



DIOCESE OF SOUTHWELL
& NOTTINGHAM

MULTI ACADEMY TRUST

SNMAT

Artificial Intelligence (AI) Guidance

Policy:	Use of Artificial Intelligence Guidance
Approved by:	SNMAT Board of Directors
Date:	March 2026
Review Cycle:	Annual

Versions:			
VERSION	DATE	AUTHOR	CHANGES
Template	2023	Mark Anderson and Laura Knight.	Used under Creative Commons License: CC BY-NC-SA 4.0
2024	Feb 2024	MJH – IT Manager	Initial version.
2024.7	July 2024	MJH	Updated after consultation feedback. Moved Department for Education (DfE) and National Cyber Security Centre (NCSC) guidance to Appendixes. Added Generative AI definition. Added specific responsibility of SLT Digital Lead to ensure that AI use meets the needs of staff and students. Altered the formation of the AI Evaluation Team to give academies autonomy in its construction.
2024.9	Sept 2024	MJH	Modified after consultation to be guidance over policy. Added EU AI act.
2025	April 2025	MJH	No changes.
2025.9	Sept 2025	MJH	Added Appendix for example AI risks for Evaluation Teams to consider when creating DPIA documents.
2026.3	March 2026	Mark Hardisty	https://www.gov.uk/government/publications/generative-ai-product-safety-standards/generative-ai-product-safety-standards Include new standards to evaluate AI tools again.

EXECUTIVE SUMMARY

The objective of this guidance is to provide a framework for the integration and management of Artificial Intelligence (AI) in SNMAT Partner Academies, encompassing ethical compliance, data security and integrity, educational enhancement, workload reduction.

This guidance demonstrates the commitment from SNMAT to use evolving technologies to reduce workload, enhance student learning, foster skill development, and ensure that safeguarding and protection of our pupils and students is at the heart of what we do.

DEFINITION

Generative AI refers to technology that can be used to create new content based on large volumes of data that models have been trained on from a variety of works and other sources. Microsoft Copilot, ChatGPT and Google Bard are Generative AI tools built on large language models.

Other forms of AI can produce audio, code, images, text, simulations and videos and we already use a form of AI in email management, navigation applications and internet searching for example.

For the scope of this policy, AI refers to both Generative AI and other tools that can perform a variety of outputs.

RATIONALE

SNMAT recognises the positive impact that using AI in an education setting can bring, especially in reducing workload and supporting pupils with educational needs. However, we are committed to ensuring compliance with guidelines on data protection, plagiarism and exam malpractice to maintain safeguarding and academic integrity.

AI offers an incredible opportunity to transform the way that we teach and learn, and empowers educators and students to personalise their learning, produce smart content, automate tasks and deliver better engagement.

AI will not replace direct instruction or teacher interaction but serves as an additional resource to enrich the educational experience. SNMAT's investment in learning with AI will support lifelong learning, future education and employment prospects of our students and pupils.

SCOPE

1. This guidance sets out a framework for responsible adoption and use of AI tools across the MAT.
2. This guidance aims to:

Provide direction and guidance on how to use AI in a responsible way.
3. This guidance applies to:

Every SNMAT member of staff, pupils and students and stakeholder.
4. This guidance does not:

Recommend any specific AI software tool.

5. This guidance should be read and applied in conjunction with:

DfE Guidance – Using Generative AI In Education
SNMAT IT Acceptable Use Policy
SNMAT eSafeguarding Policy
SNMAT GDPR Policy

ROLES & RESPONSIBILITIES

BOARD OF DIRECTORS

6. It is the responsibility of the board to ensure oversight of AI use, and that the management of its use is effective.

LOCAL GOVERNING BODIES

7. It is the responsibility of the governing body to ensure there is management of AI within the school and the school meets its legislative and policy obligations on safeguarding and data protection.

