Safe Use of Artificial Intelligence Policy

Signed by headteacher: 

Signed by Chair of Governors: 

Date of Approval: 13th May 2026

Date for review: May 2027

1. Statement of intent

At Bitterne Manor Primary School, we recognise that artificial intelligence (AI) can support teaching, learning and school operations, including reducing workload and preparing pupils for future technologies. However, AI also presents risks, including inaccurate content, safeguarding concerns, data protection breaches and misuse in pupil work. As AI systems may produce inaccurate, biased or misleading content, all outputs require human review.

This policy ensures that AI is used:

- Safely
- Responsibly
- Lawfully
- In a way that supports high-quality education

The school will ensure that all use of AI complies with data protection, safeguarding and intellectual property law.

2. Definitions

- **AI -** Computer systems able to perform tasks normally requiring human intelligence.
- **Generative AI** - AI systems that generate new content (e.g. text, images, code).
- **Personal Data** - Any information relating to an identified or identifiable living individual.
- **Special Category Data** - Personal data requiring additional protection, including health, disability, ethnicity, religion, biometric data and safeguarding-related information.
- **Misuse of AI** - Any use of AI which means that pupils have not independently demonstrated their own attainment.

3. Legal Framework

This policy has due regard to:

- Data Protection Act 2018
- UK GDPR
- Online Safety Act 2023
- DfE *Keeping Children Safe in Education*
- DfE *Generative AI in Education*
- DfE *Product Safety Expectations for AI*
- JCQ guidance on AI and malpractice

This policy operates alongside:

- Data Protection Policy
- Child Protection and Safeguarding Policy
- Cyber-security Policy
- Acceptable Use Agreements
- Assessment policies

4. Roles and Responsibilities

Governing Board

- Ensure compliance with legislation
- Review policy annually
- Maintain oversight of AI use
- Receive updates regarding significant AI-related incidents or risks
- Monitor the effectiveness of this policy through regular review

Headteacher

- Approve AI tools for school use
- Ensure risk assessments and (where required) DPIAs are completed

- Ensure staff training
- Ensure compliance with DfE standards
- Maintain and publish a list of approved AI tools
- Ensure AI tools are assessed for safeguarding, GDPR compliance, age restrictions and cyber security prior to use
- Ensure staff understand the benefits, limitations and risks of AI systems

DPO
- Advise on data protection and AI use
- Oversee DPIAs
- Monitor compliance

DSL
- Lead on safeguarding risks related to AI
- Record and respond to concerns

Staff
- Follow this policy and related policies
- Use only approved AI tools
- Maintain professional judgement
- Remain accountable for all AI outputs
- Report concerns

Pupils
- Use AI safely and appropriately
- Submit work that reflects their own understanding
- Report concerns

5. Data Protection and Cyber Security

The school recognises that AI tools present data protection and cyber security risks.All use of AI must comply with the school's Data Protection Policy and UK GDPR.

Use of Personal Data

Staff must not input personal or special category data into publicly available AI tools.
AI tools may only process personal data where:
- The tool has been formally approved
- A DPIA has been completed where required
- Appropriate safeguards are in place
- Processing complies with the school's lawful basis under UK GDPR

Staff must ensure:
- Data is minimised
- Data is anonymised or pseudonymised where possible
- No identifiable data is used unless authorised

Transparency
- Privacy notices will be updated where required
- Individuals will be informed where AI is used to process data

Cyber Security

Staff must:
- Verify AI-generated content
- Be alert to phishing and scams
- Report concerns

The school will:

- Maintain filtering and monitoring systems
- Review AI-related cyber risks
- Follow DfE cyber standards

Procurement and Third-Party Providers

The school will assess third-party AI providers before adoption. This may include consideration of:

- Data processing agreements
- Data storage locations
- Retention and deletion arrangements
- Security standards
- Compliance with UK GDPR

Approval of AI Tools

All AI tools used within the school must be formally approved prior to use with pupils or school data.
Approval will consider:

- Data protection compliance
- Safeguarding and filtering arrangements
- Age restrictions and suitability for pupils
- Storage and processing of data
- Security and cyber risks
- Whether user data may be used to train AI systems
- Alignment with DfE guidance

Staff must not use unapproved AI tools for school business.

Data Breaches

All AI-related data breaches must be reported immediately in line with the Data Protection Policy.

6. Intellectual Property (IP)

The school will comply with copyright law when using AI.

Staff must:

- Ensure AI-generated content does not infringe copyright
- Not publish AI-generated content without checking ownership and permissions

The school will not allow pupil work to be used to train AI systems without appropriate consent.

