TrustEd Schools

Stokesay Primary School

Artificial Intelligence Policy

Setting expectations for the safe, responsible and effective use of artificial intelligence by staff, governors and pupils

Review frequency	Annually
Date of determination	3/11/26
Committee	Stokesay LGB
Date of next review	September 27
Policy owner	William Vaughan

Statement of intent

Stokesay Primary School recognises that artificial intelligence (AI) has the potential to support teaching and learning, improve pupil outcomes, reduce workload and strengthen organisational effectiveness. The school also recognises that AI can create risks relating to accuracy, data protection, safeguarding, equality, intellectual property and assessment integrity.

The purpose of this policy is to enable the school community to benefit from AI while ensuring that its use is safe, responsible, transparent and subject to appropriate human judgement and oversight.

AI should support, rather than replace, professional knowledge, critical thinking, creativity, safeguarding responsibility or the important relationship between teachers and pupils.

1. Aims and scope

This policy applies whenever AI is used for school business or learning by staff, governors, contractors, volunteers or pupils, regardless of the device or location used.

- Support appropriate use of AI to enhance teaching, learning and pupil outcomes.
- Enable approved AI use that improves efficiency and reduces unnecessary workload.
- Prepare pupils to understand and use AI critically, safely and responsibly.
- Protect personal data, confidential information, intellectual property and individual rights.
- Ensure meaningful human oversight and professional accountability.
- Provide a clear process for approving AI tools and use cases.

2. Legal and regulatory framework

This policy has due regard to relevant legislation and current guidance, including:

- UK General Data Protection Regulation and Data Protection Act 2018.
- Data (Use and Access) Act 2025.
- Equality Act 2010.
- Copyright, Designs and Patents Act 1988.
- Freedom of Information Act 2000.
- Department for Education guidance on generative AI in education and AI product safety standards.
- Keeping Children Safe in Education and filtering and monitoring standards.
- Joint Council for Qualifications guidance on AI use in assessments.

3. Definitions

- Artificial intelligence (AI): digital systems that perform tasks commonly associated with human intelligence, including generating content, answering questions, analysing data, automating tasks, transcribing, recommending, ranking or classifying.
- Generative AI: AI that creates new text, images, audio, video, code or other content in response to a prompt.
- AI tool: any application, platform, feature, integration, plugin or service that uses AI.
- Prompt: information, instructions or material entered into an AI system.

- Output: content, analysis, recommendations or other results produced by an AI system.
- Approved use: a defined use of an approved AI tool by an identified user group for an agreed purpose.

4. Principles for AI use

- Purpose and benefit: AI use must have a clear educational or operational purpose and expected benefits that outweigh the risks.
- Human responsibility: users remain responsible for the accuracy, legality, quality and appropriateness of final work.
- Privacy by design: personal data must be minimised and must not be entered into an unapproved tool.
- Fairness: AI must not be used in ways that cause unlawful discrimination or unfair treatment.
- Transparency: material AI assistance should be acknowledged where appropriate.
- Security: only approved tools may be used for approved purposes.
- Age appropriateness: pupil use must be suitable for pupils' age, educational needs and safeguarding context.
- Proportionality: the level of assessment, approval and oversight must reflect the level of risk.

5. Roles and responsibilities

5.1 Governing body

- Approve and monitor this policy.
- Hold the headteacher to account for safe, effective and ethical implementation.
- Receive sufficient information to oversee benefits and risks.
- Use only approved tools and follow the same expectations as staff.

5.2 Headteacher

- Take overall responsibility for AI use.
- Ensure the policy is implemented, communicated and reviewed.
- Obtain appropriate DPO, IT and DSL advice.
- Approve tools and use cases following section 6.
- Ensure staff training and pupil education.

5.3 AI lead, where appointed

- Coordinate day-to-day implementation, maintain the approved tools register, support staff, share effective practice and monitor impact. Where no lead is appointed, responsibilities sit with the headteacher or delegated senior leader.

5.4 Data Protection Officer and IT support

- Advise on privacy, lawful processing, security, suppliers, data flows, retention, access controls and DPIAs.
- Support assessment of integrations, transfers, encryption, logging and audit.
- Support incident response.

5.5 Designated safeguarding lead

- Advise on pupil-facing tools and safeguarding risks.

- Remain aware of emerging AI-related safeguarding threats.
- Reflect risks in training and online safety arrangements.
- Respond to concerns and contribute to filtering and monitoring decisions.

5.6 Staff and governors

- Use only approved tools for approved purposes.
- Seek advice where use is unclear or potentially high risk.
- Protect information, check outputs, acknowledge material AI use and report concerns.
- Help pupils understand opportunities, limitations and risks.

5.7 Pupils

- Follow section 10, staff instructions, the approved uses register and relevant school rules.

