Pupil Online Media Policy

A local school policy for
Polehampton CE Schools and Nursery

KEYS
Academy Trust

Version control summary and overview details

Local school policy • This is a policy which the Board of Trustees has delegated to the Local Governing Body to agree on and approve. • LGBs have minuted that they have approved this policy.	
Version control V01 – creation of new policy, in line with recommendations from national agencies and organisations. • Consideration of the need for identifiable pupil images in publications. • Consideration of the risks to schools of posting media of pupils online.	
Reviewed by (School Lead)	Phil Sherwood, Executive Headteacher
Approved by LGB:	Polehampton LGB
Date of approval:	Autumn 2026
Date of next review:	Autumn 2027

TKAT vision
We are a family of distinctive schools at the heart of the diverse communities we serve. In line with our Christian ethos, we aspire to excellent learning and pastoral care for pupils and staff and are committed to being open and welcoming to all.

School vision
At Polehampton CE Schools and Nursery, our vision is "Let your light shine" (Matthew 5:16). Jesus reminded us in Matthew's gospel that we are lights for the world. As we seek to follow him, we can share his light with others and change the world. Supported by our school values of gratitude, friendship, perseverance, forgiveness, honesty and compassion, we seek to help pupils make positive choices in all they do. We follow our Christian values to enable everyone in our school community to let their light shine.

Key areas of note
Please note the following, which will be applicable throughout the policy:
- Any reference to 'everyone' to staff, trustees, local governors and pupils.
- Any reference to 'we' should be read as The Keys Academy Trust.
- Any reference to 'parents' should be read as 'parents, carers and guardians'.

Table of Contents

1. Purpose 4
2. Aims 4
3. Scope 4
4. Legal and regulatory framework 5
5. Core principles and considerations 5
6. Governance and responsibilities 6
7. Lawful, fair and transparent use 6
8. Permission and pupil assent 6
9. Taking and selecting media 7
10. Storage, transfer and access 7
11. Official social media and websites 7
12. Events, parents, visitors and pupils 8
13. Responding to misuse, AI manipulation or image-based abuse 8
14. Training, monitoring and review 9

1. Purpose

1.1 This policy sets out how the school will create, select, store, use, publish, share, retain and delete photographs, video, audio and other media featuring pupils. However, the information will not replace or contradict the expectations of the Trust's Data Protection Policy.

1.2 It places safeguarding before publicity and reduces the risk that pupils' images are copied, scraped, identified, manipulated by artificial intelligence (AI), sexualised, used for blackmail or otherwise abused.

1.3 The school recognises the value of celebrating pupils' learning and achievements. No publication benefit, however, outweighs a foreseeable safeguarding or privacy risk to a child.

2. Aims

2.1 The aims of this policy are as follows:

a) Protect pupils' safety, dignity, privacy and wellbeing, including in online spaces.
b) Use the minimum amount of identifiable pupil imagery needed for a clear and legitimate purpose.
c) Apply UK Data Protection 2018 (DPA 2018) and GDPR principles and an appropriate lawful basis to every use.
d) Give parents clear choices and respect pupils' views and developing autonomy.
e) Establish consistent, secure practice across all the school and its staff, contractors and channels.
f) Reduce opportunities for image scraping, AI manipulation, image-based abuse and location or routine tracking.
g) Respond promptly, lawfully and compassionately when an image is lost, misused, altered or threatened.

3. Scope

3.1 This policy applies to governors, employees, agency staff, volunteers, contractors, visitors and any person creating or handling media on behalf of the Trust. It covers pupils in school, nursery, wraparound provision, trips, residential visits, performances, sporting events, remote learning and school/Trust activities.

3.2 "Media" includes still photographs, video, livestreams, audio recordings where a pupil is identifiable, screenshots, thumbnails, scanned work containing identifying information, CCTV extracts used for communications, and AI-generated or AI-edited material based on a pupil's likeness or voice. It covers Trust- and school-controlled websites, learning platforms, parent communication systems, email, printed publications, press activity and social media.

3.3 Parents' and visitors' personal photography at events is addressed within this policy in a separate section. CCTV used for security is principally governed by the Trust's CCTV and data protection arrangements, but any wider use or publication falls within this policy.

3.4 It is recognised that, due to the age of the pupils at the school, consent/permission/assent will be gained through parents' agreement. However, pupils in Year 6 may be asked their views as well.

