

AI Policy



Belton Lane
Primary School

Approved by:	Jonathan Mason	Date: September 2026
Last reviewed on:	September 2026	
Next review due by:	September 2027	

Contents

1 Purpose and scope	3
2 Policy statement.....	3
3 Quick rule for staff	3
4 Roles and responsibilities.....	4
5 Approved tools and accounts	4
6 Data protection confidentiality and security	4
7 Safeguarding and harmful content.....	5
8 Pupil use of AI	5
9 Teaching learning and assessment	6
10 Human oversight and significant decisions	6
11 Transparency authorship and communications	6
12 Copyright intellectual property and records	7
13 Recording transcription and meeting tools.....	7
14 Procurement and approval of AI systems	7
15 Incident reporting	7
16 Training monitoring and assurance	8
17 Non-compliance	8
18 Review and legal framework	8
Appendix 1 Approved AI register.....	9
Appendix 2 Staff pre use checklist	10
Appendix 3 Suggested acknowledgement wording	10
Appendix 4 Key contacts.....	10

1 Purpose and scope

This policy applies whenever school work, school information, school devices or school accounts are used with an AI system. It covers generative AI, automated decision tools, transcription and summarisation tools, image and media generators, adaptive learning tools and other systems that use machine learning. It applies to all staff, governors, volunteers and contractors. Pupil use is governed by section 9.

This policy supplements, and does not replace, the school's safeguarding, child protection, data protection, acceptable use, online safety, cyber security, records management, behaviour, assessment, equality, complaints, staff conduct and curriculum policies. Where rules conflict, the safer and more protective requirement applies.

2 Policy statement

AI is a support tool. It does not replace professional knowledge, relationships, creativity or judgement. The person who uses, adapts, approves or publishes AI-assisted work remains accountable for the final content and decision.

- AI use must have a clear educational or operational purpose.
- Only school-approved tools, accounts and uses may be used for school business.
- Personal, confidential or safeguarding information must not be entered into a public or unapproved AI tool.
- AI outputs must be checked by a competent person before they are used or shared.
- AI must not make significant decisions about pupils or staff.
- Use must be lawful, fair, inclusive, transparent, secure and consistent with the school's values.

3 Quick rule for staff

Stop

Before entering a prompt or uploading a file, check whether it contains identifiable pupil, parent or carer, staff or governor information; safeguarding, SEND, medical or behaviour information; photographs or recordings; confidential school information; login details; or third-party copyrighted material. If it does, do not proceed unless the tool and that specific use have been formally approved.

Check

Confirm that the tool, account and purpose are approved. Check age restrictions, audience, privacy settings and whether a human with appropriate expertise will verify the output.

Use

Treat the output as a draft. Verify it, edit it for the intended audience, disclose AI assistance where required, and take responsibility for the result.

4 Roles and responsibilities

Role	Responsibilities
Governing Body	Approves this policy; seeks assurance on safeguarding, data protection, equality and risk; reviews significant incidents and compliance.
Headteacher	Accountable implementation; appoints an operational AI lead; authorises approved tools and high-risk uses after appropriate advice.
Designated Safeguarding Lead	Ensures AI use aligns with safeguarding procedures; leads action on harmful content or concerns involving children.
Data Protection Officer	Advises on lawful processing, privacy notices, contracts, data protection impact assessments, breaches and data-subject rights.
IT or network lead	Assesses security, access controls, logging, retention, integration, supplier assurance and safe configuration.
Curriculum assessment leads or	Set subject and assessment expectations; ensure pupil use develops knowledge, critical thinking and digital literacy.
All users	Use approved tools only; protect information; check outputs; disclose use when required; report incidents promptly; complete training.
Pupils	Follow staff instructions and acceptable-use rules; do not use AI to deceive, bully, create harmful content or present AI work as their own.

5 Approved tools and accounts

A tool being free, popular, built into software or accessible through a search engine does not make it approved. Staff must use the school-managed account and approved settings where specified. Personal accounts must not be used for school information or school business unless expressly authorised.