6. Approval of AI tools and use cases

No new AI tool, integration, plugin or materially new use may be introduced without approval. Approval of a tool does not make every possible use appropriate or permitted.

1. Describe the tool, purpose, users, information involved, benefit and human oversight.
2. Assess educational, safeguarding, equality, copyright, accuracy, security, procurement and operational risks.
3. Consult the DPO and IT where personal data, supplier processing, integration or material information risk is involved.
4. An AI Risk Assessment should be completed where the proposed use involves pupils, personal data, recordings, transcription, decision-making, safeguarding considerations or any other medium or high-risk use. The school may use its approved AI Risk Assessment template for this purpose. A DPIA should be completed where the proposed processing is likely to create a high risk to individuals or where advised by the DPO. An equality impact assessment should be completed where appropriate.
5. Assess pupil-facing use for age restrictions, safeguarding, filtering and monitoring, accessibility, accounts and suitability.
6. Review supplier privacy notices, terms, contractual arrangements and assurances, including prompts, outputs, storage, retention, deletion, security, intellectual property, access controls, logging and exit arrangements.
7. Record the decision, conditions and review date.
8. Update and communicate the approved tools and uses register.

Uses involving children, safeguarding, special category data or significant decisions must be treated as higher risk and must not proceed without enhanced review, senior approval and clear human oversight.

Staff are encouraged to suggest new ways in which AI might improve pupil outcomes, teaching, accessibility or workload. Proposed uses must be considered through the approval process before implementation.

7. Staff and governors' use of AI

7.1 Appropriate use

Approved uses may include developing first drafts, generating ideas, summarising non-sensitive material, planning learning, supporting accessibility, conducting research and improving administrative efficiency. The approved tools register determines what is permitted.

AI should not replace professional expertise, direct knowledge of pupils or the teacher-pupil relationship. Users must consider whether AI is right for the task, even where a tool is approved.

7.2 Professional responsibility and verification

AI output must be treated as unverified draft material. AI systems can produce apparently confident but inaccurate or fabricated output, sometimes described as a "hallucination".

- Verify factual claims against reliable and preferably primary sources.
- Open and verify citations, quotations, links and legal authorities.
- Check names, dates, figures and calculations independently.
- Check omissions, bias, discriminatory assumptions, inappropriate language and accessibility.
- Check for personal, confidential, sensitive or copyrighted material.
- Correct or reject unreliable output and record checks where AI materially influences advice or decisions.

High-risk legal, financial, safeguarding, employment, regulatory or technical output must be independently reviewed by a suitably qualified person. Unverifiable output must not be relied upon.

7.3 Data protection, confidentiality and records

- Do not enter personal, confidential or sensitive information into public or unapproved tools.
- Approved personal-data processing must follow data protection principles, any DPIA and conditions of use.
- Use data minimisation, anonymisation or pseudonymisation wherever possible.
- Report unauthorised disclosure, access or processing immediately.
- Manage AI output under records, retention and freedom of information requirements.
- Personal data may include text, images, audio, voice recordings, transcripts and uploaded documents. Voice recordings and transcripts require specific approval.
- AI recording, transcription or summarising of meetings requires specific approval. Participants must be informed and records managed appropriately.

7.4 Intellectual property and copyright

- Respect copyright, licensing and intellectual property in prompts, inputs and outputs.
- Do not use pupil work or staff resources to train a model unless lawfully approved.
- Do not upload or reproduce copyright material without an appropriate right, licence or exception.
- Do not assume AI-generated content is free of third-party rights.
- Consider supplier terms and seek advice where ownership or permission is unclear.

7.5 Bias, equality and accessibility

AI can reproduce or amplify bias. Users must review outputs for discriminatory assumptions, stereotypes, unequal impact, inaccessible presentation and unintended consequences. Higher-risk uses must be tested and monitored for fairness.

7.6 Transparency

AI use should be acknowledged where it materially contributes to published content, advice or decision support. Suggested statement: “This content was developed with assistance from an AI tool. It has been reviewed and edited by the author, who takes responsibility for the final content.”

7.7 Prohibited use

- Using unapproved AI for school business.
- Entering personal, confidential or sensitive information into an unapproved tool.
- Presenting unverified output as fact, evidence or professional advice.
- Creating misleading, deceptive, discriminatory, offensive or impersonating content.
- Using AI to monitor, profile, rank or make significant decisions without approval and safeguards.
- Using AI to avoid professional duties, checks or procedures.
- Bypassing approval, security, filtering, monitoring or record-keeping controls.
- Using a personal AI account or personal device to process school information without specific approval.

8. AI-assisted and automated decision-making

AI must not take a significant decision about an individual solely through automated processing or effectively determine an outcome through a recommendation, ranking, score, classification or triage merely approved by a human.

Any exceptional proposal requires written approval, a DPIA and legal assessment, meaningful human involvement, accuracy and bias testing, transparency, a route to representations and human review, monitoring and a suspension process.

