated web-scraping, unauthorized image sharing, data breaches, and the malicious use of Artificial Intelligence (AI) tools (such as 'nudification' apps and deepfake generators) to manipulate student images into Child Sexual Abuse Material (AI CSAM).

2. Online Image Policy (Zero-Pupil Image Approach)

To ensure the absolute highest standard of safeguarding and data privacy, Vernham Dean Gillum's C of E Primary School operates a strict Zero-Online Pupil Image Policy across all public and semi-public digital platforms (including the school website, official social media accounts, digital marketing, and local press releases).

- **No Identifiable Pupil Imagery**: Photos or videos showing identifiable student faces will never be uploaded to any public online platform.
- **Focus on Learning & Environment**: Digital communications will showcase student work, classroom displays, school facilities, group activity from a distance, or perspective shots (e.g., over-the-shoulder, back-of-head, or blurred/silhouette images) where individual children cannot be recognised.
- **Names and Identities**: Student names will never be published alongside photos or videos of any kind.
- **Offline/Internal Exceptions**: Photos of pupils may still be taken on school-owned devices for internal assessment, internal displays within the physical school building, or secure internal reporting, subject to standard written parental consent forms, secure local network storage, and strict data retention schedules.

3. Content Audits and Data Retention

- **Regular Audits**: The school will conduct documented termly or biannual audits of all imagery displayed on the website, social media, and promotional materials to ensure full compliance with the Zero-Pupil Image Policy.
- **Community Transitions**: Images of any children or young people who are no longer members of the school community must be promptly removed or replaced upon their exit.
- **Storage Limitation**: In line with UK GDPR data minimisation principles, personal data and student imagery will only be retained for as long as strictly necessary and in accordance with the school's Data Retention Schedule.

4. Staff Training and Incident Response

Image security awareness and data handling practices are an essential component of regular staff safeguarding training at Vernham Dean Gillum's C of E Primary School. All staff will be trained to recognise and respond to incidents of image-based abuse, including non-consensual sharing, AI image manipulation, online grooming, and cyber-blackmail threats.

5. Protocol for Image Misuse, Alteration, or Abuse

If a student or staff image is found to have been compromised, altered, or targeted for extortion or blackmail, staff must execute the following protocol immediately:

> **School Incident Protocol: Image Misuse & Abuse**
>
> *If an image of a student or staff member is manipulated, shared without consent, or targeted for blackmail, immediately activate the four-step protocol below:*
>
> **1 CONTAIN & ESCALATE**
>
> - Preserve Evidence: Do NOT delete or further share any communication or criminal images relating to the incident.
> - Secure Storage: Retain and store all digital evidence securely (e.g. encrypted folder) to hand over to local law enforcement.
> - Remove Public Access: Immediately ensure the original version of the compromised image is taken down from public websites, social media, or portals.
> - Internal Notification: Notify the Designated Safeguarding Lead (Headteacher) or Deputy DSL immediately.
> - Document the Breach: Log full details in CPOMS/incident logging system, perform a risk assessment, and notify the Information Commissioner's Office (ICO) / LADO if statutory thresholds are met.
>
> **2 DO NOT ENGAGE**
>
> - CRITICAL WARNING FOR EXTORTION: If approached with demands or blackmail attempts, do NOT engage with the perpetrator or pay any ransom. Paying a ransom can be illegal under UK law and exacerbates extortion risks.

3 REPORT IT

- Local Police: Report immediately to Hampshire Constabulary if threats involve sexual extortion, harassment, or AI-generated Child Sexual Abuse Material (AI CSAM). Call 999 if a child is at immediate risk.
- Under 18s Protection: Assist pupils under 18 in using 'Report Remove' (Childline/IWF) or 'Take It Down' (NCMEC) to confidentially remove underage intimate images from the web.
- Over 18s / Staff Protection: Utilize 'Stop NCII' (Non-Consensual Intimate Images) or the Revenge Porn Helpline for affected staff or adult students.
- Platform Escalation: Submit formal takedown requests directly to web hosting services and social media platforms.

4 SUPPORT & PREVENT

- Prioritise Wellbeing: Maintain pupil safety, dignity, and psychological wellbeing as the top priority throughout.
- Inform Families: Keep parents/carers fully informed with transparent, actionable next steps.
- Staff Support: Direct affected staff to internal occupational health, the Professionals Online Safety Helpline, or Stop It Now.
- Prevent Recurrence: Audit all school web platforms, tighten parental consent mechanisms, update digital safeguards, and implement technical measures (e.g., image metadata scrubbing and watermarking).

6. Essential Helplines & Reporting Tools

The following statutory and specialized resources must be utilized when managing digital image incidents:

Target Audience	Tool / Helpline	Purpose & Support Scope
Under 18s (Pupils)	Report Remove (Childline/IWF) Take It Down (NCMEC)	Confidential web tool to take down and prevent sharing of underage intimate images.
Over 18s / Staff	Stop NCII Revenge Porn Helpline	Removal of adult non-consensual intimate images and digital victim support.
School Staff & Leaders	Professionals Online Safety Helpline Stop It Now!	Dedicated advisory helpline for school staff managing complex online safety incidents.
Emergency & Police	Hampshire Police / Call 999 Hampshire LADO (01962 876364)	Immediate risk intervention, reporting criminal AI CSAM creation, and statutory LADO referrals.