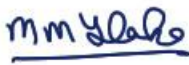




Shires Multi Academy Trust

1366 Evesham Rd, Astwood Bank, Redditch, B96 6BD
hello@shiresmat.org.uk | www.shiresmat.org.uk

Artificial Intelligence (AI) Policy

Policy Name: Artificial Intelligence (AI)	Policy Reference: MAT-OP07
Owner/Reviewer: Trust Leader, Primary, CEO	Review Date: 20th February 2026
Approved by: Trust Board	Approval Date: 25th February 2026 (link update May)
Trust Board	Review Frequency: Annually
Chair 	Date of Next Review: Spring Term 2027

Contents

1. Aims and scope
 2. Legislation
 3. Regulatory principles
 4. Roles and responsibilities
 5. Use of AI by staff across the trust, trustees and local governors
 6. Educating pupils about AI
 7. Use of AI by pupils
 8. Formal assessments
 9. Staff training
 10. Breach of this policy
 11. Monitoring and transparency
 12. Related policies
- Appendix
Risk Assessment Matrix for schools implementing AI

1. Aims and Scope

Artificial Intelligence (AI) technology is already widely used in commercial environments and is gaining greater use in education. We recognise that the technology has many benefits and the potential to enhance outcomes and educational experiences, with the opportunity to support staff in reducing workload.

We also realise that there are risks involved in the use of AI systems, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address AI risks.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which AI technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

This policy aims to:

- Support the use of AI to enhance teaching and learning
- Support staff across the trust to explore AI solutions to improve efficiency and reduce workload
- Prepare staff across the trust, trustees, local governors and pupils for a future in which AI technology will be an integral part
- Promote equity in education by using AI to address learning gaps and provide personalised support
- Ensure that AI technologies are used ethically and responsibly by all staff across the trust, trustees, local governors and pupils
- Protect the privacy and personal data of all staff across the trust, trustees, local governors and pupils in compliance with the UK GDPR

1.1 Definitions

This policy refers to both ‘open’ and ‘closed’ generative AI tools. These are defined as follows:

- Open generative AI tools are accessible and modifiable by anyone. They may store, share or learn from the information entered into them, including personal or sensitive information
- Closed generative AI tools are generally more secure, as external parties cannot access the data you input

2. Legislation

This policy reflects good practice guidelines / recommendations in the following publications:

- AI regulation white paper, published by the Department for Science, Innovation and Technology, and the Office for Artificial Intelligence
- Generative artificial intelligence (AI) and data protection in schools, published by the Department for Education (DfE)

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

3. Regulatory Principles

As a trust, we follow the 5 principles set out in the AI regulation white paper.

REGULATORY PRINCIPLE	WE WILL ...
Safety, security and robustness	<ul style="list-style-type: none"> • Ensure that AI solutions are secure and safe for users and protect users’ data • Ensure we can identify and rectify bias or error • Anticipate threats such as hacking
Appropriate transparency and explainability	<ul style="list-style-type: none"> • Be transparent about our use of AI, and make sure we understand the suggestions it makes
Fairness	<ul style="list-style-type: none"> • Only use AI solutions that are ethically appropriate, equitable and free from prejudice – in particular, we will fully consider any bias relating to small groups and protected characteristics before using AI, monitor bias closely and correct problems where appropriate
Accountability and governance	<ul style="list-style-type: none"> • Ensure that the trustees / local governing bodies and staff have clear roles and responsibilities in relation to the monitoring, evaluation, maintenance and use of AI
Contestability and redress	<ul style="list-style-type: none"> • Make sure that staff are empowered to correct and overrule AI suggestions – decisions should be made by the user of AI, not the technology • Allow and respond appropriately to concerns and complaints where AI may have caused error resulting in adverse consequences or unfair treatment

4. Roles and Responsibilities

4.1 Trust Leaders (COO/CEO/Director of IT/Trust Safeguarding Lead)

Are responsible for the strategic oversight of AI provision across the trust. This includes the development and alignment to policy across schools and ensuring appropriately trained leaders support the development and appropriate use of AI.

They are supported by designated AI Champions.

4.2 School Leadership

Are responsible for how AI will be used in the school, remaining compliant with AI policies and procedures and ensuring that all staff receive relevant training and have a clear understanding of these.

