



ACHIEVING TOGETHER

FOUR STONES GATEWAY TRUST

AI POLICY

DATE POLICY WAS APPROVED	23.04.2026
DATE POLICY WILL BE REVIEWED	Spring 2027
MEMBER OF STAFF WITH RESPONSIBILITY FOR REVIEW	Head of IT Services

FOUR STONES GATEWAY TRUST

Love Lane, Cleobury Mortimer, Shropshire, DY14 8PE · 01562 826580

office@fourstonesgateway.org.uk · www.fourstonesgateway.org.uk

Four Stones Gateway Trust is a company limited by guarantee registration number 9115941

Key Definitions

All policies incorporate the following schools or organisations within Four Stones Gateway Trust ('the Trust'):

- Clee Hill Community Academy
- Cleobury Mortimer Primary School
- Haybridge High School and Sixth Form
- Haybridge Teaching School Hub
- Haybridge SCITT
- King Charles I School
- Lacon Childe School
- SHaW (Shropshire, Herefordshire and Wolverhampton) Maths Hub
- Stottesdon CofE Primary School
- TDMS (The De Montfort School)
- Any other schools or organisations that may join the Trust from time to time and not listed above.

The terms Academy, School, Organisation and Trust are considered interchangeable in the context of all Trust policies.

Where appropriate, in this policy the term:

“CEO” includes the Chief Executive Officer

“CFO” includes the Chief Financial Officer

“Trust Senior Leadership Team” includes Executive Headteachers, Headteachers, strategic operational leads and Teaching School/SCITT Directors.

“Headteacher” includes the appropriate School Headteacher.

“Trustees or Trust Board” are appointed Trustees who oversee the business of Four Stones Gateway Trust, agreeing the overarching strategic direction and ensuring robust governance.

“Local Academy Boards (LAB)” are appointed Governors at a local level associated with the Trust's Worcestershire Schools. LAB Governors act as advocates for their school's Safeguarding, SEND, Standards and Stakeholder engagement.

“Local Governing Bodies (LGB)” are appointed Governors at a local level associated with the Trust's Shropshire Schools. LGB Governors are advocates for their school's Safeguarding, SEND, Standards and Stakeholder engagement.

“Chair” responsible for leading the board and ensuring its effectiveness

“Stakeholders” are any individuals or companies who are invested in the welfare and success of the Trust and/or School and its students, including staff members, students, parents, community members, LAB, LGB or Trust members, trade unions, local business leaders etc.

Contents

1. Guiding Principles	3
2. Roles and Responsibilities	3
3. Ethical Considerations	4
4. Data Privacy and Security	4
5. Bias and Fairness	4
6. Transparency and Explainability	5
7. Professional Development	5
8. Compliance and Monitoring	5
9. Communication and Transparency	5
Appendix A – Key Terms	6
Appendix B – Key Performance Indicators	7
Appendix C – Risk Assessment Matrix for using AI Technologies in School	8

This policy outlines the guidelines and procedures for the ethical and responsible use of artificial intelligence (AI) technologies by all staff members in the Four Stones Gateway Trust. As a Trust committed to fostering learning, innovation and ethical citizenship, it is imperative that we leverage AI technologies effectively whilst prioritising the wellbeing, privacy and dignity of all individuals involved. Key terms related to AI can be found in Appendix A.

1. Guiding Principles

The Trust recognises the transformative potential of artificial intelligence (AI) in enhancing educational outcomes, administrative efficiency, and organisational effectiveness. However, we also understand the importance of ensuring that AI systems operate within ethical boundaries and align with our core values. To this end, we have established the following guiding principles to govern the development, deployment, and use of AI within our Trust:

- **Fairness:** We design, procure and use AI that does not discriminate, and test, audit and monitor for bias with prompt action to address any identified biases or inequities.
- **Transparency:** We explain AI purpose and strive to maintain transparency in the design, operation, and outcomes of AI systems, providing clear explanations so stakeholders can make informed decisions.
- **Accountability:** We accept responsibility for the outcomes of AI systems deployed within our Trust and establish clear lines of accountability for its development and deployment.
- **Privacy:** We implement measures to restrict, anonymise and protect personal data used by AI systems, minimising the risk of unauthorised access, misuse, or data breaches.
- **Equity:** We use AI to reduce barriers and support inclusive practice so all learners benefit equitably.

