

# **JOHN TAYLOR MULTI ACADEMY TRUST**



## **Artificial Intelligence (AI) Policy**

Implementation date: November 2025

Next Review Date: June 2026

Policy Owner: Mark Crompton (Director of Technology & Information)

## 1. Purpose

The purpose of this policy is to set out the Trust's expectations for the safe, ethical, transparent and legally compliant use of Artificial Intelligence (AI) across all Trust schools. AI must be used to **support professional practice**, not to replace it. AI should reduce workload where appropriate, but **must not be used to produce work that a member of staff is incapable of producing or validating themselves**.

AI presents opportunities to improve administration, enhance teaching, support pupil learning, identify patterns in data and automate repetitive tasks. However, AI also presents risks relating to data protection, safeguarding, misinformation, assessment integrity, cybersecurity and professional competency. This policy provides a consistent Trust-wide framework for managing both the benefits and risks of AI.

## Policy Source and Development Statement

This Artificial Intelligence (AI) Policy has been developed using a combination of nationally recognised guidance, best practice and Trust-specific requirements. It draws substantively from the **Derbyshire "AI-Policy-2025" template** and the **SWGfL Artificial Intelligence in Schools Policy Template**.

The policy is further informed by current national guidance, including:

- The **Department for Education (DfE)** advice on the safe and responsible use of generative AI in education;
- The **Joint Council for Qualifications (JCQ)** guidelines on the use of AI in assessments; and
- The **Information Commissioner's Office (ICO)** guidance on AI, data protection, and the appropriate handling of personal and sensitive data.

Where appropriate, the policy includes Trust-specific additions to ensure compliance with local governance arrangements, safeguarding obligations and the Trust's approach to educational integrity, staff practice, and data protection.

## 2. Scope

This policy applies to:

- All employees of the Trust (including temporary staff, agency staff and contractors).
- All volunteers and governors using Trust systems.
- All pupils using AI for learning purposes.
- All devices and systems owned, managed or connected to the Trust network.
- AI systems used for teaching, administrative, operational or analytical purposes.

## 3. Definitions

**Artificial Intelligence (AI)** – any system capable of generating text, images, audio, video, analysis or decisions using machine-learning or algorithmic processes (including generative AI such as ChatGPT, Copilot, Gemini, Bromcom AI modules and similar tools).

**Generative AI** – tools which create new content based on prompts (e.g., text summarisation, lesson ideas, feedback statements, report drafts).

**Automated Decision-Making** – decisions made by AI without human input.

**AI-Assisted Content** – any document, message, resource or communication that is partially or wholly generated using AI tools.

## 4. Roles & Responsibilities

- **Trust Board** - Sets strategic direction and approves AI policy.
- **Director of Technology & Information** - Monitors implementation and risk management.
- **Headteachers** - Ensure compliance within their school.

- **Data Protection Officer** - Oversees DPIAs, compliance and data governance.
- **Staff** - Follow the policy, use AI safely, report concerns.
- **Pupils** - Use AI responsibly and follow school rules.

## 5. Monitoring & Review

This policy will be reviewed annually or sooner if:

- DfE or ICO guidance changes.
- New AI systems are introduced.
- Significant incidents occur.
- There is evidence of non-compliance.

## 6. Core Principles

1. **AI supplements but does not replace human judgement.**  
All AI outputs must be **reviewed, checked, and validated** by a human. Staff retain full ownership and responsibility for any output produced with AI assistance.

AI may never be used to autonomously make decisions affecting pupils, staff or third parties e.g. the use of AI to shortlist candidates for a vacancy.

2. **AI must not produce work the user cannot personally explain or create independently.**  
Staff must retain the professional competencies associated with their role.  
*Example:* A teacher who has never written a parental communication cannot rely solely on AI to construct it.
3. **AI use must be transparent.**  
Staff should disclose meaningful AI assistance in internal professional output (e.g., policies, reports, summaries).
4. **AI may not process personal, sensitive or safeguarding data unless specifically authorised.**  
Public AI platforms must never be used because any data entered may be used to train external models and becomes irretrievable and outside the control of the user and the Trust.
5. **AI must be secure and approved.**  
Only AI tools approved by the Trust and subject to a DPIA may be used – See **Appendix A**.
6. **AI must not undermine learning or assessment integrity.**  
AI must never be used by pupils for work intended to assess their independent understanding, this is determined by the Trust, which also approves all systems permitted for use in teaching, learning and assessment.

## 7. Acceptable Use (Staff)

Staff **may use AI** for:

- Drafting lesson ideas, plans, or schemes of work.
- Summarising professional reading, long documents or meeting notes (with no personal data).
- Producing administrative templates.
- Generating exemplars, model answers or marking rubrics.
- Reducing repetitive workload tasks.

