A place for fun, creativity, friendship, ambition and discovery

Social Media and Artificial Intelligence Policy

1. Purpose and scope

Social media and artificial intelligence (AI) are part of everyday life and can bring benefits to communication, learning and creativity. They also create risks, including online bullying, inappropriate contact, misinformation, impersonation, the misuse of images and the loss of personal information.

This policy sets out the expectations for the use of social media and AI by everyone in the Langham Village School community: pupils, staff, parents and carers, governors, volunteers and other people working on behalf of the school. It applies to use both during and outside school hours where this may affect pupils, members of the school community or the reputation and effective running of the school.

For the purposes of this policy, AI includes generative tools that create or alter text, images, audio, video or other digital content, including chatbots, image generators, voice cloning and deepfake tools.

2. General principles

- Everyone should communicate respectfully and responsibly online, remembering that content can be copied, shared and retained even when an account or post is private or later deleted.
- Information shared online remains subject to applicable data protection, copyright, confidentiality, safeguarding and defamation requirements.
- No one should use social media or AI to bully, harass, threaten, impersonate, humiliate or target another person.
- Content should not be assumed to be genuine simply because it looks or sounds realistic. AI-generated content may be inaccurate, misleading, biased or deliberately harmful.
- Concerns about online safety, social media or AI misuse should be reported to the school promptly and handled in line with safeguarding and other relevant school policies.

A. Use of social media and AI by pupils

- While at school, pupils must not access social networking sites or use AI tools unless a member of staff has given permission for a specific educational activity.
- Pupils and parents are reminded that some social media platforms and AI tools have age restrictions and are not appropriate for primary-aged children. These restrictions must be followed.
- Pupils must not create, request, share or forward hurtful, threatening, discriminatory, sexualised or humiliating content, including AI-generated images, videos, voice recordings or messages.
- Pupils must not use AI tools to make or alter images or recordings of another pupil, member of staff or other person without permission. This includes face-swapping, voice cloning and deepfakes.

- Pupils should not share personal information, photographs, passwords, school details or identifying information about themselves or others with online services or AI tools.
- If pupils see something upsetting, receive an inappropriate message, or discover that an image, video or recording of them has been manipulated or shared, they should tell a trusted adult. They should not retaliate or forward the content.

The school will teach age-appropriate online safety, including how to recognise misleading content, protect personal information, behave respectfully and seek help. Any pupil use of AI for a school activity must be directed and supervised by a member of staff.

B. Use of social media by employees in a personal capacity

Staff may use personal social media accounts, but must protect their professional reputation, the reputation of the school and the privacy and safety of the school community.

- Staff should familiarise themselves with privacy settings and review them regularly. Privacy settings reduce visibility but do not guarantee that content will remain private.
- Staff must not post, share, like or endorse content which could bring the school into disrepute; lead to valid parental complaints; be derogatory towards the school, colleagues, pupils, parents or governors; call into question their suitability to work with children; or breach professional standards.
- Staff must not form online friendships with pupils or communicate with pupils through personal social media accounts. Any necessary online communication with pupils must take place only through school-approved channels and in accordance with safeguarding procedures.
- Staff must not post photographs, videos, names or identifying information about pupils, school events or colleagues without the Headteacher's prior approval and any required permissions.
- Staff must not use personal accounts to discuss individual pupils, families, colleagues, safeguarding matters or confidential school business.
- Staff must not use AI tools to create or alter content about pupils, families or colleagues in a way that could identify, embarrass, misrepresent or harm them.
- If staff become aware of content or online activity that may breach this policy or raise a safeguarding concern, they should report it to the Headteacher or Designated Safeguarding Lead (DSL) promptly.

A breach of this policy may result in disciplinary action. Inappropriate use by employees should be referred to the Headteacher in the first instance. Where the concern relates to the Headteacher, it should be referred to the Chair of Governors.

C. Use of social media and AI for school purposes

- All social media accounts, platforms and services used on behalf of the school must be approved in advance by the Headteacher.
- Only authorised staff may publish content on official school accounts. Posts must be appropriate, accurate, respectful and consistent with the school's values and communications procedures.
- Staff may use an AI tool to support routine tasks such as drafting or improving general communications, planning content or creating non-identifying illustrations, provided the tool has been approved for school use where required.
- Staff must not enter pupils' or families' names, contact details, photographs, videos, voice recordings, safeguarding information, SEND information, medical information, assessment information or other personal or confidential data into a public or unapproved AI tool.