4.3 In School Designated Safeguarding Person (DSP) / Online Safety Lead

Our Designated Safeguarding Person / Online Safety Lead has responsibility for online safety in the school. They are expected to have knowledge of AI and its safeguarding implications and an in-depth working knowledge of key guidance. We ensure that they receive appropriate specialist training, commensurate with their role and that ongoing training is provided for all school staff.

4.4 Data Protection Officer

The DPO will be responsible for providing advice and guidance about data protection obligations in relation to the use of AI, including related Data Protection Impact Assessments (DPIAs).

4.5 Technical Staff (internal IT managers and contracted providers)

Technical staff / IT Leads will be responsible for technical support and guidance, with particular regard to cyber-security and the effectiveness of filtering and monitoring systems.

4.6 Staff

It is the responsibility of all staff to have read and understood this policy and associated Acceptable Use Agreements. All staff must report any incidents or suspected incidents concerning the use of AI in line with school policy. All staff will challenge any inappropriate behaviour. Staff have a duty to ensure that:

- the school environment is safe
- sensitive and confidential data / information is secure
- that their actions do not put the reputation of the school at risk and that
- learners understand their responsibilities

4.7 Governors/Trustees

We ensure that our Trust Board / Local Governance Committees have a good understanding of how AI is used in a school context and potential benefits and risks of its use. They receive regular training and updates, enabling them to support the school and challenge where necessary. This may include evaluation of the use of AI in the curriculum, administration and communications, ensuring that risks relating to these issues are identified, that reporting routes are available, and that risks are effectively mitigated. Risk management is reviewed through the Audit and Risk Committee.

4.8 Parents/carers

We work hard to engage parents and carers by:

- *periodic in school/online sessions (in person/Teams)*
- *sharing newsletters*
- *sharing information online e.g., website, social media*
- *providing curriculum information*

Our parents and carers are made aware of how AI is used in school and receive guidance on both good practice in its use and the risks of misuse that may affect children's learning or safety. They are encouraged to report any concerns to the school and are made aware that all incidents will be handled with care and sensitivity.

4.9 Pupils

Pupils must follow the guidelines set out in section 7 of this policy (*Use of AI by pupils*)

5. Use of AI by staff across the trust, trustees and local governors

5.1 Approved use of AI

At Shires MAT we are committed to helping staff, trustees and local governors reduce their workload. Generative AI tools can make certain written tasks quicker and easier to complete, but cannot replace the judgement and knowledge of a human expert.

Whatever tools or resources are used to produce plans, policies or documents, the quality and content of the final document remains the professional responsibility of the person who produced it.

Any plans, policies or documents created fully or heavily influenced by AI should be clearly labelled with the following image:



Any member of staff, trustee or local governor using an AI-generated plan, policy or document should only share the AI-generated content with other members of staff, trustees or local governors for use if they are confident of the accuracy of the information, as the content remains the professional responsibility of the person who produced it.

Always consider whether AI is the right tool to use. Just because the trust has approved its use doesn't mean it will always be appropriate.

5.2 Process for Approval

Staff are encouraged to use AI where there is evidence it can improve pupil outcomes and/or reduce workload by liaising with their school QoE, IT or AI Lead. The Trust AI Lead is responsible for signing off on approved uses of AI, or new AI tools after reviewing the request and Data Protection Impact Assessment (DPIA).



To submit a request, please use this form: [Shires MAT - AI Request Form](#)

To view the list of approved AI tools, please visit: [AI - Approved Applications \(Shires MAT\) : Bordesley IT](#)

5.3 Data Protection and Privacy

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Shires MAT will treat this as a data breach and will follow the personal data breach procedure outlined in our data protection policy. Please also refer to section 10 of this policy.

5.4 Intellectual Property

Most generative AI tools use inputs submitted by users to train and refine their models.

Pupils own the intellectual property (IP) rights to original content they create. This is likely to include anything that shows working out or is beyond multiple choice questions.

Shires MAT will not allow or cause intellectual property, including pupils' work, to be used to train generative AI models without appropriate consent or exemption to copyright.

Exemptions to copyright are limited – we will seek legal advice if we are unsure as to whether we are acting within the law.