7. Using AI Tools

For example, AI may be used to:

- Support planning and administration
- Enhance teaching and learning
- Develop pupils' understanding of technology
- Draft lesson ideas
- Adapt texts
- Generate quizzes
- Summarise documents
- Create model examples
- Administrative support

AI must:

- Always have outputs reviewed by professionals
- Support - not replace - professional judgement
- Be used appropriately and proportionately
- Be approved by the school

- Be subject to risk assessment

Pupil Access
Pupils must not use AI tools or create independent accounts for AI tools unless specifically authorised by the school. Pupils may only use AI tools approved by the school. Staff must ensure that:

- AI use is age-appropriate
- Pupils are supervised where appropriate
- Any minimum age requirements are complied with
- Pupils understand how to use AI safely and critically

Prohibited Uses
AI must not be used to:

- Make safeguarding decisions
- Make SEND or pastoral judgements
- Make behaviour or disciplinary decisions
- Determine assessment outcomes or grades

Never Upload
The following are prohibited from upload:

- safeguarding records
- CPOMS/MyConcern entries
- EHCPs
- medical information
- CAMHS reports
- identifiable SEND data
- HR disciplinary information
- confidential parent complaints
- exam scripts with candidate identifiers

Accountability
Staff remain fully responsible for all AI-generated content.

All AI outputs must be:

- Checked for accuracy, bias or fabricated information
- Adapted to the school context

8. Misuse of AI

Preventing Misuse
The school will:

- Supervise pupil work
- Use in-class assessment where appropriate
- Design tasks that require independent thinking
- Teach pupils when and how AI use is acceptable

Identifying Misuse
Staff will:

- Compare work to previous work
- Look for inconsistencies in style, knowledge and accuracy

Response
Suspected misuse will be managed in line with behaviour and assessment policies.

9. Safeguarding

AI tools may expose pupils to harmful or inappropriate content. The school will:

- Apply filtering and monitoring systems
- Teach pupils safe use
- Follow safeguarding procedures for all concerns

All AI-related safeguarding concerns will be recorded and managed in line with the Child Protection Policy.

10. Teaching Pupils About AI

The school will teach pupils:

- Safe and responsible use of AI
- Limitations and risks
- How to evaluate online information
- Digital literacy and critical thinking

11. Monitoring and Review

This policy will be reviewed by the Headteacher, DSL and DPO:

- Annually
- Following any significant incident
- Following changes in legislation

Appendix A

Approved AI Tools

Tool	Overall Risk	Approved Use	Restrictions / Key Conditions	Status
Microsoft Copilot (School Account)	Low–Medium	Staff planning, drafting documents, summarising information, administrative support	No safeguarding/SEND/confidential data. Outputs must be checked for accuracy and bias. Use only through school-managed accounts. Enterprise data protection means prompts are not used to train public foundation models in protected education/business environments.	Green – Approved
Google Gemini (Google Workspace for Education)	Low–Medium	Staff planning, research support, document drafting, productivity support	Use only through school Google accounts. No safeguarding/SEND/confidential uploads. Gemini for Workspace for Education does not use Workspace data to train public models. Outputs require checking.	Green – Approved
Canva AI	Low–Medium	Displays, presentations, classroom resources, image editing, worksheet design	Teacher review required before publication/use. No uploading identifiable pupil photographs unless specifically authorised. AI-generated images/content must be checked for appropriateness and copyright concerns.	Green – Approved
Adobe Express AI	Low–Medium	Creative resources, posters, classroom media, image editing	Teacher supervision required. No inappropriate image generation. No confidential uploads. Outputs must be checked before sharing with pupils.	Green – Approved
ChatGPT (School-Approved Use Only)	Medium	Drafting lesson ideas, adapting texts, generating quizzes, creating model examples	No pupil personal data or confidential information. Staff must not use personal accounts for school business. In ChatGPT settings, "Chat History & Training" should be disabled where possible. Free accounts still present governance risks. Human review mandatory.	Amber – Restricted Use
Chalkie	Medium	Curriculum planning, lesson/resource generation, teaching support	No pupil personal data or confidential uploads. Staff must review all generated content for accuracy and suitability. Uploaded content should not include protected safeguarding or assessment material.	Amber – Restricted Use
MagicSchool AI	Medium	Lesson planning, differentiation ideas, quiz/question generation, administrative support	Staff use only unless otherwise authorised. No personal or safeguarding data. Outputs may contain inaccuracies or bias and must be reviewed. Vendor settings should be configured to minimise data retention where available.	Amber – Restricted Use

