Policy Approved:	24 March 2026
Next Review:	April 2027
Effective Date:	25 March 2026

1. Purpose

Unity Schools Trust recognises that artificial intelligence (AI) tools can support teaching, learning and administration when they are used thoughtfully. The purpose of this policy is to:

- encourage responsible and innovative use of AI
- make sure that personal, sensitive and confidential information is not shared inappropriately with AI tools
- ensure that our use of AI is consistent with UK GDPR, safeguarding duties and our wider Trust policies.

The Trust is not opposed to AI. We want staff and pupils to understand how to use it safely, ethically and effectively.

2. Scope

This policy applies to all schools within the Trust, to all staff (including leaders, teachers, support staff, peripatetic staff, volunteers, governors and trustees) and to all pupils. It also applies to contractors or third parties who use Trust systems or data.

It covers all AI tools, including generative tools such as ChatGPT, Microsoft Copilot and Google Gemini, AI features embedded in systems such as Microsoft 365, and any future AI tools adopted by the Trust.

3. What We Mean by AI

For the purposes of this policy, AI refers to technologies that can analyse or generate text, images, audio, video or code, or that make predictions or recommendations in ways that imitate elements of human intelligence. Generative AI tools are those that can produce new content in response to a prompt, such as writing an email, creating an image or generating code.

4. Key Principles

The Trust's approach to AI is based on the following principles:

1. AI should be used where it has clear educational or operational benefit.
2. AI must always be used with a "human in the loop". Staff remain responsible for checking the quality, accuracy and fairness of any AI output.

3. Personal data, special category data and confidential Trust information must not be shared with external AI tools unless the tool has been formally approved for that specific purpose.

4. AI use must never undermine safeguarding, equality, or our obligations to keep pupils and staff safe.

5. AI must not be used in ways that mislead others about authorship, originality or assessment outcomes.

5. Roles and Responsibilities

The Chief Executive Officer holds overall responsibility for the safe and lawful use of AI across the Trust.

The Chief Technology Officer (CTO) leads on technical implementation, security controls and the approval of AI tools and integrations.

The Trust Data Protection Officer (DPO) advises on data protection and carries out, or supports, data protection impact assessments where AI tools are being considered.

Principals are responsible for implementing this policy in their schools.

The IT team supports configuration, access controls and monitoring.

All staff and all pupils must follow this policy and report any concerns or incidents promptly.

6. Information That Must Not Be Uploaded to AI Tools

Unless a tool has been explicitly approved for a particular purpose, the following must not be entered into any AI tool by staff or pupils:

Personal and special category data
This includes names or identifiable details of pupils, parents, carers, staff, governors, volunteers or contractors; pupil identifiers such as UPNs and candidate numbers; email addresses, phone numbers and postal addresses; HR records and payroll information; health, SEND, EHCP and medical information; behavioural, safeguarding or disciplinary records; photographs, videos or audio clips that identify individuals.

Confidential Trust information
This includes: internal financial information, budgets and salary details; system information such as usernames, passwords, Wi-Fi keys, VPN details, network diagrams, firewall rules and security logs; contracts, tender documents and commercially sensitive information that is not already public.

Assessment and examination materials
Live or unpublished examination questions, exam papers or controlled assessments must not be uploaded. Where exam boards permit particular uses of AI, staff must follow those specific rules.

Third-party copyrighted materials
Textbooks, purchased resources and other licenced content must only be shared with AI tools if the licence terms clearly allow it.

A simple rule of thumb for everyone is: if you would not send the information to an unknown company by email, you should not paste it into an AI tool.

7. AI Use by Staff

7.1 Appropriate Use

Staff may use AI to support teaching, learning and administration where it is helpful and low risk. Typical uses include:

- generating ideas for lessons, examples, questions or activities
- improving or differentiating explanations of a topic
- drafting generic resources such as worksheets, rubrics and checklists, provided they do not contain personal data
- drafting routine communications that do not contain personal or confidential information
- obtaining help with code or scripts using anonymised or synthetic data.