Staff **must not**:

- Enter personal data of parents, pupils, staff or governors into unauthorised AI tools.
- Use AI to write safeguarding records, SEND notes, behaviour logs or incident reports.
- Use AI to write academic reports or feedback without full review and editing.
- Produce work relying solely on AI that the staff member could not produce independently.

- Use AI note-takers to record meetings without a DPIA + explicit consent.
- Use AI for JCQ-regulated assessments except in permitted ways.

**The above is intended to be indicative of our general approach, not an exhaustive list.**

## **8. Acceptable Use (Pupils)**

The Trust does not envisage primary aged pupils using AI.

Pupils may use AI:

- As part of structured classroom tasks.
- Under teacher supervision.
- With clear learning intentions and boundaries.

Pupils may not use AI:

- To complete assessed work including homework.
- To produce content misrepresenting themselves or others.
- To create deepfakes, manipulated images, synthetic sexual imagery or harmful content.
- To bypass independent thinking, reading or problem-solving.

## **9. Data Protection & GDPR**

### **9.1 DPIA Requirements**

A Data Protection Impact Assessment (DPIA) is required for any AI system that:

- Processes identifiable personal data.
- Analyses pupil behaviour, performance or patterns.
- Performs predictive analytics (attendance risk, attainment prediction).
- Includes note-taking or transcription functionality.
- Integrates with other Trust systems.

The Trust Data Protection Lead and Data Protection Officer are responsible for approving AI systems and any DPIAs.

### **9.2 Personal Data**

Staff must not:

- Store personal data on AI tools outside the Trust environment.
- Use public AI tools for communications containing names or identifiers.
- Use AI to process safeguarding or sensitive category data.

## **10. Safeguarding & Online Safety**

AI may introduce specific safeguarding threats, including:

- Deepfakes of pupils or staff.
- Nudification tools producing synthetic child sexual imagery.
- AI-assisted grooming or impersonation.
- Mis/dis-information harmful to pupils wellbeing.

Schools must include AI risks within:

- The Safeguarding/Child Protection Policy/Procedure.
- PSHE and digital citizenship curriculum.

- Staff safeguarding training.
- Behaviour and Anti-Bullying Policies.

Any AI-related safeguarding concern must be escalated immediately to the Trust.

## **11. Curriculum Expectations**

All schools must integrate age-appropriate AI literacy covering:

- Bias, fairness and ethical issues.
- Misinformation, hallucinations and reliability.
- Risks of deepfakes, manipulation and impersonation.
- Safe prompting (no personal data).
- Understanding how AI is used in the workplace.

AI must not replace core learning or independent study.

## **12. Assessment Integrity**

In line with **JCQ 2024 guidance**:

- AI cannot be used in any controlled assessment, coursework or examination unless explicitly allowed.
- Pupils must receive explicit teaching on acceptable academic practice.
- Teachers must design assessments that ensure genuine understanding.
- Staff must clearly differentiate between AI-assisted and independently-produced work.

## **Appendix A - Approved AI Tools**

The Trust maintains an **AI Approved Tools Register**, including:

- Microsoft 365 Copilot (subject to DPIA)
- Bromcom MIS AI Functions (subject to DPIA)
- Trust-approved teaching/learning AI tools

No other AI tools may be used unless formally approved.

## Appendix B - AI Risk Assessment Matrix

### 1. Data Protection, Privacy & Legal Compliance

Risk	Description	Likelihood	Impact	Level	Controls
Personal Data Entered into Unauthorised AI	Staff/pupils input identifiable information into public tools.	Medium	High	High	Policy, Acceptable Use Policies, blocking, DPIA, training
AI Note-Takers Recording Meetings	Automated transcription without consent or DPIA.	Medium	High	High	Prohibited unless consent + DPIA
Inaccurate "Hallucinated" Output	AI invents false information.	High	Medium	High	Mandatory verification, labelling
Automated Decision-Making	AI suggests/automates decisions about pupils.	Low	High	Medium	Human decision only

### 2. Safeguarding, Behaviour & Pupil Welfare

Risk	Description	Likelihood	Impact	Level	Controls
Deepfakes & Synthetic Media	Misuse to bully or humiliate pupils.	Medium	High	High	Curriculum, sanctions, monitoring
AI-Assisted Grooming	Impersonation or harmful contact.	Medium	High	High	Staff training, filtering
Nudification Tools	Synthetic sexual imagery.	Medium	High	High	Zero tolerance, reporting
Pupil Overuse / Dependency	Anxiety or loss of resilience.	Medium	Medium	Medium	PSHE curriculum