The school will maintain an approved AI register using Appendix 1. Approval is specific to the tool, version or service, account type, permitted purpose and data classification. Material changes to supplier terms, training practices, integrations or security may suspend approval pending review.

Staff must not procure, trial, connect or invite pupils to use a new AI service without approval from the designated lead. Browser extensions, meeting bots and tools built into existing platforms are included in this rule.

6 Data protection confidentiality and security

6.1 Information that must not be entered into unapproved AI

Users must not type, paste, upload, photograph, record or otherwise provide the following to a public or unapproved AI service:

- pupil, parent or carer, staff, volunteer or governor names or other identifying details;
- dates of birth, addresses, contact details, identification numbers or account details;
- safeguarding, child protection, SEND, medical, wellbeing, behaviour, attendance or assessment information;
- photographs, video, voices, handwriting, biometric information or identifiable work;
- passwords, access tokens, system configurations, security information or confidential correspondence;
- unpublished governing body, HR, legal, financial, complaint, investigation or procurement information;
- any dataset from which a person could reasonably be identified, including through combination with other information.

6.2 Exceptional approved processing

Personal data may be processed by AI only where the school has approved both the system and the exact purpose; identified a lawful basis; applied data minimisation; checked retention, deletion, location, access, training and onward-sharing arrangements; updated privacy information where required; and completed a data protection impact assessment where the DPO considers one necessary. Pseudonymisation is not automatically sufficient because information may still be personal data.

6.3 Security

Users must follow school access controls, multifactor authentication and device rules. They must not connect an AI system to school email, storage, management information, safeguarding or learning platforms without technical approval. Confidential outputs must be stored and shared only through approved school systems.

7 Safeguarding and harmful content

AI must never replace professional safeguarding judgement or established reporting routes. It must not decide whether a child is at risk, whether a concern should be recorded or referred, or what safeguarding action should be taken. Staff must record and report concerns through the school's safeguarding procedures and consult the Designated Safeguarding Lead without delay.

Users must not use AI to create, transform, sexualise, humiliate, impersonate or fabricate images, audio or video of pupils, staff or others. Deepfakes, discriminatory content, bullying, grooming, violent or sexual material and attempts to bypass safety controls are prohibited. Suspected illegal content must not be copied or circulated; staff must preserve only what safeguarding or law-enforcement procedures require and seek immediate DSL advice.

If an AI tool displays harmful or concerning material to a pupil, staff should secure the pupil's immediate safety, stop access where appropriate, reassure without promising confidentiality, record the facts and follow safeguarding and online-safety procedures.

8 Pupil use of AI

Pupils may use AI only as part of a planned, age-appropriate learning activity using a school-approved tool and under the level of supervision set by the teacher. The school must check supplier age limits and terms before access. Where an account or consent is required, the school will determine the lawful and appropriate route; staff must not ask pupils to create personal accounts informally.

Teaching should help pupils understand that AI can be persuasive but wrong, can reflect bias, and does not have human understanding or responsibility. Tasks should protect opportunities to practise foundational knowledge, reading, writing, mathematics, creativity, problem-solving and independent thought.

Pupils must not:

- enter personal or confidential information about themselves or anyone else;
- use AI to bully, harass, impersonate, deceive or create harmful or inappropriate content;
- circumvent filters, age restrictions or staff controls;
- submit AI-generated work as their own where this has not been permitted;
- use AI during an assessment unless the teacher or assessment rules expressly allow it.

A pupil will not be sanctioned solely because an automated detector labels work as AI-generated. Staff will consider the pupil's work, process, explanation and other relevant evidence and will follow the school's behaviour and assessment procedures.

9 Teaching learning and assessment

Permitted uses may include generating initial ideas, adapting non-confidential resources, creating low-stakes practice material, improving accessibility, drafting model text and reducing routine administrative workload. Teachers must ensure outputs are suitable for the curriculum, accurate, inclusive, accessible and age appropriate.

