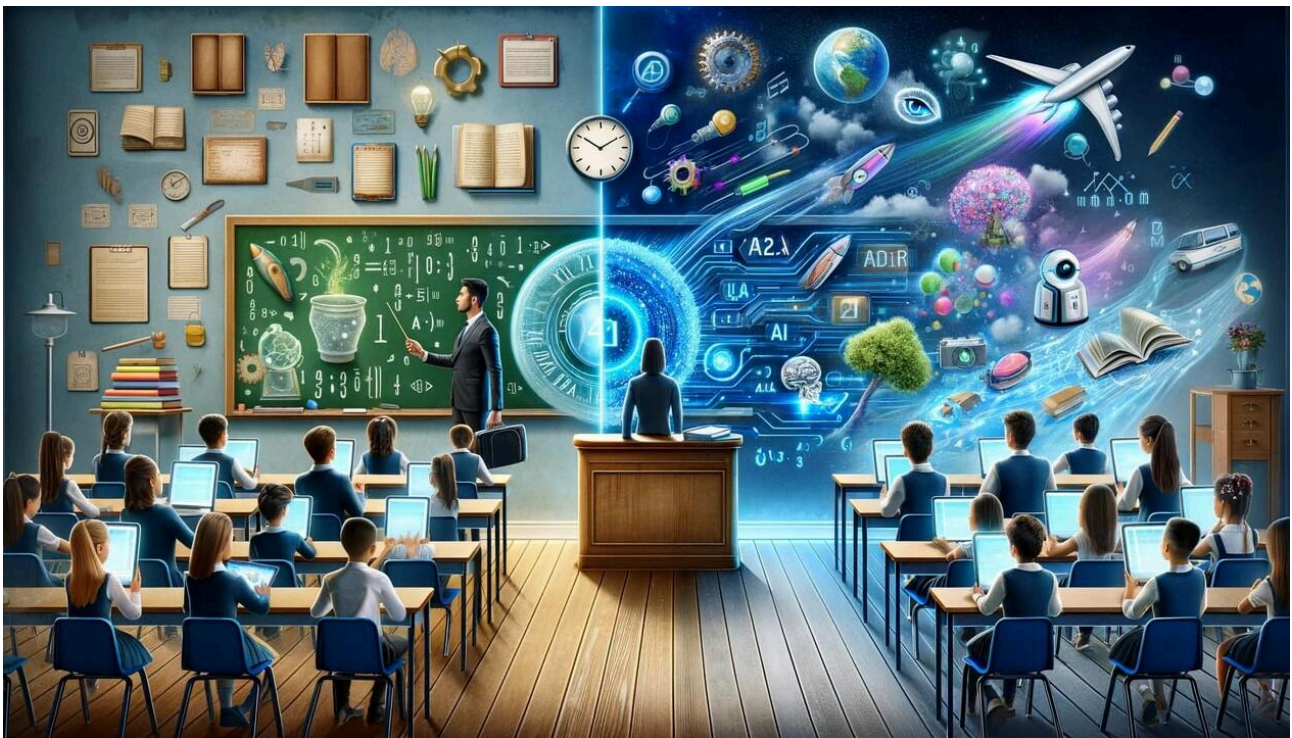




# Artificial Intelligence Policy



## The Stour Federation

Date of publication: May 2026

Review date: September 2027

This foundation of this policy is based on the work of [ICT Evangelist](#) and is protected by a Creative Commons License: CC BY-NC-SA 4.0. This licence requires that reusers give credit to the creator. It allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, for noncommercial purposes only. If others modify or adapt the material, they must license the modified material under identical terms.

Additions and amendments have been made to be in line with The National Society for Education's *Fully Human: AI and the Flourishing (Small) School of the Future* working group

## 1. POLICY STATEMENT

The Stour Federation views Artificial Intelligence not merely as a tool for efficiency, but as a means to amplify human potential. In line with our 2030 Strategy, we leverage technology to create headroom for what is fully human: pastoral care, building communities of belonging, and spiritual development. We believe that while AI can handle the "heavy lifting" of administration and resource generation, it can never replace the uncountable human elements of care, collective wisdom sharing, and deep empathy.