### 3. Teaching, Learning & Assessment

Risk	Description	Likelihood	Impact	Level	Controls
Over-Reliance on AI by Staff	Erosion of core skills.	Medium	High	High	Policy, appraisal oversight
Misaligned Lesson Content	AI generates inaccurate lesson content.	Medium	Medium	Medium	Teacher validation
AI-Assisted Plagiarism	Pupils submit AI-generated work.	High	Medium	High	JCQ training, assessment redesign

### 4. Bias, Fairness & Ethics

Risk	Description	Likelihood	Impact	Level	Controls
Algorithmic Bias	Misclassification affecting marginalised groups.	Medium	High	High	Review analytics
Stereotyping Outputs	AI generates harmful or biased content.	Medium	Medium	Medium	Review, reporting

## 5. Technical & Cybersecurity

Risk	Description	Likelihood	Impact	Level	Controls
AI-Driven Phishing	Highly realistic fraud attempts.	High	High	High	Staff training, filtering
Data Leakage via Integrations	Plugin/extension access to data.	Medium	High	High	Lockdown integrations

## 6. Operational & Reputational

Risk	Description	Likelihood	Impact	Level	Controls
Inconsistent Implementation Across Schools	Fragmented adoption.	Medium	Medium	Medium	Central governance
Parent Misunderstanding of AI	Fear or mistrust.	Medium	Medium	Medium	Transparent communication

## 7. Risk Information

### 7.1. Risk Categories

Risks are grouped into:

- Data Protection, Privacy & Legal Compliance risks
- Safeguarding, Behaviour & Pupil Welfare risks
- Teaching, Learning & Assessment risks
- Bias, Fairness & Ethics risks
- Technical & Cybersecurity risks
- Operational & Reputational risks

### 7.2. Risk Levels

- LOW (Green): Minimal disruption; manageable through routine controls.
- MEDIUM (Amber): Requires increased monitoring and specific mitigation.
- HIGH (Red): Requires immediate action and senior oversight.

### 7.3. Risk Monitoring

- Reviewed termly by Trust Executive Team
- Reviewed annually by the Trust Board
- Updated after any AI incident
- Updated when new tools are introduced

Each school must report emerging or potential AI-related risks immediately.

## Appendix C – AI Curriculum Guidance (Suggestions)

AI literacy is essential for preparing pupils for modern life. The Trust embeds age-appropriate AI understanding into the curriculum from Early Years to Post-16.

AI is not a subject in itself but a cross-cutting digital literacy element.

### 1. Primary Phase Expectations (EYFS–Y6)

Pupils should learn:

- What AI is in simple terms (e.g., “machines that make guesses”).
- Examples of AI in everyday life (maps, assistants, spell checkers).
- That AI can be wrong and needs checking.
- That photographs and videos online may be edited or fake.
- That personal data should not be shared with AI.
- Early digital citizenship skills.

Class activities may include:

- Sorting tasks (“how might a machine decide?”)
- Exploring safe AI tools using teacher-guided prompts
- Spotting real vs fake images

### 2. Secondary Phase Expectations (Y7–Y11)

Pupils should understand:

- How algorithms and machine learning work (conceptually).
- How data trains AI — and the risks of biased data.
- Why AI sometimes provides incorrect answers.
- How to question and verify AI responses.
- How deepfakes are produced and identified.
- Ethical issues such as fairness, privacy and deception.
- Responsible use of generative AI for research support.

Students should also learn:

- AI’s role in future careers
- Digital footprints
- Academic honesty in assessments

### 3. Post-16 Expectations

Students should explore:

- Real-world AI applications in specific industries.
- Automation and workforce impacts.
- Safe and ethical use of AI for research projects.
- Data protection and privacy law.

### 4. CROSS-CURRICULAR INTEGRATION

- **Computing:** Algorithms, modelling, responsible tool use.
- **English:** Evaluating AI-generated writing; style, bias, tone.
- **Science & Maths:** Data analysis with teacher-led AI tools.
- **Humanities:** Evaluating sources; misinformation; deepfake analysis.
- **PSHE & Citizenship:** Online safety, digital identity, AI ethics.
- **Careers:** Understanding AI in workplaces.

## 5. Teaching Principles

- AI should **support**, not replace, pupil thinking.
- Teachers must check all AI-produced materials.
- Pupils must never input personal data into AI tools.
- Pupils must learn to question AI, not trust it blindly.
- AI must not be used in assessments unless permitted.

## Appendix D – Parental Information Sheet (Suggestion)

This information sheet explains how Artificial Intelligence (AI) is used safely and responsibly within the Trust.

The Trust follows DfE guidance (2023/24), GDPR requirements and safeguarding frameworks to ensure that AI use supports – not replaces – teaching and learning.

### 1. What is AI and how is it used?

AI refers to computer systems that can create text, analyse data, or assist with tasks.

In schools, AI can help staff by:

- Reducing workload through drafting templates and resources.
- Summarising complex documents.
- Supporting teachers with ideas and planning.
- Helping identify learning patterns using approved systems.