4. Legal and regulatory framework

4.1 The Trust will have regard to the following, as amended or replaced:

a) UK General Data Protection Regulation (UK GDPR), including the principles of lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.
b) Data Protection Act 2018.
c) Children Act 1989 and Children Act 2004, including duties to safeguard and promote children's welfare.
d) Education Act 2002, section 175, where applicable, and the safeguarding requirements applying to academies through the Education (Independent School Standards) Regulations 2014 and funding arrangements.
e) Keeping Children Safe in Education (KCSIE), using the version in force at the relevant time.
f) Protection of Children Act 1978 and Criminal Justice Act 1988 concerning indecent images of children, including images created or altered using AI.
g) Sexual Offences Act 2003, where image-related conduct amounts to sexual offending.
h) Human Rights Act 1998, particularly respect for private and family life.
i) Copyright, Designs and Patents Act 1988 and any applicable performer rights.

4.2 This policy should be read with the Trust's child protection and safeguarding, online safety, data protection, privacy notice, records retention, acceptable use, social media, staff code of conduct, CCTV and incident response policies.

4.3 Whilst not part of a legal framework, the following were used as references for the creation of this policy:

a) Image guidance for education settings - UK Safer Internet Centre
b) Protecting your setting's images from AI manipulation and abuse
c) New guidance for parents and carers as AI-manipulated images of children become a growing concern - National Crime Agency.

5. Core principles and considerations

5.1 **Safeguarding first:** Before taking or using media, staff must consider whether it could expose a child's identity, location, routine, vulnerability or protected status, or be readily manipulated or misused.

5.2 **Necessity:** Use identifiable pupils only where the purpose cannot reasonably be achieved with non-identifiable alternatives, such as hands at work, over-the-shoulder images, distant group images or pupils' work.

5.3 **Least identifiable form:** Do not pair a recognisable face with a full name, class, precise location (e.g. remove EXIF and other metadata, including geolocation, device and timestamp information), timetable or other information that makes the child easier to identify or locate.

5.4 **Respect and dignity:** Media must show pupils positively and appropriately. It must not be embarrassing, sexualised, intrusive or likely to cause distress now or later.

5.5 **No assumption of safety:** A privacy setting, watermark or consent form reduces some risks but cannot prevent copying, screenshots, scraping or AI manipulation.

5.6 **Child voice:** A pupil's refusal must normally be respected even where parental permission exists. Staff must not pressure a pupil to be photographed or recorded.

6. Governance and responsibilities

6.1 Headteacher

a) Implements this policy locally and approves official channels and authorised users.
b) Takes overall responsibility for the policy and media taken/used.

6.2 **Operations Manager**

a) Ensures permissions, pupil vulnerability information and publication decisions are checked.
b) Ensures regular image audits and prompt removal of outdated material.

6.3 Designated Safeguarding Lead (DSL)

a) Advises on children for whom identification or publication creates additional risk.
b) Leads the safeguarding response to misuse, alteration, sexualisation, threats or blackmail.
c) Liaises with children's social care, police and specialist services where appropriate.

6.4 Data Protection Officer (DPO)

a) Advises on lawful basis, transparency, data protection impact assessments (DPIAs), processors, international transfers and breaches.
b) Assesses whether an incident must be reported to the Information Commissioner's Office (ICO) and/or affected individuals within the statutory timescales.

6.5 Staff and authorised users

a) Use only approved devices, accounts, storage and workflows.
b) Check permissions and safeguarding restrictions before capture and publication.
c) Report mistakes or concerns immediately.
d) Never use pupil media for personal purposes, portfolios or personal social media.

7. Lawful, fair and transparent use

7.1 A photograph or recording is personal data where a pupil is identified or identifiable. The school will follow the Data Protection Policy and UK DPA 2018 / GDPR for processing.

7.2 It is recognised that most purposes will be under consent given by parents.

7.3 The school may take or use images without publicity consent where this is necessary for education, safeguarding, identification, evidential, legal or operational purposes and another lawful basis applies. Such images must not be repurposed for publicity without a separate lawful basis and the required permission.

8. Permission and pupil assent

8.1 Obtain permission through an accessible form that distinguishes internal use, secure platforms (i.e. Teams), website/publications, social media, press and third-party promotional use. However, some of these aspects may be grouped together based on our school's choice/decision in how it manages its media.

8.2 Explain – to parents – the purpose, likely audience, retention approach, foreseeable risk of copying or AI

manipulation, protective measures, and how to withdraw consent.

8.3 Remind parents of their ability to review and renew their choices on consent at least annually and at key transition points, and update them promptly if/when circumstances change.

8.4 Seek parents' informed consent. If applicable to ask pupils, ask for consent in language appropriate to age and understanding. Re-check consent at the point of capture where practicable.

8.5 Record and communicate to relevant school staff any withdrawals promptly. Withdrawal does not make earlier lawful processing unlawful and cannot guarantee recall of copies already lawfully distributed, but the school will stop new use and remove material it controls where reasonably practicable.

