



The
Rise
Partnership
Trust

Love • Learn • Laugh

Artificial Intelligence (AI) Policy

September 2026

Contents

1. Policy statement	2
2. Scope	2
3. Principles for the use of AI	3
3.1 Safeguarding First	3
3.2 Human Accountability	3
3.3 Data Protection and Information Security	3
3.4 Accuracy and Professional Standards	3
3.5 Fairness and Inclusion	3
4. Acceptable use	3
5. Unacceptable use	4
6. Pupil use of AI	4
7. Roles and responsibilities	4
8. Monitoring and review	5
9. Assurance matrix	5
10. Version Control	6
APPENDIX 1. AI guidance for staff	7
APPENDIX 2. Approved AI tools register	8
APPENDIX 3. AI procedures	9

1. Policy statement

The Trust recognises that Artificial Intelligence (AI) technologies can support teaching and learning, communication, administration, accessibility, and operational efficiency. The Trust encourages the responsible use of AI where it enhances outcomes for pupils, staff, and the wider organisation.

AI can be used as a tool to **support** professional practice and decision-making. It does not **replace** professional judgement, safeguarding responsibilities, or accountability. Individuals remain responsible for the accuracy, appropriateness, and lawful use of any AI-generated content, advice, or outputs.

This policy establishes the principles and expectations for the safe, ethical, and compliant use of AI across the Trust, ensuring that its use supports educational objectives while maintaining safeguarding, data protection, information security, and professional standards.

This policy was written with input from the trust's AI Working Party, which consists of Senior and Curriculum Leaders from all 3 of our schools, and is chaired by the trust's Director of Communications, IT, and Data.

This policy was written with reference to:

- DFE's 'Generative artificial intelligence (AI) in education' policy paper (August 2025)
- The ICO's 'Guidance on AI and data protection'
- The ICO's 'AI and data protection risk toolkit'
- Keeping Children Safe in Education (KCSIE 2025)

This policy should be read in conjunction with the following Trust documentation:

- Code of Digital Conduct
- Generative Artificial Intelligence Usage Statement
- Data Protection Policy
- Data Breach Policy
- Online Safety Policy
- Cyber Security Policy

2. Scope

This policy applies to all individuals working for or on behalf of the Trust, including:

- Contracted staff (employees)
- Trustees and governors
- Agency workers
- Contractors and consultants
- Volunteers
- Any other authorised users of Trust systems

The policy applies to the use of AI technologies in connection with all Trust activities, whether accessed through Trust-owned or personally owned devices, and whether used for educational, administrative, operational, communication, or business support purposes. Where pupils are permitted to use AI technologies, they must do so in accordance with Trust policies and guidance, as well as any applicable school/trust rules relating to technology use, behaviour, and assessment.

3. Principles for the use of AI

The Trust supports the responsible use of AI technologies in ways that enhance education, communication, accessibility, and operational efficiency. All use of AI for Trust activities must follow the principles below.

3.1 Safeguarding First

The safety and wellbeing of children and young people must always take precedence over the use of AI.

AI must not be used as a substitute for professional safeguarding judgement, risk assessment, or decision-making. Any safeguarding concerns identified through the use of AI must be managed in accordance with the Trust's safeguarding procedures.

3.2 Human Accountability

AI is a tool to support professional practice and decision-making. It does not replace professional judgement or accountability. Individuals remain responsible for all decisions, actions, and content produced using AI. AI-generated outputs must be reviewed before being relied upon, shared, or published.

3.3 Data Protection and Information Security

AI must be used in a manner that protects personal, confidential, and sensitive information. Users must only use AI tools approved by the Trust and must comply with the Trust's Data Protection and Information Security policies, as must adhere to the Trust's Code of Digital Conduct at all times. Personal data, safeguarding information, and other confidential information must not be entered into AI systems unless authorised and appropriate safeguards are in place.

3.4 Accuracy and Professional Standards

AI-generated content may be inaccurate, incomplete, biased, or out of date. Users must review and verify AI-generated outputs before use and ensure that any information, advice, educational materials, communications, or reports meet appropriate professional standards and are suitable for their intended purpose.

3.5 Fairness and Inclusion

AI should be used in a way that promotes fairness, inclusion, and accessibility. Users should consider whether AI-generated outputs may contain bias, stereotypes, or inappropriate assumptions and should ensure that materials and decisions remain inclusive and appropriate for all pupils, parents, staff, and other stakeholders.

4. Acceptable use

AI may be used to support Trust activities where its use is consistent with this policy and all other relevant Trust policies and procedures.