AI **does NOT** replace teachers. All decisions affecting pupils are made by qualified staff.

### 2. How is AI protected and supervised

The Trust uses AI carefully, ensuring:

- Only **approved** tools are used.
- AI does **not** replace staff supervision or judgement.
- AI does **not** make decisions about children.
- AI does **not** handle personal or sensitive information unless approved and protected.
- All AI systems undergo a **Data Protection Impact Assessment (DPIA)** before use.

AI cannot be used for safeguarding documentation, behaviour logs, or SEND records.

### 3. How pupils AI in school – Secondary Pupil Only

Pupils may use AI:

- Under teacher supervision in structured lessons.
- To support digital literacy and critical thinking.
- To understand online misinformation and safety.

Pupils may NOT use AI to:

- Complete homework or coursework dishonestly.
- Create or edit images of other pupils or staff.
- Upload personal information into AI tools.
- Use AI unsupervised during lessons.

### 4. Safeguarding and Online Safety

The Trust ensures pupils are protected from:

- AI-generated misinformation.
- Deepfakes and image manipulation.
- AI-assisted online grooming or impersonation.
- Synthetic imagery and nudification tools.

Pupils receive explicit teaching about:

- Digital safety.
- The limitations and risks of AI.
- How to verify information.

## **5. Data Protection**

We comply fully with the UK GDPR:

- No pupil data is used in public AI tools.
- Only secure, approved platforms are used.
- Only anonymised or non-personal data is used where appropriate.

## **6. How parents can support at home**

Parents are encouraged to:

- Discuss AI use with children and emphasise critical thinking.
- Remind pupils that AI may be incorrect or biased.
- Encourage responsible and ethical use.
- Monitor usage at home and set healthy boundaries.
- Contact the school with any concerns.

## Appendix E – Staff AI Acceptable Use Policy

To be integrated into standard acceptable use policy at next review.

### 1. Introduction

This Acceptable Use Agreement sets out how all staff within the Trust must safely, ethically and professionally use Artificial Intelligence (AI). It ensures compliance with UK GDPR, safeguarding requirements, DfE AI guidance, and the Trust AI Policy.

AI may support professional practice and reduce workload, but it must **not replace professional judgement, understanding, or essential role-based skills**.

AI must not produce work that a staff member is **incapable of producing, checking, or explaining independently**.

### 1. Professional Responsibilities

All staff must:

- Retain full responsibility for any work created using AI.
- Be able to explain, justify and defend any AI-assisted content.
- Not use AI to produce work they could not create independently.
- Check all output for accuracy, appropriateness, bias and tone.
- Declare meaningful AI assistance when creating internal or formal documents.
- Ensure all AI use aligns with safeguarding, GDPR and Trust expectations.

Staff must ensure AI does **NOT**:

- Replace safeguarding, SEND or behaviour documentation.
- Replace pedagogical knowledge or curriculum understanding.
- Replace communication skills required for parental engagement.

### 2. Approved AI Uses

Staff may use AI for:

- Drafting letters, templates, lesson ideas and resources.
- Summarising long or complex documents.
- Drafting administrative documents (risk assessments, checklists).
- Generating exemplars, revision materials or scaffolds.
- Providing structured marking frameworks (never final marks).
- Translating general information (no personal data).
- Automating repetitive tasks.

All output must be reviewed, edited and validated.

### 3. Prohibited AI Uses

Staff must NOT:

- Enter any **personal, sensitive, safeguarding, SEND, or behavioural** data into AI tools.
- Use public AI for communications containing names or identifiers.
- Ask AI to write academic reports, assessments or evaluations without full staff review.
- Use AI notetakers (Otter, Zoom Companion) without **DPIA + explicit written consent** from all attendees.
- Use AI to predict, analyse, classify or profile pupil performance without Trust approval.
- Use AI to generate ANY content related to safeguarding cases.

#### **4. Data Protection**

- Only Trust-approved AI tools may be used.
- No personal data may be uploaded to public AI systems.
- All AI use must follow data minimisation principles.
- A DPIA is required if an AI tool processes or analyses personal data.
- Staff must report AI-related concerns or breaches immediately to the DPO.

#### **5. Safeguarding**

Staff must never:

- Request, create or use synthetic media involving pupils.
- Allow AI content to influence safeguarding decisions.
- Use AI to analyse behaviour or emotional state without DPO approval.
- Discuss safeguarding or pastoral information with AI tools.

All AI-related safeguarding concerns must be escalated to the DSL.

#### **STAFF DECLARATION**

"I agree to follow the Trust's AI Policy and Staff Acceptable Use Agreement. I understand that AI usage remains my responsibility and misuse may result in disciplinary action."

Signature: \_\_\_\_\_ Date: \_\_\_\_\_