AI-generated lesson plans, questions, model answers, reading passages and images require professional review. Staff must check facts, calculations, quotations, sources and references against authoritative material. Fabricated citations must be removed. Legal, medical, safeguarding, SEND and HR content requires review by an appropriately competent person and must not be treated as professional advice.

Teachers must state when and how AI may be used in an activity or assessment. Where relevant, pupils should acknowledge substantial AI assistance and be able to explain their choices and learning. For formal qualifications, the current rules of the awarding body and Joint Council for Qualifications must be followed.

10 Human oversight and significant decisions

AI must not be the sole or determinative basis for a significant decision. This includes decisions about safeguarding, SEND identification or support, admissions, attendance action, behaviour sanctions, suspension or exclusion, attainment, grouping, access to opportunities, complaints, recruitment, disciplinary action or performance management.

A suitably authorised person must understand the information used, consider relevant context, challenge the AI result, identify possible bias or error, record reasons where appropriate and make the final decision. Individuals must have an accessible route to question decisions and seek human review.

11 Transparency authorship and communications

The school will be open about material uses of AI. Staff should not use AI to shape published curriculum content, reports, formal advice, consultation responses, decisions or communications presented as personal professional judgement.

Routine spelling, grammar, formatting or approved accessibility support does not normally need individual disclosure unless the context requires it. Disclosure does not transfer responsibility to the AI provider.

AI must not be used to imitate a named person's voice or writing style in a misleading way. Messages to parents and carers, pupil reports and sensitive communications must be checked and personalised by the responsible member of staff.

12 Copyright intellectual property and records

Before publication, staff must consider whether generated material may reproduce protected content, misuse a trade mark, or falsely attribute a quotation or source. The same citation and permissions standards apply to AI-assisted work as to other work.

Prompts, outputs and approval records that form part of a significant decision, formal communication or school record must be retained in the appropriate approved system for the period required by the school's records management schedule. Users must not rely on an AI chat history as the official record.

13 Recording transcription and meeting tools

AI recording, transcription, note-taking or analysis may be used only with prior approval. The organiser must establish a lawful purpose, inform participants before recording begins, respect objections or provide an alternative where appropriate, restrict access, check the transcript, and delete recordings and drafts in line with the approved retention period. Safeguarding, HR, grievance, capability, medical, special educational needs and other sensitive meetings require specific advice before use.

14 Procurement and approval of AI systems

Before approval, the Headteacher or delegated lead will coordinate proportionate review with the DPO, DSL, IT lead and relevant curriculum or business lead. The assessment will cover:

- educational or operational need and less intrusive alternatives;
- supplier identity, contractual terms, age restrictions and support arrangements;
- data categories, lawful basis, training use, retention, deletion, international transfers and subprocessors;
- security, account controls, integrations, audit logs, incident management and exit arrangements;
- accuracy, limitations, bias, accessibility, equality and evidence of effectiveness;
- human oversight, explainability, routes to challenge and potential impact on children;
- whether a DPIA, equality impact assessment, safeguarding review or pilot is required;
- cost, staff training, monitoring, renewal and removal of data at contract end.

Approval will be recorded, time limited where appropriate and reviewed after significant changes or incidents. High-risk uses will not proceed until the necessary assessments and controls are complete.

15 Incident reporting

A user must stop, preserve relevant information safely and report immediately if personal or confidential data is entered into an unapproved tool; an account, integration or prompt is compromised; harmful, discriminatory or safeguarding-related content is produced; an AI output contributes to an incorrect significant decision; or use appears unlawful or contrary to this policy.

Reports should go to the designated AI lead and, according to the issue, the DPO, DSL or IT lead. Existing data-breach, cyber-security, safeguarding, whistleblowing and complaints procedures apply. Staff must not attempt to conceal an error or delete evidence needed for investigation. The school will consider notification obligations and lessons learned.