Examples of acceptable use include:

- Supporting lesson planning, curriculum development, and resource creation.
- Adapting, differentiating, or making materials more accessible for learners.
- Drafting communications, reports, presentations, and other documents.
- Summarising information or identifying key themes from non-confidential content.
- Supporting administrative and operational tasks.
- Generating ideas, suggestions, or alternative approaches to support professional practice.

All AI-generated outputs must be reviewed for accuracy by an appropriate member of staff before being used, shared, published, or relied upon.

Use of AI must always comply with the Trust's safeguarding, data protection, information security, copyright, and professional standards requirements.

5. Unacceptable use

The use of AI is not permitted where it:

- Replaces professional judgement, safeguarding responsibilities, or decision-making.
- Breaches the Trust's safeguarding, data protection, information security, copyright, or other applicable policies.
- Involves the use or disclosure of personal, confidential, safeguarding, health, HR, or other sensitive information without appropriate authorisation and safeguards.
- Generates, shares, or publishes content that is inaccurate, misleading, discriminatory, harmful, or otherwise inappropriate.
- Is intended to deceive, misrepresent authorship, or conceal the use of AI where disclosure is required.
- Is unlawful, unethical, or inconsistent with the values and standards of the Trust.

Where there is uncertainty about whether a proposed use of AI is appropriate, guidance should be sought from an appropriate leader or the relevant Trust lead before proceeding.

6. Pupil use of AI

The Trust recognises that AI technologies are increasingly becoming part of everyday life, education, and employment. Where appropriate, pupils may be supported to use AI as part of their learning and digital literacy development.

Any use of AI by pupils must be age-appropriate, educationally appropriate, and consistent with the Trust's Behaviour, Online Safety, Acceptable Use, and Assessment policies.

Pupils should be encouraged to use AI critically and responsibly, recognising that AI-generated content may be inaccurate, incomplete, biased, or misleading.

School leaders remain responsible for determining when and how AI may be used to support learning and assessment activities. This must be discussed and agreed with Trust leaders prior to implementation.

7. Roles and responsibilities

The safe, effective, and compliant use of AI is a shared responsibility. The following roles have specific responsibilities for supporting, governing, and overseeing the use of AI across the Trust.

- Trustees: responsible for providing oversight of the Trust's strategic approach to AI and associated risks.
- Executive Leaders (Director of Communications, IT, and Data): responsible for ensuring appropriate governance, training, data protection compliance, guidance, and controls are in place to support the safe and effective use of AI across the Trust.

- **AI Working Party:** responsible for evaluating emerging AI technologies and practices, developing and maintaining AI-related guidance and training materials, making recommendations regarding the appropriate use of AI within the Trust, and supporting the ongoing review of this policy.
- **Senior Leaders (School SLTs):** responsible for supporting staff to use AI appropriately and for addressing concerns relating to its use within their areas of responsibility.
- **IT Support Team (Head of IT):** responsible for providing advice and guidance on information security, approved technologies, and compliance requirements relating to AI.
- **Staff (all staff users of AI):** responsible for complying with this policy and associated Trust policies, exercising professional judgement, and ensuring that AI-generated outputs are reviewed before being used, shared, or relied upon.

8. Monitoring and review

The Trust will monitor the implementation and effectiveness of this policy and will keep its approach to AI under regular review to reflect changes in technology, legislation, regulation, and educational practice.

Concerns, incidents, or suspected misuse of AI will be managed through the Trust's existing safeguarding, data protection, information security, staff conduct, or disciplinary procedures, as appropriate.

The Trust's AI Working Party will support the ongoing review of this policy and the development of associated guidance, training, and recommended practices.

This policy will be reviewed annually, or sooner where significant changes in legislation, guidance, technology, or organisational requirements make this necessary.

9. Assurance matrix

AI Policy area	Assurance source
Safeguarding	KCSiE; Safeguarding Policy
Data Protection	UK GDPR; Data Protection Act 2018; ICO Guidance
Information Security	DfE Digital & Technology Standards; Information Security Policy
Staff Conduct	Staff Code of Digital Conduct
Pupil Use	Online Safety, Behaviour, and Assessment Policies
Governance & Oversight	Academy Trust Handbook; Governance Handbook
Monitoring & Review	Internal Scrutiny; Risk Management Framework

10. Version Control

Version Control Table v1.0				
Version	Date	Owner	Summary of Changes	Next Review
1.0	4/6/26	DoCID	n/a - first version of the AI Policy.	July 2026
1.1	9/7/26	DoCID	Added changes suggested by our AI Working Group.	July 2027

Approval Record			
Approval Level	Approver	Date Approved	Notes
Document Owner	DoCID	8/7/26	Responsible for document content, maintenance and annual review.
Governance Oversight	ARC Committee (Board of Trustees)	TBC (Aut 2026)	Confirms governance oversight, where required by the Trust's scheme of delegation.