9. Educating pupils about AI

- How AI generates content and why output may be inaccurate, incomplete or biased.
- How to check evidence, claims and sources.
- How to protect personal information and privacy.
- Copyright, ownership, attribution, plagiarism and academic integrity.
- Ethical use and risks from harmful, misleading, manipulated or impersonating content.
- How AI can support learning without replacing thinking, practice, creativity or teacher guidance.
- How to report harmful content or concerns.

10. Pupil use of AI

Pupils may use AI only when approved for their age group and purpose and permitted or directed by the school. Staff instructions take precedence.

10.1 Permitted use may include

- Exploring ideas or researching where permitted.
- Discussing and evaluating AI output.
- Using approved accessibility or language support.
- Planned computing, creative, media-literacy or subject activities.

10.2 Pupils must

- Follow age restrictions, staff instructions and the approved uses register.
- Protect personal information.
- Check AI-generated information.
- Acknowledge AI use when required, including tool and date.
- Submit their own work and distinguish it from AI output.
- Retain drafts or evidence where required.
- Report harmful or concerning content.

10.3 Pupils must not

- Use AI where not permitted in assessment or schoolwork.
- Present AI-generated output as their own.
- Impersonate, bully, harass, deceive or harm others.
- Generate or share inappropriate content.
- Upload another person's work, image, voice or information without permission and approval.
- Bypass filtering, monitoring, access controls or age restrictions.

11. Formal assessments and academic integrity

The school will follow current JCQ and awarding-body requirements.

- AI must not be used in assessment, coursework or non-examination assessment unless expressly permitted.
- Permitted use must be acknowledged and pupils must retain evidence of their own work.
- Staff must explain plagiarism, authentication and legitimate assistance.
- Suspected misuse will be addressed through relevant procedures.

12. Safeguarding, online safety, filtering and monitoring

AI-related risks may include grooming, harassment, coercion, bullying, harmful or misleading content, impersonation and harmful alteration of images, audio or video.

- Report safeguarding concerns immediately to the DSL.
- Consider pupil-facing tools within filtering and monitoring arrangements.
- Consider content restrictions, monitoring, accounts, access and reporting mechanisms.
- AI must not replace safeguarding judgement or referral procedures.

13. Training and awareness

- Staff receive appropriate training before use and updates as practice develops.
- Training covers data protection, safeguarding, security, verification, bias, copyright, academic integrity and effective use.
- Approvers and high-risk users receive additional guidance.
- Governors receive sufficient information for oversight.
- Pupils receive age-appropriate teaching before using approved tools.

14. Raising concerns

Staff and governors should raise concerns with the headteacher, AI lead, DPO, IT support or DSL, as appropriate.

Pupils, parents and carers may raise concerns through usual procedures. Where AI materially influences a decision, an affected person must be able to request meaningful human review.

15. Incidents and breaches

- Report safeguarding concerns immediately to the DSL.
- Report data breaches or security incidents through the breach procedure and to the DPO.
- Report material errors, unfair outcomes or unreliable advice to a senior leader.
- Address staff breaches through conduct or disciplinary procedures where appropriate.
- Address pupil misuse through relevant school procedures.
- Suspend access while a concern is assessed where necessary.

16. Monitoring, evaluation and transparency

- Monitor effectiveness, risks and benefits.
- Review approved tools after significant change or incident.
- Consider feedback from staff, pupils, parents and carers.
- Inform the school community about significant educational uses as appropriate.
- Maintain the approved tools register as a separate living document.

17. Monitoring and review of this policy

Review at least annually and sooner following significant changes to law, guidance, technology, supplier terms, school practice or identified risk.

18. Links with other policies

- Data protection and personal data breach procedures.
- Information security, records management, retention and information sharing.
- Child protection, online safety, acceptable use, filtering and monitoring.
- Behaviour, homework, assessment, exams and staff conduct.
- Equality, accessibility, complaints, copyright, procurement and finance.

Appendix 1: Local policy information

Completion guidance: The headteacher or delegated senior leader completes this table before adoption. Insert names, roles and links. Update it whenever responsibilities or document locations change.

School name	[Insert school name]
Headteacher	[Insert name]
AI lead or responsible senior leader	[Insert name and role]
Data Protection Officer	[Insert name and contact details]
Designated safeguarding lead	[Insert name and contact details]
IT support contact	[Insert contact details]
School approved AI tools register	[Insert link or folder location]
AI proposal and approval form	[Insert link or folder location]
AI risk assessment template	[Insert link or folder location]
DPIA process and template	[Insert link or folder location]

Appendix 2: AI tool and use approval process

Completion guidance: Staff first check the Trust and school approved tools registers. A proposal form is needed only where the tool or intended use is not already approved. The headteacher may delegate initial review.