- Any proposed use of personal data in an AI tool must be discussed with the Headteacher and the school's Data Protection Officer (DPO) before use. Staff must not assume that a tool is safe because it is free, widely used or has privacy settings.
- AI-generated material must be checked by a member of staff before it is used or shared. Staff remain responsible for checking accuracy, suitability, bias, copyright and whether the content could be misleading or inappropriate.
- AI must not be used as a substitute for professional judgement, safeguarding decisions, assessment decisions or direct communication with families.
- Staff should be transparent where AI has materially contributed to content where this would help avoid misleading the audience. AI-generated images or media must not be presented as genuine photographs or recordings of real school events or people.
- Photographs or recordings of pupils must not be uploaded to public AI image, video or voice tools for editing, enhancement, animation or generation. Any exceptional proposal must receive prior written approval from the Headteacher and DPO and meet safeguarding, consent and data protection requirements.
- Staff must respect copyright and intellectual property. AI-generated content should not reproduce protected material or use another person's image, voice or work inappropriately.

D. Comments and content posted by parents and carers

- Parents and carers are made aware of their responsibilities through this policy, the school website, letters and newsletters.
- Parents and carers are asked not to post photographs or videos of pupils other than their own children on social media unless they have the permission of the parents or carers of every other child shown.
- Parents and carers should not upload photographs, videos or identifying information about other pupils, staff or families to AI tools, or use AI to alter, imitate or create content depicting them.
- Parents and carers are asked to raise queries, concerns or complaints directly with the school so that these can be addressed appropriately, rather than posting them on social media.
- Parents and carers should not post malicious, threatening, discriminatory or fictitious comments about any member of the school community. This includes sharing or presenting AI-generated or manipulated content as if it were genuine.
- If a parent or carer becomes aware of an online post or AI-generated item that may put a child or member of the school community at risk, they should report it to the school rather than circulate it further.

E. Online bullying, harmful content and AI-related incidents

All cases of online bullying will be dealt with in accordance with the school's Anti-Bullying Policy. This includes bullying carried out through social media, messaging services, games, chatbots or AI-generated content.

Examples of incidents include:

- Cyberbullying, harassment, threats or discriminatory abuse.
- Fake accounts, impersonation or the use of AI to imitate a person's face, voice or identity.
- AI-generated or manipulated images, videos or audio used to embarrass, threaten, sexualise or exploit a person.

- The creation or sharing of false, misleading or defamatory content about a pupil, member of staff, parent, governor or the school.
- Inappropriate contact with a child by another user or an AI application that simulates personal relationships or encourages unsafe behaviour.

Pupils, parents and staff should report concerns to the Headteacher or DSL as soon as possible. The school will consider safeguarding action, support for those affected, preservation of relevant evidence and referral to external agencies or the police where appropriate. Staff should not download, copy or forward potentially illegal images; they should seek immediate advice from the DSL.

The school may take action in relation to incidents that take place outside school hours where they have repercussions for the orderly running of the school, pose a threat to a member of the school community, or could adversely affect the reputation of the school or its employees or governors. The school will act proportionately and in accordance with its policies and legal responsibilities.

F. Monitoring, review and related policies

The school will consider social media and AI risks as part of its wider online safety and safeguarding arrangements. This policy should be read alongside the school's Child Protection and Safeguarding Policy, Online Safety Policy, Acceptable Use Agreements, Anti-Bullying Policy, Data Protection Policy and staff code of conduct.

The school will review this policy at least annually and sooner if changes in technology, guidance or safeguarding risks make this necessary. Staff will be made aware of relevant changes and provided with appropriate guidance.

Policy administration

Policy owner	Headteacher
Reviewed	November 2026
Approval	Approved by the Governing Body November 2026
Next review	November 2027

Guidance informing this policy

This policy has been updated with reference to the Department for Education's Keeping Children Safe in Education 2026 and its guidance on generative AI and data protection in schools. It should be read alongside current statutory guidance and the school's own data protection and safeguarding arrangements.