APPENDIX 1. AI guidance for staff

Before using AI, ask yourself:

1. Is this use consistent with the Trust's AI Policy?
2. Am I using an approved tool?
3. Will I be sharing personal, safeguarding, HR, health, or confidential information?
4. Would I be comfortable explaining this use to a parent, colleague, regulator, or inspector?

*If the answer to **any** of the above is "No" or "Unsure" you must seek guidance before proceeding.*

Remember

- AI can make mistakes.
- AI can invent information.
- AI can reflect bias.
- AI should support, not replace, professional judgement.

Always

- Review outputs before use.
- Check important facts.
- Adapt outputs for your audience.
- Apply professional judgement.
- Follow safeguarding and data protection requirements.

Never

- Use AI to make safeguarding decisions.
- Upload confidential information into unapproved tools.
- Assume AI-generated content is accurate.
- Present AI-generated content as verified fact without checking it.

Examples of appropriate use

- Lesson planning
- Resource creation
- Differentiation and accessibility support
- Draft communications
- Meeting summaries
- Brainstorming ideas
- Administrative support

Examples where you will need additional approval before proceeding

- Processing personal data
- Analysing pupil information
- Analysing staff information
- Integrating AI into Trust systems
- Using AI directly with pupils

APPENDIX 2. Approved AI tools register

This register records commonly used AI tools, their status within the Trust, and where applicable, all associated conditions of use.

Tool	Approved Use	Permitted Users	Personal Data Permitted?	Conditions	Review Period
Arbor AI ◆	Access to student information, attendance statistics, AI Smart Reports	Leaders, Teachers, MAST, BSS	Yes (due to internal Arbor data controls and DPA)	n/a	Termly
Gemini for Education ◆	Learning resource creation, administration	Leaders, Teachers, MAST, BSS	No	No personal, safeguarding, HR, or confidential data	Termly
ChatGPT Free ◆	Drafting, planning, resource creation	Staff	No	No personal, safeguarding, HR, or confidential data	Termly
Microsoft Copilot ◆	Not approved for use	Not approved for use	Not approved for use	Not approved for use	Not approved for use

MAST: Multi Agency Support Team | BSS: Business Support Services

Approval status conditions (colour-coded)

1. Approved ◆
2. Approved with conditions ◆
3. Pilot ◆
4. Suspended ◆
5. Not approved ◆

Register Ownership

The register is maintained by the Trust's AI Working Party and reviewed at least annually, or sooner where significant changes occur.

APPENDIX 3. AI procedures

1. Purpose

These procedures support the Trust's AI Policy by establishing a consistent approach to evaluating, approving, implementing, and monitoring the use of AI technologies.

2. Requesting a New AI Tool

Where a member of staff wishes to use an AI tool that is not currently approved by the Trust, they should submit a request to their line manager and/or the designated Trust lead.

The request should include:

- Name of the tool
- Intended use
- Intended users
- Whether personal data will be processed
- Expected benefits
- Any known risks

3. Evaluation Process

The Director of Communications, IT, and Data, with input from the Trust's AI Working Party, will evaluate proposed AI tools against the following criteria:

- Educational or operational benefit
- Safeguarding considerations
- Data protection compliance
- Information security requirements
- Accessibility and inclusion
- Cost and value for money
- Reputational risk

Where required, the Trust may undertake:

- Supplier due diligence
- Data Protection Impact Assessment (DPIA)
- Cyber security review
- Contract review

4. Approval

Following evaluation, the Director of Communications, IT, and Data will recommend one of the following outcomes to the Trust's Executive Leadership Team:

- Approved
- Approved with conditions
- Pilot (to support further/deeper review)
- Not approved

Final approval remains subject to the Trust's established governance and decision-making arrangements.

The outcome and, where appropriate, next steps will then be communicated to the original requester.

5. Monitoring

Approved AI tools will be reviewed periodically to ensure they remain:

- Safe
- Effective
- Compliant
- Appropriate for Trust use

Significant incidents or concerns may result in approval being suspended or withdrawn.

6. Reporting concerns

Concerns relating to AI should be reported through existing Trust procedures, including:

- Safeguarding procedures
- Data protection incident reporting
- Information security incident reporting
- Staff conduct procedures