We evaluate all AI integration through three reflective lenses:

- **The Use Lens:** Focuses on the practical "how," ensuring staff competency and high-quality "use cases" for teaching and learning.
- **The Human Lens:** Asks "who" is being formed, ensuring AI use enhances human flourishing and supports our belief that every individual is unique and precious.
- **The Mission (Vision) Lens:** Evaluates the "why" through the unique DNA of our schools, ensuring AI nurtures Christian values and service to others.

This policy ensures compliance with:

- Keeping Children Safe in Education (KCSIE).
- UK GDPR and Data Protection Act 2018.
- DfE Guidance on Generative AI in Education 2025.
- JCQ Guidance on AI in Assessments 2024.
- The Stour Federation's Acceptable Use Policy (AUP), Online Safety Policy, Data Protection Policy and Information Security Policy

This policy applies to all staff, children, governors and third-party providers who use AI in the school environment.

## 2. REGULATORY PRINCIPLES

AI is rapidly becoming an integral part of education, influencing teaching methods, administrative processes, and student learning. This section outlines where AI applies within The Stour Federation and the principles governing its responsible use.

This policy applies to all AI tools, platforms, and applications used within The Stour Federation, including:

- AI tools used for teaching, learning, assessment, and administration.
- Any third-party AI platforms accessed by students or staff in a school-related capacity.
- AI systems embedded in school-approved software and services.

The Trust adheres to the five principles of AI regulation to ensure safety and ethics:

- **Safety, Security, and Robustness:** We prioritise the safeguarding of learners and will not use technology that increases risk.
- **Appropriate Transparency:** We are open about where AI is used and how it informs teaching or administrative suggestions.
- **Fairness:** We actively monitor and rectify algorithmic bias, particularly regarding protected characteristics, to ensure equitable outcomes for all pupils.
- **Accountability:** Humans remain professionally responsible for all AI-generated output. AI must never make independent decisions affecting students or staff.
- **Contestability and Redress:** Staff are empowered to overrule AI suggestions. Decisions are made by the human user, not the technology.

### 3. ROLES AND RESPONSIBILITIES

Effective oversight and accountability are essential to ensure AI is used appropriately and safely within the school. The following sections define the key responsibilities of school leadership, staff, children, and IT teams in managing AI systems.

#### Leadership and Governance

Trust and school leadership plays a vital role in overseeing AI governance, ensuring policies align with national regulations, and implementing best practices for safe and ethical AI use.

- Ensure AI governance aligns with DfE, KCSIE, and GDPR regulations.
- Approve AI tools before they are used in teaching, learning, or administration.
- Conduct annual AI risk assessments and policy reviews.
- Ensure AI use is transparent, fair, and free from bias.
- Leadership and Governance teams must engage in regular update training to ensure compliance and risk mitigation for the latest risks.
- Leaders will actively listen to staff concerns and manage the "AI anxiety" caused by rapid technological change through transparent communication.

#### Teaching and Support Staff

Teachers and support staff are responsible for ensuring AI is used as an educational aid while maintaining academic integrity, supporting student learning, and preventing misuse.

- Use AI as a teaching aid, not as a replacement for pedagogy.
- Educate students on AI literacy, misinformation, and deepfakes.
- Ensure AI use does not compromise academic integrity or safeguarding.
- Staff are encouraged to use AI to streamline "countable" tasks (lesson planning, resource generation) so they can prioritise relational work such as mentoring and SEND support.
- Teaching and Support staff must engage in annual update training to ensure compliance and risk mitigation for the latest risks.
- Staff must develop the skills to critically evaluate AI for accuracy, currency, and bias, providing necessary human context to all digital materials

#### Pupils

Students must develop an understanding of AI's capabilities and limitations while using AI tools ethically and responsibly within the guidelines set by the school.

- Use AI tools responsibly and in line with school policies.
- Declare AI use in coursework, assignments, and assessments where required.
- Understand ethical considerations and avoid over-reliance on AI.
- Pupils will be taught not just how to use AI, but how to discern between reliable and unreliable information, protecting their own privacy and respecting the intellectual property of others.

### **IT and Data Protection Teams**

The IT and Data Protection teams are responsible for ensuring AI systems comply with data protection laws, cybersecurity standards, and safeguarding requirements.