2. Roles and Responsibilities

Trust Leadership

- **Head of IT Services** - is ultimately accountability for AI implementation: strategy, policy approval and legal/ethical compliance; leads technical implementation, security and technology road-mapping.
- **Director of Curriculum and Learning** - ensures initiatives align to mission and pedagogy; steers adoption and resources.
- **Trust and in-school leaders** - operates KPI framework (Appendix B), evaluates impact and drives improvements.

Data Protection and Data Teams

- **Data Protection Representatives** - ensures GDPR compliance; conducts privacy impact assessments; oversees data lifecycle and handles inquiries/incidents.

- **Data Leads / Heads of Data** - owns datasets used by AI; ensures data quality, accuracy and ethical use in collaboration with developers.

IT Support Team - evaluates case studies and models performance; integrates AI with Trust infrastructure; ensures compatibility, reliability and scalability.

Educational Staff - co-designs and adopts AI tools; integrates into teaching; monitors engagement/outcomes; completes AI/data-literacy training.

3. Ethical Considerations

The Trust prioritises ethical considerations as we integrate AI technologies into our classrooms and education processes to ensure that the well-being, autonomy, and learning outcomes of our Students/Pupils remain paramount. The following ethical principles serve as foundational guidelines for the responsible use of AI within our educational context.

- **Equity and inclusion:** we ensure AI Technologies are accessible tools to enhance equity and inclusion in education and acknowledge the potential for AI to exacerbate existing inequalities if not implemented thoughtfully.
- **Transparency and accountability:** we explain how tools are used and be transparent about the data collected and how it is used to inform decision-making.
- **Data privacy and security:** we adhere to strict data protection protocols, ensure that AI systems comply with relevant data privacy regulations and share with AI systems only after approved risk assessment (Appendix C).
- **Student/Pupil autonomy and agency:** we advocate that AI should complement and enhance, not replace, Student/Pupil judgement and learning experiences.
- **Bias and fairness:** we regularly evaluate for bias and mitigate promptly.
- **People-centred design:** we prioritise Student/Pupil and Staff needs and context.
- **Continuous reflection and improvement:** we review practices with stakeholder input as technology and norms evolve.

4. Data Privacy and Security

The Trust recognises the importance of safeguarding Student/Pupil and staff data privacy and security in the age of digital advancement. As custodians of sensitive information, every member of the Trust community plays a critical role in upholding the highest standards of data protection. The following outlines the roles and responsibilities concerning data privacy and security:

- **Standards and Curriculum Committee** - sets policy, ensures UK GDPR alignment, resources and oversees implementation.
- **Data Protection Officer (DPO)** - leads governance, audits, risk assessments, policy and training.
- **School Leaders and Administrators** - implements policy locally; restricts access; runs risk assessments with DPO and reports incidents promptly.
- **Teaching and Support Staff** – utilises only necessary data; obtains required authorisations; follows retention and consent rules and completes mandatory training.
- **IT Support Team** - applies technical controls (firewalls, encryption, access); patches; monitors and audits; operates backup/recovery.
- **External Partners and Service Providers** - uses vetted vendors under contract with clear data-protection clauses; performs due diligence.

5. Bias and Fairness

The Trust acknowledges that AI systems have the potential to perpetuate and even exacerbate biases present in data or inadvertently introduce new biases. Therefore, it is imperative for us to actively mitigate bias at every stage of the AI lifecycle and continuously evaluate our systems for fairness and inclusivity.

- **Identify bias:** we use diverse datasets; review collection and algorithms for inclusivity.
- **Mitigate bias:** we build diverse teams; prefer transparent models; run regular audits; deploy bias-aware techniques.
- **Evaluate and accountability:** we monitor metrics by group; assign clear ownership; train staff on bias awareness and mitigation.

6. Transparency and Explainability

The Trust is committed to fostering an environment of trust, accountability, and fairness, it is imperative that the decision-making processes of AI systems are transparent and understandable to all stakeholders, particularly our staff members.

- **Communicate decisions:** We communicate all decisions made in relation to AI systems within our Trust clearly to all stakeholders and provide supportive visuals/interfaces where possible.
- **Training:** We train staff to interpret outputs and to remain informed about advancements in AI technology.
- **Accountability and oversight:** The AI Committee reviews decision making processes, deployments and feedback to address issues or concerns.

7. Professional Development

The Trust is committed to ensuring that our staff members are equipped with the necessary skills and knowledge to harness AI effectively and ethically through comprehensive professional development opportunities in AI literacy and best practice.