Member of staff identifies an AI tool or a new AI use

▼

Check the Trust and school approved AI tools registers

▼

YES: tool and intended use already approved	NO: tool or intended use not approved
Use in line with the recorded conditions. No proposal form is required.	Complete Part A of Appendix 4 and submit it to the headteacher, AI lead or delegated senior leader.

▼

Initial school review: Is there a genuine educational or operational benefit, and is the use necessary and proportionate?

▼

NO	YES
Decline or return for further information. Record and communicate the reason.	Complete the simple screening questions in Part B of Appendix 4.

▼

Does it involve personal information, pupil use, safeguarding, recording or transcription, or connection to another school system?

▼

NO: low-risk use	YES or UNSURE: enhanced review
Headteacher or delegated senior leader may approve locally with recorded conditions.	Seek relevant DPO, IT and/or DSL advice. Complete an AI risk assessment or DPIA only where advised or required.

▼

Record the decision and conditions in Part D of Appendix 4

▼

If approved, add the tool and permitted use to the school approved tools register

▼

Review by the recorded date or sooner if the tool, use or risks change

Appendix 3: School approved AI tools and uses register

Completion guidance: Keep this as a separate living document in an accessible shared location. Add one row for each approved tool and use. Separate rows should be used where one tool has different approved purposes.

- Tool / supplier: product and supplier name.
- Approved users: staff group, department or pupils allowed to use it.
- Approved use: the specific agreed purpose.
- Restrictions or conditions: limits such as no pupil data, staff supervision or approved accounts only.
- Review date: when the school will check the tool remains useful, safe and appropriate.

Tool / supplier	Approved users	Approved use	Restrictions or conditions	Review date

Example only

Tool / supplier	Approved users	Approved use	Restrictions or conditions	Review date
Example lesson planning tool / supplier	Teaching staff	First drafts of lesson plans and non-personalised resources	No pupil names, work or personal information. Staff check all output.	[Insert date]

Appendix 4: AI proposal and approval form

Completion guidance: Use only where the tool or intended use is not already approved. The proposer completes Part A. The headteacher, AI lead or delegated senior leader completes Parts B and D. Complete Part C only where specialist advice is needed.

Part A: Proposal - completed by the member of staff

Completion guidance: Give enough information to explain what the tool does and why it would be useful. Do not include pupil or staff personal information on this form.

Name of proposer	[Complete]
Role / department	[Complete]
Date	[Complete]
Tool and supplier	[Complete]
Website or product link	[Complete]
Who would use it?	[Complete]
What would it be used for?	[Complete]
Expected benefit	[Complete]
Could an approved tool meet the same need?	[Complete]
Would pupils use or interact with it?	[Complete]
Would pupil, parent or staff information be entered, uploaded, recorded or generated?	[Complete]
Would it record, transcribe or summarise meetings or conversations?	[Complete]
Would it connect to another school system, account or browser extension?	[Complete]
Proposed trial or implementation	[Complete]
Anything else the reviewer needs to know	[Complete]

Part B: Initial review - completed by the headteacher or delegated reviewer

Completion guidance: Answer Yes, No or Unsure. A Yes or Unsure answer does not automatically mean refusal. It identifies where advice or safeguards may be needed.

Question	Yes / No / Unsure	Brief note or action
Is there a clear educational or operational benefit?		
Is the tool or use already approved?		
Would pupils use or interact with it?		
Would pupil, parent or staff information be entered, uploaded, recorded or generated?		
Would meetings or conversations be recorded or transcribed?		
Would it connect to another school system or account?		
Are there safeguarding concerns?		

Could it influence an important decision about a pupil or member of staff?		
Is DPO, IT or DSL advice needed?		

Part C: Specialist advice - complete only where needed

Completion guidance: Contact the DPO where personal data or recording is involved; IT support where the tool connects to school systems or accounts; and the DSL where pupils will use the tool or safeguarding concerns may arise. Record key advice or attach supporting evidence.

Advice	Required?	Main advice, action or reference
DPO advice	☐ Yes ☐ No	
IT / information security advice	☐ Yes ☐ No	
DSL advice	☐ Yes ☐ No	
Other advice	☐ Yes ☐ No	

Part D: Decision - completed by the headteacher or delegated decision-maker

Completion guidance: Select one outcome, state the reason and any conditions clearly. If approved, add the tool and permitted use to Appendix 3 or the separate school register.

Decision	☐ Approved ☐ Approved with conditions ☐ Pilot approved ☐ More information required ☐ Declined
Short reason	[Complete]
Conditions or restrictions	[Complete or state none]
Who may use it and for what purpose	[Complete]
Training or guidance required	[Complete or state none]
Approved by	[Name and role]
Decision date	[Date]
Review date	[Date]
Added to school register	☐ Yes ☐ Not applicable
Outcome at review	[Complete at review]