- Implement security measures to ensure AI tools comply with data protection laws.
- Ensure that AI tools used in school settings do not process or store personal data without anonymisation.
- Ensure that all technologies undertake an annual (minimum) DPIA process before use is permitted within The Stour Federation.
- Conduct regular cybersecurity audits to monitor AI-related risks.
- IT and Data Protection teams must engage in annual update training to ensure compliance and risk mitigation for the latest risks.

## **4. DATA PROTECTION AND THE WALLED GARDEN**

In The Stour Federation, our servers and chromebooks are managed by the Warwickshire ICT Development Service. Only staff devices have access to our approved AI tools - Microsoft Copilot, Google Gemini and Oak National Academy (Aila).

Our Data Protection Officer is a service provided by Warwickshire Legal Services.

AI should be implemented in ways that are fair, transparent, and aligned with ethical considerations. This section outlines the key principles for ensuring AI use remains accountable, unbiased, and secure.

### **Open vs. Closed AI Tools**

- **Closed Generative AI (Approved):** Currently, the Trust permits the use of Microsoft Copilot, Google Gemini, and Google NotebookLM. These are "closed" or enterprise-grade tools where data is generally more secure.
- **Open Generative AI (Prohibited):** Staff must not enter identifiable student or staff data into "open" tools that store or learn from user inputs.

### **Transparency and Accountability**

It is essential that AI use within the school remains transparent, and that decisions made using AI are documented and subject to human oversight.

- AI must not be used to make independent decisions affecting students or staff.
- The use of AI in assessment, recruitment, or administrative decision-making must be documented.
- AI-generated content must be identified where used.

### **Bias and Fairness**

AI systems must be reviewed and monitored to minimise bias, ensuring fairness in learning,

assessment, and administrative decision-making.

- AI tools must be vetted to ensure fairness and prevent bias.
- Training must be provided to recognise AI bias and hallucinations and mitigate its impact.
- Human checking is required for all AI output.
- All stakeholders are responsible for any output shared that has been generated by AI.

### **Data Protection and Anonymisation**

To comply with data protection regulations, AI tools must not process personal data unless approved. Where possible, anonymisation techniques should be used to protect individual privacy.

- AI tools must not process or store personally identifiable student or staff data unless explicitly approved by the IT and Data Protection teams.
- AI inputs should be anonymised where possible.
- A Data Protection Impact Assessment (DPIA) must be conducted before new AI tools are introduced. Colleagues are NOT allowed to install or use any new software without prior permission from the IT and Data Protection team.

## **5. AI IN TEACHING, LEARNING, ASSESSMENTS AND ACADEMIC INTEGRITY**

AI integration is prioritised where it supports Equity and Inclusion:

- **Special Educational Needs (SEND):** Using AI for adaptive teaching and to provide personalised support for pupils with specific learning needs.
- **Adaptive Teaching:** Leveraging AI to activate prior knowledge and provide responsive feedback, ensuring every child reaches their potential.
- **Workload Reduction:** Using AI as a tool for heavy-lifting tasks, allowing teachers to focus on "unreasonable hospitality" and connection.

AI must not compromise academic integrity. To maintain assessment integrity, children must declare AI-assisted work, and staff must monitor submissions for signs of unauthorised AI use.

## **6. SAFEGUARDING AND ONLINE SAFETY**

AI must be used safely within the school environment, preventing harm and ensuring students and staff understand the potential risks associated with AI-generated content.

### **Preventing AI-Generated Harm**

- AI tools must not be used to create harmful, misleading, or inappropriate content.
- Children and staff must be trained to recognise AI-generated deepfakes, misinformation, and impersonation risks.
- The school's filtering and monitoring systems must detect and prevent AI-generated threats (as per the Government's Filtering and Monitoring standards).

### **AI and Cybersecurity**

As AI systems become more integrated into school operations, cybersecurity risks must be managed to prevent unauthorised access, phishing attempts, and data

breaches.

- AI-related phishing scams, fraud, and cybersecurity risks must be monitored.
- IT teams must ensure AI tools do not introduce security vulnerabilities.

## **7. MONITORING AND REVIEW**

AI technologies and regulations evolve rapidly. This section ensures the school regularly reviews its AI policy, assesses risks, and gathers feedback to maintain compliance and best practices.

- This policy will be reviewed annually in line with updates to DfE, KCSIE, and JCQ guidance.
- DPIA risk assessments will be conducted before any new AI tool is introduced.
- Feedback will be sought from staff, students, and parents on AI's impact in education.