- **Training programmes:** regular role-specific AI literacy and ethics training; pedagogy-focused sessions for educators; decision-support for admin teams.
- **CPD hub:** central repository for curated resources, case studies and guidance.
- **Expert support:** access to internal AI specialists, data and IT Support teams.
- **Collaboration:** cross-school projects to share practice and innovation across the Trust.
- **Continuous learning:** support for external courses and conferences.
- **Monitoring and evaluation:** surveys and performance data inform programme updates.

8. Compliance and Monitoring

The Trust acknowledges the importance of adhering to the AI policy to ensure responsible and ethical use of artificial intelligence technologies across all schools within the Trust. The Head of IT Services is responsible for overseeing compliance with the AI policy.

- **AI Champion:** each school appoints a liaison between the Director of Curriculum and Learning and the Head of IT Services.
- **Reporting Mechanisms:** we ensure periodic reviews of usage, data handling and legal compliance; corrective action and training for issues found.
- **Regular review:** we review at least annually with stakeholder input; communicate updates and provide training as needed.

9. Communication and Transparency

The Trust recognises the importance of fostering open communication channels between all stakeholders involved in our educational community. This includes staff members, Parent/Carers, Student/Pupils and any other relevant parties. As we integrate AI initiatives into our educational practices, we are committed to ensuring transparency and facilitating dialogue to address any questions, concerns, or uncertainties that may arise.

- **Regular updates:** we use meetings, briefings, bulletins, emails, website and social channels to explain purpose, impact and changes.
- **Open forums and workshops:** we enable dialogue and shared learning across stakeholders.
- **Feedback mechanisms:** we have clear feedback routes for Staff, Parents/Carers and Student/Pupils to raise questions and suggestions.
- **Transparent decisions:** we publish rationale, evaluation criteria and risk considerations; maintain oversight and routes for recourse.

Appendix A – Key Terms

Term	Definition
Accountability	The principle that individuals, organisations, or systems responsible for the development, deployment, and use of AI should be answerable for their actions, decisions, and impacts.
AI Committee	A dedicated group responsible for overseeing the ethical and logistical implications of AI initiatives within the Trust, providing guidance, review, and recommendations to ensure ethical and safe AI practices.
AI Literacy	The knowledge and understanding of AI concepts, capabilities, limitations, and ethical considerations among staff members, enabling informed decision-making and responsible use of AI technologies within the organisation.
Algorithm	A set of step-by-step instructions or rules followed by a computer program to solve a problem or perform a specific task.
Artificial Intelligence (AI)	Refers to the development of computer systems capable of performing tasks that typically require human intelligence. These tasks may include learning, reasoning, problem-solving, perception, and decision-making.
Bias	Systematic errors or inaccuracies in AI systems that result from the improper influence of factors such as incomplete or unrepresentative data, algorithm design, or human assumptions and prejudices.
Data	Raw facts, figures, or information, often in the form of text, numbers, images, or audio, which are used as inputs for AI systems to learn from and make decisions.
Deep Learning	A type of machine learning that utilises artificial neural networks with multiple layers to learn representations of data. Deep learning has been particularly successful in tasks such as image and speech recognition.
Ethical AI	The development and use of AI systems in a manner that is fair, transparent, accountable, and aligned with societal values and ethical principles.
Governance	The framework of policies, procedures, and mechanisms used to guide and regulate the development, deployment, and use of AI within the Trust, ensuring compliance with legal, ethical, and organisational requirements.
Machine Learning (ML)	A subset of AI that involves the development of algorithms that enable computers to learn from and make predictions or decisions based on data, without being explicitly programmed.
Privacy	The right of individuals to control their personal information and to have it protected from unauthorised access or misuse, particularly in the context of AI systems that process sensitive data.
Security	Measures taken to protect AI systems, data, and infrastructure from unauthorised access, manipulation, or disruption, ensuring confidentiality, integrity, and availability.
Testing Data	A separate dataset used to evaluate the performance of an AI model after it has been trained. It helps assess the model's ability to generalise to new, unseen data.
Training Data	The dataset used to train an AI model. It consists of examples or instances with known input and output values, which the model uses to learn patterns and relationships.
Transparency	The principle of making AI systems and their decisions understandable and explainable to users, stakeholders, and affected individuals, facilitating trust and accountability.

