Artificial Intelligence (AI) Policy

2026–2027 | Safe, responsible and purposeful use of AI

Policy owner	Headteacher
Headteacher	Mrs Melissa Lawrenson
Designated Safeguarding Lead	Mrs J Lloyd
Chair of Governors	Mr Paul Willerton
Policy date / effective from	November 2026 (following approval)
Approved by governors	Approved
Date approved	24.11.2026
Review frequency	Annually, or sooner if guidance, technology or risks change
Next scheduled review	November 2027

1. Purpose

Eaves Primary School recognises that artificial intelligence (AI) can help staff plan, prepare resources and work efficiently. We will use it only when it supports high-quality education, professional judgement and the safety of our children. AI does not replace teachers, school leaders or established safeguarding procedures.

2. Who this policy applies to

This policy applies to all staff, governors, volunteers, trainees and other adults using AI on behalf of Eaves. It also sets out expectations for any supervised pupil use. It should be read alongside our Safeguarding and Child Protection, Data Protection and UK GDPR, Online Safety, Staff Code of Conduct, and acceptable-use arrangements.

3. Appropriate use by staff

- Staff may use school-approved AI tools to generate ideas for lessons, adapt non-identifiable resources, draft routine communications and support administrative tasks.
- All AI output must be checked for accuracy, bias, suitability, accessibility and alignment with the Eaves curriculum before it is used.
- Teachers remain responsible for teaching, assessment, feedback and decisions about individual pupils. AI-generated material must not be presented as verified evidence.
- Staff must follow any school approval arrangements before using a new AI service for school business.

4. Protecting personal and confidential information

- Do not enter identifiable pupil, parent, staff or safeguarding information into public or AI tools. This includes names combined with details, photographs, medical information, SEND records, behaviour information and CPOMS content.
- Use fictional or fully anonymised examples where appropriate, checking that a person cannot be identified from the details provided.
- Any proposed use of AI with personal information requires prior school authorisation, data protection checks and advice from the Data Protection Officer where appropriate. A data protection impact assessment may be required.

- Report any accidental disclosure or suspected data breach immediately through the school's data protection and safeguarding procedures.

5. Safeguarding and online safety

AI-generated material may be inaccurate, inappropriate or misleading. Staff must not use AI to create or alter images, audio or video of pupils without a specifically authorised, lawful and safeguarded purpose. AI must never be used to create humiliating, discriminatory, sexualised or deceptive content. Any safeguarding concern, including harmful AI-generated material or impersonation, must be reported promptly to the DSL in line with school procedures.

6. Pupil use and teaching about AI

Pupils will learn age-appropriate messages about online safety, checking information and the limitations of AI. Any pupil use of an AI service must be approved, age-appropriate, supervised and consistent with the provider's age restrictions and school filtering and monitoring arrangements. Children must not be asked to create personal accounts on unsuitable services or share personal information with AI tools. AI should support, not replace, pupils' own thinking, reading, writing and creativity.

7. Assessment, inclusion and fairness

AI may support staff with resource ideas and accessible formats, but it must not independently determine attainment, SEND provision, safeguarding actions, sanctions, admissions or other significant decisions about a child. Staff must check for inaccurate, stereotyped or biased outputs and ensure materials meet pupils' individual needs. Professional assessment and school procedures remain authoritative.

8. Transparency, copyright and quality

Staff should be open about significant use of AI where this matters to colleagues, pupils or families. They must check the ownership, permissions and reliability of content, including images and quoted material, before sharing or publishing it. AI output should be edited into the school's own voice and checked against trusted sources.

9. Roles and responsibilities

- Headteacher and senior leaders: approve and oversee school use, communicate expectations, arrange training and review risks.
- DSL: oversee safeguarding concerns connected with AI and ensure incidents are recorded and addressed.
- Data Protection Officer and relevant leaders: advise on privacy, contracts, security and any required assessments.
- Staff and governors: follow this policy, check outputs and raise concerns promptly.
- Governing body: provide oversight and approve/review the policy in line with school arrangements.

10. AI leadership and oversight

The Headteacher is the designated lead for oversight of AI use at Eaves, supported by senior leaders, the DSL and the Data Protection Officer (DPO) as appropriate. The Headteacher will maintain a proportionate overview of approved uses, staff awareness, identified risks and any concerns. Governors will receive relevant assurance through established reporting arrangements.

11. Oversight of AI tools

The Headteacher will maintain oversight of AI tools used within school. Staff must seek approval before introducing new AI applications for school use

12. Staff awareness and training

Leaders will ensure staff receive proportionate guidance and updates on approved tools, acceptable use, prompt-writing without personal information, checking outputs, bias, copyright, safeguarding and incident

reporting. Expectations will be revisited when guidance or approved tools change. Staff should ask a senior leader before using AI where they are unsure.

13. Reporting concerns and responding to misuse

Staff must promptly report harmful content, unsafe pupil use, inappropriate staff use, security concerns or accidental disclosures to the appropriate school lead. Safeguarding matters go directly to the DSL; data breaches follow the school's data protection reporting route. The school will respond proportionately under its existing safeguarding, conduct and behaviour procedures and review controls where necessary.

14. Monitoring and review

Leaders will review AI use, staff guidance, emerging risks, training needs and any incidents, and report significant matters to governors. This policy will be reviewed annually, next in November 2027, or sooner if guidance, technology, school arrangements or identified risks change.