Staff are expected to read and edit AI outputs, to ensure they are accurate, age-appropriate and aligned with Trust values. AI should be seen as a tool to support professional judgement, not a replacement for it.

7.2 Data Protection and Confidentiality

When using AI, staff must remove or anonymise personal details before using real examples. Names should be replaced with neutral labels such as “Pupil A” and any identifying details should be changed. Staff must not upload pupil records, safeguarding information, behaviour logs, HR files or financial information into general AI tools.

Where AI features are built into Trust-managed systems, for example within Microsoft 365, staff should still avoid unnecessary sharing of sensitive information and should follow any specific guidance issued by the Trust.

7.3 Academic Integrity and Decisions

Staff must not use AI as the sole basis for academic, disciplinary or pastoral decisions about pupils or colleagues. AI can assist with drafting reports or comments, but final wording should be checked carefully and reflect genuine professional judgement.

Where AI is used in relation to assessment, staff must ensure their approach is consistent with exam board rules and the school’s assessment and academic honesty policies.

7.4 Use of Tools and Accounts

Staff should, wherever possible, use AI tools that the Trust has approved and made available through Trust accounts. Staff must not connect unapproved AI tools or plug-ins directly to Trust systems such as OneDrive, SharePoint or the MIS. Personal accounts on AI platforms must not be used to process Trust documents or data. The current approved integrated AI is Co-Pilot.

8. AI Use by Pupils

8.1 General Approach

Pupil use of AI should be planned and age appropriate. AI can help pupils to explore ideas, see concepts explained in different ways and practise skills, but it must not replace their own thinking or effort.

Teachers should set clear expectations about when AI may be used in a subject and when it may not. They should explain that AI can make mistakes and may be biased, so it must always be treated as a tool rather than a source of unquestioned truth.

8.2 What Pupils Must Not Do

Pupils must not:

- share personal information about themselves or others with AI tools. This includes full names, addresses, contact details, usernames and passwords
- upload or generate photos, videos or audio that identify individuals without clear permission from staff and appropriate consent
- use AI to create abusive, hateful, discriminatory, sexually explicit or violent content
- use AI to bully, threaten or harass others, or to create fake content that misrepresents someone
- use AI to complete homework, coursework or assessments where the teacher has said that AI use is not allowed
- attempt to bypass school filtering, security or monitoring systems to access AI tools.

8.3 Using AI to Support Learning

When a teacher allows AI to be used, pupils may use it to get alternative explanations of a topic, generate practice questions, check their understanding or gain ideas for improvement. Teachers may also ask pupils to reflect on how they used AI and what they learned from it.

Work that is submitted must still represent the pupil's own understanding. A teacher may ask to see drafts, notes or evidence of the process to confirm that AI has been used appropriately.

9. Safeguarding and Online Safety

All AI use in the Trust sits within existing safeguarding and online safety frameworks. Any AI-related concern, such as harmful content, harassment, deepfakes or attempts to exploit pupils, must be reported using the standard safeguarding procedures.

Where the Trust deploys AI tools for pupil use, it will, as far as reasonably possible, configure them with age-appropriate settings and monitoring.

10. Approval, Monitoring and Review of AI Tools

New AI tools or integrations that will process Trust data or be used widely across schools must go through an approval process led by the CTO, CEO, MAT Education Director and DPO. This includes consideration of educational benefit, data flows, security, lawful basis, contractual terms and any required data protection impact assessment.

The Trust may monitor use of AI tools on Trust devices and networks in line with existing monitoring and acceptable use policies. Monitoring is carried out for safeguarding, security, training and policy enforcement.

This policy will be reviewed at least annually, or sooner if there are significant changes in law, regulatory guidance or Trust use of AI.

11. Incidents and Breaches

If personal, sensitive or confidential information is accidentally uploaded to an AI tool, or if an AI-related incident raises safeguarding or security concerns, this must be reported immediately through the usual IT or Data Protection channels. The Trust will manage potential data breaches in line with its Data Breach and Incident Response procedures, including notification to the ICO where required.