16 Training monitoring and assurance

Staff will receive role-appropriate training before using approved AI tools and refresher training when risks or guidance change. Training will cover data protection, safeguarding, checking outputs, bias, copyright, assessment integrity, security and incident reporting.

The school may monitor use of school accounts and systems in accordance with its policies and privacy information. Monitoring will be proportionate and used to support safety, compliance, value and improvement. The designated lead will review the approved register, incidents, complaints, supplier changes and training needs at least annually and report material matters to governors.

17 Non-compliance

Concerns will be considered fairly and proportionately under the relevant staff conduct, disciplinary, pupil behaviour, safeguarding, data protection, complaints or contractual procedure. Deliberate misuse, concealment of an incident, unauthorised disclosure, harmful content creation or repeated disregard of instructions may result in formal action. The school will distinguish malicious conduct from good-faith mistakes and will use incidents to improve controls and training.

18 Review and legal framework

This policy will be reviewed annually and sooner following a significant incident, material change in law or guidance, introduction of a high-risk use, or substantial change to an approved supplier. The policy should be read with current requirements and guidance, including:

- UK data protection legislation, including the UK GDPR and Data Protection Act 2018 as amended;
- Department for Education guidance on generative AI in education, data protection in schools and generative AI product safety standards;
- Keeping Children Safe in Education and the school's safeguarding arrangements;
- Information Commissioner's Office guidance on AI, children's information, profiling and automated decision-making;
- Equality Act 2010, Human Rights Act 1998 and relevant copyright law;
- current awarding-body and Joint Council for Qualifications rules where applicable.

Legislation and guidance change over time. The school will follow the current published version even where a link or title in this policy is later updated.

Appendix 1 Approved AI register

The school should complete and maintain this register. No named product is approved merely because it appeared in an earlier policy draft.

Tool account and	Permitted purposes users and	Approved Usage	Owner and review
Chat GPT	JM and AM for administrative purposes	Drafting, summarising, analysing documents	JM
Chat GPT	All staff	Drafting, summarising, analysing documents	JM
Arbor AI	All staff	MIS searches, pupil summaries, communications, attendance and behaviour analysis, reports, formulas and absence processing	JM
Teams	All staff	Meeting summaries, transcripts, actions	JM
Co-Pilot	All staff	Drafting, summarising, analysing documents	JM
Grammarly AI	All staff	Writing/rewording	JM

Minimum approval record

- Supplier, product, version and approved account type
- Purpose, user group and whether pupil access is permitted
- Data classification and any prohibited information
- Required settings, human checks and disclosure
- DPIA or other assessment reference where applicable
- Approver, approval date, review date and withdrawal process

Appendix 2 Staff pre use checklist

- Need — Is there a clear educational or operational reason to use AI?
- Approval — Are this tool, account and exact purpose listed as approved?
- Data — Have I removed personal, confidential, safeguarding and security information?
- Rights — Am I permitted to upload or reuse the source material?
- Safety — Is the activity age appropriate and consistent with safeguarding rules?
- Check — Have I verified facts, calculations, citations, bias, tone and accessibility?
- Judgement — Is a qualified person making every significant decision?
- Transparency — Should I acknowledge material AI assistance?
- Record — Does the prompt, output or decision need to be saved in an approved system?
- Report — Do I know who to contact if something goes wrong?

Appendix 3 Suggested acknowledgement wording

Short form: “AI was used to support the initial drafting of this material. A member of staff reviewed and approved the final content.”

Expanded form: “An approved generative AI tool was used to support [describe purpose]. No unapproved personal or confidential data was provided. The final content was checked, adapted and approved by [role].”

Appendix 4 Key contacts

Responsibility	Name or contact
Headteacher	Jonathan Mason
Designated AI Lead	Audra Midgley
Designated Safeguarding Lead	Jonathan Mason
Data Protection Officer	Joe Lee
IT or network lead	ARK ICT