5.5 Bias

We are aware that AI tools can perpetuate existing biases, particularly towards special characteristics including sex, race and disability. This means that critical thought must be applied to all outputs of authorised AI applications. This means fact and sense-checking the output before relying on it.

Shires MAT will ensure we can identify and rectify bias or error by training staff in this area.

We will also regularly review our use of AI to identify and correct any biases that may arise.

If parents/carers or pupils have any concerns or complaints about potential unfair treatment or other negative outcomes as a consequence of AI use, these will be dealt with through our usual complaints procedure.

5.6 Raising Concerns

We encourage staff to speak to their school leader in the first instance if they have any concerns about the potential use of AI, or the use of AI that may have resulted in errors that lead to adverse consequences or unfair treatment.

5.7 Ethical and Responsible Use

Shires MAT will always:

- Use generative AI tools ethically and responsibly
- Remember the principles set out in our trust's equality policy when using generative AI tools
- Consider whether the tool has real-time internet access, or access to information up to a certain point in time, as this may impact the accuracy of the output
- Fact and sense-check the output before relying on it

Staff members, trustees and local governors must not:

- Generate content to impersonate, bully or harass another person
- Generate explicit or offensive content
- Input offensive, discriminatory or inappropriate content as a prompt

6. Educating Pupils about AI

6.1 All pupils

Our school's educational approach seeks to develop knowledge and understanding of emerging digital technologies, including AI.

This policy outlines our commitment to integrating Artificial Intelligence (AI) responsibly and effectively within our school environment. We will use AI responsibly, safely and purposefully to support these aims:

- **Enhance academic outcomes:** Improve educational experiences and performance for pupils.
- **Support all staff:** Assist in managing workloads more efficiently and effectively.
- **Educate on AI use:** Promote safe, responsible, and ethical AI practices among staff and learners.
- **Develop AI literacy:** Incorporate AI as a teaching tool to build AI skills and understanding.
- **Prepare for the future:** Equip staff and pupils for a future where AI is integral.
- **Promote educational equity:** Use AI to address learning gaps and provide personalised support.

Our school's approach is to deliver this knowledge and understanding wherever it is relevant within the curriculum. This will include, but is not limited to:

- Computing/IT
- PHSE
- Cross curricular programmes
- Discrete subjects (for example where AI packages are used in English or science)
- Assemblies, careers sessions, external visits and visitors into school.

Our approach is given the time it deserves and is authentic i.e., based on current issues nationally, locally and within our school's risk profile. It is shaped and evaluated by learners and other members of the school community to ensure that it is dynamic, evolving and based on need.

6.2 Vulnerable Pupils

We recognise that vulnerable learners are more likely to be at risk from the misuse of AI (both in their own use or through the actions of others). We ensure that vulnerable learners are offered appropriate support to allow them to gain full benefit of the use of AI, while being aware of the potential risks.

Children are considered to be vulnerable data subjects and therefore any process involving their personal data is likely to be "high risk". If an AI/ automated process is used to make significant decisions about people, this is likely to trigger the need for a Data Protection Impact Assessment (DPIA).

7. Use of AI by Pupils

Shires MAT recognises that AI has many uses to help pupils learn.

Pupils may use AI tools:

- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images

All AI-generated content must be properly attributed and appropriate for the pupils' age and educational needs.

AI may also lend itself to cheating and plagiarism.

To mitigate this, pupils may not use AI tools:

- During assessments, including internal and external assessments, and coursework
- To write their homework or class assignments, where AI-generated text is presented as their own work
- To complete their homework, where AI is used to answer questions set and is presented as their own work (for example, maths calculations)

This list of AI misuse is not exhaustive.

Where AI tools have been used as a source of information, pupils should reference their use of AI. The reference must show the name of the AI source and the date the content was generated.

We consider any unattributed use of AI-generated text or imagery to be plagiarism and will follow our plagiarism procedures as set out in assessment policy.

Pupils must consider what is ethical and appropriate in their use of AI and must not:

- Generate content to impersonate, bully or harass another person
- Generate explicit or offensive content
- Input offensive, discriminatory or inappropriate content as a prompt

8. Formal Assessments

Shires MAT will continue to take reasonable steps where applicable to prevent malpractice involving the use of generative AI in assessments.