TeachMateAI	Medium	Planning support, report drafting assistance, administrative workload reduction	No safeguarding/SEND/confidential information. Staff review required. AI outputs must not replace professional judgement. Use only through approved school accounts/settings.	Amber – Restricted Use
DeepAI	High	Limited staff experimentation only	Not for pupil use. No school/confidential data. Open public AI environment with image/deepfake generation risks and limited educational safeguards. Leadership approval required before any school use.	Red – Leadership Approval Required

Appendix B

Questions for Risk Assessing AI Tools:

Concern	Questions to Assess	Red Flags
Data protection	Is any data used to train the AI model? Can training on our data be disabled? Where is data stored and processed? Is there a UK GDPR-compliant DPA available? What data retention periods apply? Can conversations be deleted? Are accounts centrally managed through Microsoft/Google SSO? Is pupil data prohibited by the vendor? Does the system support role-based permissions? Is encryption used at rest and in transit? Does the tool share data with third parties?	No DPA available Vague privacy policy "We may use content to improve services" No clear deletion process Personal staff accounts required Unknown data hosting location No admin controls Vendor unwilling to answer GDPR questions
Safeguarding	Can pupils freely chat with the AI? Are harmful outputs filtered/moderated? Can users generate images/audio/video? Does the system allow anonymous access? Are interactions logged for safeguarding review? Is there age verification or age guidance? Can the AI imitate real people? Is there a reporting mechanism for unsafe content? Does the vendor publish safety policies?	Unmoderated chatbot access No content filtering Deepfake generation capability without controls Sexual/violent content easily generated Emotional dependency-style interactions Anonymous pupil access No safeguarding documentation

Technical & Cyber Security	Does the vendor hold recognised certifications (ISO 27001, Cyber Essentials etc.)? Is MFA supported? Are admin controls available? Can access be restricted by age or role? Is there audit logging? Does the platform integrate securely with existing systems? Are vulnerabilities disclosed responsibly?	No security documentation No admin dashboard Shared generic accounts Poor password/security controls Unknown ownership/company background No breach reporting process
Educational Value & Pedagogy	What genuine teaching problem does this solve? Does it improve workload, feedback, accessibility, or learning? Does it encourage thinking or shortcut thinking? Can outputs be trusted educationally? Does it support adaptive learning appropriately? Is teacher oversight built in? Is it appropriate for the age group?	"Magic solution" marketing Replaces teacher judgement Generates inaccurate explanations regularly Overpromises attainment impact Encourages passive copying No evidence of educational testing
Equality, Bias & Inclusion	Could outputs disadvantage groups of pupils? Does the AI handle SEND needs appropriately? Is accessibility built in? Can staff challenge biased outputs easily? Does it support multiple reading levels/languages?	Stereotyped outputs Poor accessibility support Biased disciplinary/recruitment recommendations Inaccurate SEND assumptions Lack of transparency around model limitations
Operational & Leadership Oversight	Who owns implementation? Is there staff training? Is there an acceptable use policy? Is approval centralised? Are there escalation procedures? Is usage monitored and reviewed? Is there a clear "never upload" list?	No policy Staff using random AI tools independently No training No review cycle AI decisions relied upon without checking

Appendix C

Risk Level	Typical Tools/Uses	Characteristics	Recommended Controls

Low Risk	Spellcheckers, Canva AI, quiz generators, presentation tools, image background removal, grammar assistants	Minimal/no personal data; limited pupil interaction	Staff guidance only
Low Risk	Lesson starter generators, worksheet creators, translation tools	Teacher-supervised content creation	Basic acceptable use policy
Medium Risk	ChatGPT, Microsoft Copilot, Gemini, MagicSchool, TeachMateAI	Staff-entered prompts; open-ended generation	Staff training + GDPR review
Medium Risk	AI marking assistance, report drafting, differentiated planning	Risk of hallucinations or bias	Human review mandatory
Medium Risk	Pupil research/chatbot use under supervision	Direct pupil interaction	Safeguarding controls + classroom supervision
High Risk	AI tutoring bots with unrestricted access	Persistent pupil interaction	Full DPIA + safeguarding review
High Risk	Emotion detection/behaviour prediction AI	Sensitive inference about pupils	Senior leadership/trust approval
High Risk	Automated grading or disciplinary recommendations	High-stakes decisions	Formal governance + human override
High Risk	AI analysing safeguarding/SEND data	Special category data processing	DPO + DSL approval
High Risk	Deepfake/image/audio generation for pupils	Safeguarding/reputation risk	Strict controls or prohibition

Green Approved	Amber - Restricted Use	Red - Leadership Approval Required
Low-risk tools No personal data Staff-facing only	Generative AI tools Requires training and policy compliance No sensitive data allowed	Pupil-facing AI Sensitive data processing Automated decision-making Behaviour/emotion analysis