8.6 Where adults share parental responsibility or there is disagreement, the school will seek to work with the parents to agree a resolution. A court order or known safeguarding restriction must be followed.

9. Taking and selecting media

9.1 Before capture, the responsible member of staff must consider the purpose, intended audience and storage location, and check the current permission record and any DSL restriction.

9.2 Use school-managed equipment, unless given specific agreement by a member of the senior leadership team, and whilst following the Online Safety Policy's expectations.

9.3 Do not use facial recognition, biometric categorisation, emotion recognition, face-swapping, voice cloning, generative fill or other AI processing involving pupils unless separately approved following a DPIA, safeguarding assessment, clear lawful basis and senior authorisation. See the Trust's AI Policy for further details on this.

10. Storage, transfer and access

10.1 Transfer media promptly to approved school storage and delete it from the capture device once transfer is verified and no longer needed there.

10.2 Apply the Trust retention schedule. Delete rejected, duplicate, test and out-of-date files securely.

10.3 Treat lost devices, misdirected messages, unauthorised access and unintended publication as potential personal data and safeguarding incidents and follow the Data Protection Policy.

11. Official social media and websites

11.1 Only agreed staff may publish through school-operated accounts, using approved devices and account security controls.

11.2 Settings must be reviewed regularly, but public social media must always be treated as fully public, permanent and capable of copying.

11.3 Comments, direct messages, tags and mentions must be moderated. Staff must not engage publicly about individual pupils.

12. Events, parents, visitors and pupils

12.1 The school may allow parents to take images for personal use at specified events. It may prohibit or restrict photography where needed to protect pupils, comply with venue or performance rights, or enable the event to proceed safely. Restrictions will be explained clearly and must be followed.

12.2 The school will ask families not to post identifiable images of other people's children online without the permission of those children's parents and, where appropriate, the children themselves.

12.3 Staff must not promise that the school can control personal images lawfully taken by others, but will act on safeguarding concerns and breaches of event conditions.

13. Responding to misuse, AI manipulation or image-based abuse

13.1 Any concern that pupil media has been copied, altered, sexualised, shared without authority, used to impersonate someone, or connected with threats or blackmail is both a safeguarding concern and a potential data/security incident.

13.2 **Protect the child:**

a) Notify the DSL and headteacher immediately.
b) Address immediate safety, dignity, emotional wellbeing and any risk of further sharing.
c) Call 999 if a child is at immediate risk of significant harm.

13.3 **Contain:**

a) Remove or restrict the original school-controlled source where appropriate.
b) Secure accounts and preserve relevant logs.
c) Do not contact, negotiate with or pay a blackmailer.

13.4 **Preserve evidence safely:**

a) Do not forward, copy, print, download or ask a child to send illegal sexual imagery.
b) Do not delete relevant communications unless advised.
c) Record URLs, usernames, dates and actions without unnecessarily viewing imagery.
d) Seek police/DSL advice on secure preservation.

13.5 **Report and assess:**

a) The DSL considers referrals to police and children's social care.
b) The DPO assesses the personal data breach, documents the decision and makes any required ICO or individual notification.
c) Report illegal child sexual abuse material to the appropriate police/IWF route; do not submit known illegal material through ordinary platform forms.

13.6 **Remove:**

a) Use platform reporting and appropriate specialist services.
b) Support under-18s and their parents.
c) Follow current guidance specific images to ensure they are appropriately managed.

13.7 **Support and communicate:**

a) Involve parents/carers unless doing so would increase risk or conflict with safeguarding advice.
b) Provide non-blaming, age-appropriate support and consider support for affected staff.

13.8 **Review:**

a) Audit other published media, permissions and technical controls.
b) Record lessons learned.
c) Update training and risk assessments.

13.9 The creation, possession or distribution of an indecent image of a child is illegal whether the image is photographic, pseudo-photographic or AI-generated. Staff must follow DSL and police guidance and avoid creating additional copies.

14. Training, monitoring and review

14.1 All staff receive induction and regular refresher training (either in person, via training materials or the publication of policies) on safe capture, approved systems, permission checks, metadata, AI manipulation, image-based abuse and incident reporting.

14.2 Pupils receive age-appropriate teaching about consent, privacy, AI-generated and manipulated media, reporting and help-seeking.

14.3 The headteacher, SLT and DSL will review compliance and emerging risks at least annually. Material changes in law, KCSIE, technology, platform practice or incidents trigger an earlier review.

14.4 Breaches of this policy may be managed under disciplinary, safeguarding, contractual or behaviour procedures as appropriate.