9. Staff Training

As AI becomes an integral part of modern education, it is essential for staff to be trained in its effective use. Training equips educators with the knowledge and skills to integrate AI tools responsibly into teaching, learning, and administrative processes. It ensures that AI is used to enhance educational outcomes, streamline workloads, and promote equity while safeguarding ethical practices and data privacy. By fostering AI literacy, staff can confidently prepare pupils for a future where AI is a key driver of innovation and opportunity.

- We will provide training to all staff on the effective, responsible, and ethical use of AI technologies in education, ensuring these tools enhance teaching, learning, and administrative processes.
- We will integrate AI-related risks and safeguards into annual safeguarding training, aligning with statutory guidance, including "Keeping Children Safe in Education."
- We will ensure all staff are equipped with the knowledge and skills to confidently integrate AI into their professional practice and to prepare pupils for a future shaped by AI-driven innovation and opportunities.
- We will train staff to identify, assess, and mitigate risks associated with AI technologies, including issues such as biased algorithms, privacy breaches, and harmful content.
- We will train staff on robust data protection practices, ensuring compliance with UK GDPR and other relevant regulations while using AI systems.
- We will promote ethical practices in the use of AI, ensuring that these technologies contribute to equity, fairness, and inclusivity in education.
- We will empower educators to teach learners about the safe and ethical use of AI, cultivating a culture of awareness, resilience, and informed decision-making in the digital age.
- We will train staff to use AI responsibly as a tool to monitor and address online risks, reinforcing our commitment to a safe learning environment.

10. Breach of this Policy

10.1 By Staff

Breach of this policy by staff will be dealt with in line with the trust's staff code of conduct.

Where disciplinary action is appropriate, it may be taken whether the breach occurs:

- During or outside of working hours
- On an individual's own device or a school device

- At home, at school or from a remote working location

Staff members will be required to co-operate with any investigation into a suspected breach of this policy. This may involve providing the trust with access to:

- The generative AI application in question (whether or not it is one authorised by the trust)
- Any relevant passwords or login details

You must report any breach of this policy, either by you or by another member of staff, to your senior leader immediately.

10.2 By Trustees or Local Governors

Trustees or local governors found in breach of this policy will be subject to the trust's Trustee/Governor code of conduct.

10.3 By Pupils

Any breach of this policy by a pupil will subject to the school's behaviour policy

11. Monitoring and Transparency

AI technology, and the benefits, risks and harms related to it, evolves and changes rapidly. Consequently, this policy is a live document that must be kept updated by the Audit and Risk committee whenever there is a significant change to either AI use by the trust or the associated risks of AI usage.

This policy will also be regularly reviewed and updated to align with emerging best practices, technological advancements and changes in regulations.

The policy will be shared with the board of trustees at least annually.

All staff are expected to read and follow this policy. responsible for ensuring that the policy is followed.

Trust AI Lead will monitor the effectiveness of AI usage across the trust.

We will ensure we keep members of the trust community up to date on the use of AI technologies for educational purposes. As part of our regular surveys, feedback from pupils, parents/carers and staff will be considered in the ongoing evaluation and development of AI use across the schools in our trust.

12. Related Policies

This policy should be read in conjunction with other school policies:

- Data Protection Policy
- Online Safety Policy
- The Staff Code of Conduct
- Acceptable Use Agreements
- Behaviour Policy
- Anti-bullying Policy

Appendices

Risk Assessment Matrix for Schools Implementing AI

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

The matrix considers potential risks across various domains, including data protection, ethical considerations, and operational integrity. There is a particular focus on safeguarding and wellbeing issues, highlighting potential risks to student welfare and offers strategies to mitigate these risks effectively. Schools should amend the content of the matrix as necessary and consider the risk profile that is relevant to their own circumstances.

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 commercial risk.				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 support.
Over-reliance on AI	Over-reliance on AI tools reducing interpersonal interactions among students. 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 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				Monitor usage patterns, provide mental health resources, and set

	dependency in learners.				expectations on use of AI systems.
Bias and Discrimination	AI systems propagating biases that impact student wellbeing or inclusion. AI models producing discriminatory or biased outcomes.				Regularly audit AI algorithms for bias and provide inclusive 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.