Appendix B – Key Performance Indicators

1. Operational Efficiency
 - Time saved on administrative tasks: measure the reduction in time spent on repetitive tasks due to AI automation.
2. Accuracy & Performance
 - AI accuracy rate: measure the percentage of correct predictions, recommendations, or classifications by AI systems.
3. User Satisfaction & Engagement
 - User adoption rate: percentage of Staff and Student/Pupils actively using AI tools and their satisfaction with AI-driven services collected through feedback surveys.
4. Compliance
 - Data privacy and compliance incidents: track the number of data breaches or non-compliance issues related to AI usage.

Appendix C – Risk Assessment Matrix for using AI Technologies in School

Introduction

The following risk assessment matrix is intended to help schools in the Trust identify, evaluate, and mitigate risks associated with implementing Artificial Intelligence (AI) in educational processes.

The matrix considers potential risks including data protection compliance, ethical considerations, and operational integrity. There is a particular focus on safeguarding and wellbeing issues, highlighting potential risks to Student/Pupil welfare and offers strategies to mitigate these risks effectively.

Risk Assessment Matrix

Risk Area	Risk Description	Likelihood (Low/Med/High)	Impact (Low/Med/High)	Risk Level (Low/Med/High)	Mitigation Measures
Data Protection and Privacy Breaches	Unauthorised access to sensitive data or personal information, leading to safeguarding concerns and risk to privacy.				Implement strong encryption, regular audits, and GDPR-compliant data management policies and conduct regular privacy audits.
Cyberbullying	Increased potential for bullying through AI-mediated communication tools.				Monitor AI communication tools, implement clear reporting mechanisms, and provide Student/Pupil support.
Over-reliance on AI	Over-reliance on AI tools reducing interpersonal interactions among Student/Pupils. Reduction in teacher autonomy and critical decision-making by overusing AI tools.				Encourage collaborative learning activities and balance AI use with social engagement. Define clear boundaries for AI use and regularly review its impact on pedagogy.
Emotional Manipulation	AI systems unintentionally affecting Student/Pupils mental health through curated content.				Monitor AI-generated content, involve mental health professionals, and promote media literacy.
Inappropriate Content or Conduct	AI exposing learners to harmful or unsuitable materials / behaviour				Conduct rigorous testing of AI tools, apply effective filtering and monitoring and ensure human oversight.
Mental Health Impacts	Overuse of AI tools causing stress, anxiety, or dependency in learners.				Monitor usage patterns, provide mental health resources, and set expectations on use of AI systems.
Bias and Discrimination	AI systems propagating biases that impact				Regularly audit AI algorithms for bias and provide inclusive

	Student/Pupil wellbeing or inclusion. AI models producing discriminatory or biased outcomes.				media literacy education and training.
Misuse of AI	Learners using AI tools for harmful, unethical or illegal purposes (e.g. nudification).				Educate learners on responsible and appropriate AI use and establish clear usage policies.
Misinformation	Creation or spread of harmful or misleading AI-generated content.				Educate staff and learners to verify AI outputs and establish clear policies for verifying content authenticity.
Digital Divide	Inequitable access to AI tools among learners from diverse demographic groups.				Provide equitable access to AI resources and ensure alternative solutions are available.
AI Ethics Awareness	Lack of awareness among staff and learners about ethical implications of AI.				Provide training and education on AI ethics and its responsible usage. Establish an 'Ethics in AI' group.
Data Accuracy	AI systems generating inaccurate or misleading recommendations.				Regularly validate AI outputs and involve human oversight in decision-making.
Legal Compliance	Non-compliance with laws regarding AI usage and learner data.				Understand legal requirements. Conduct legal reviews and consult experts on AI-related regulations.
Cyber-Security	Increased use of AI tools in cyberattacks targeting school systems and data.				Strengthen cybersecurity protocols and educate staff and learners on safe online practices.

Likelihood and Impact Definitions

- **Likelihood:** The likelihood that the identified risk will occur.
 - Low: Unlikely to occur under normal circumstances.
 - Medium: Possible occurrence based on past trends or vulnerabilities.
 - High: Likely to occur without intervention.
- **Impact:** The severity of impact should the risk materialise.
 - Low: Minimal disruption with limited consequences.
 - Medium: Moderate disruption affecting key processes.
 - High: Significant disruption with severe consequences.

Action Plan

The DPO, DPRs and IT Network Managers will support schools in creating an action plan where the risk assessment matrix identifies medium or high-risk status that cannot be mitigated.

Review and Update

The DPO supported by DPRs and IT Network Managers will review and update this matrix annually or whenever new AI technologies or safeguarding challenges arise.