THE PRINCIPAL/HEADTEACHER

8. It is the responsibility of the principal/headteacher to ensure responsible use of AI.
9. The principal/headteacher must ensure that adequate and effective training is provided to staff in using AI and that statutory requirements of GDPR and Safeguarding legislation and SNMAT policy obligations are upheld.
10. The principal/headteacher must ensure that an effective consultation, evaluation and adoption process of AI tools and usage is enacted and supported in an effective manner.

AI EVALUATION TEAM

10. It is recommended that each academy form an AI Evaluation Team. Teams can comprise of any member of staff they see fit, but it is recommended that it should compose of the Data Protection Officer, Digital Learning Lead / SLT responsible for Digital Technology, a representative from teaching staff, SENCO and a member of the school's IT Support Team.
11. It is the responsibility of the AI Evaluation Team to establish a clear workflow for the recommendation, adoption and review of AI tools, platforms and subscriptions.

SLT DIGITAL LEAD

12. It is the responsibility of the SLT Digital Lead to ensure that use of AI is reflected within the academy's digital technology strategy and meets the needs of staff and students.

STAFF

13. It is the responsibility of all staff to ensure they use AI in an ethical manner, understand the limitations, protect personal and special category data in accordance with data protection legislation and respect intellectual property rights.
14. It is the responsibility of all staff to embed safe and secure use of AI into all aspects of the curriculum ensuring that pupils and students have a good understanding of the skills needed

to use the technology safely and securely.

15. In lessons or guidance where AI use is planned – workflow, tools and sites must be evaluated by the AI Evaluation Team.

STUDENTS & PUPILS

16. It is the responsibility of all students to ensure they understand the guidelines laid out in this policy for the use of AI in education.

TRUST IT SUPPORT TEAM

17. It is the responsibility of the Trust IT Support Teams to provide support to the AI Evaluation Team and to ensure that infrastructure and devices are secure, compliant and not open to misuse or malicious attacks.

OBJECTIVES

This guidance has the following objectives:

18. Educational Enhancement: To improve teaching and learning outcomes.
19. Ethical Compliance: To ensure ethical and legal use of AI.
20. Data Security: To protect the privacy and data of all stakeholders.
21. Workload Reduction: To utilise AI to reduce the administrative and academic workload of staff.
22. Innovation: To remain at the forefront of education by integrating AI to enhance and supplement the school's mission to best support young people.
23. Safeguarding: Ensuring a proactive stance about AI-related safeguarding risks.
24. Empowerment: To provide students and pupils a framework in which to utilise the benefits of AI safely and securely.

STAFF GUIDELINES

ETHICAL USE

Respect for intellectual property:

25. Ensure all AI technologies used are properly licenced and respect intellectual property laws.
26. Consult the AI Evaluation Team to ensure any AI Tool is approved for educational use.

Transparency and Disclosure:

27. Be prepared to explain how adopted AI technologies are used, and under which contexts. Inform staff, students and parents when and how AI is being used.
28. Periodic checks should be made by SLT and Digital Lead to ensure transparency measures are consistently applied.

Avoiding Bias and Discrimination:

29. Ensure AI tools that have been vetted and approved by the AI Evaluation Team for potential biases related to race, gender, or any other factor.
30. Conduct periodic reviews and seek feedback from students and staff to identify any issues of bias.
31. If a concern arises, consult with the AI Evaluation Team for further assessment.

RESPECT FOR SPECIAL CATEGORY, PERSONAL DATA AND PRIVACY

31. Protect personal and special category data in accordance with data protection legislation.
32. Ensure that AI tools are compliant with GDPR and other relevant data protection laws, as verified by the Data Protection Officer.
33. Conduct a Data Protection Impact Assessment (DPIA) for each AI system, particular for those handling special category or student data.
34. Regularly review updates from the AI Evaluation Team on data storage and handling procedures to ensure compliance.
35. If concerns arise, consult with the AI Evaluation Team for further evaluation.

INNOVATION

36. Ensure that AI tools are aligned with curriculum goals and objectives.
37. Evaluate the pedagogical benefits of AI tools before use.

WORKLOAD REDUCTION

38. AI should enhance, not replace, human creativity, but it can be used to accelerate the creation of examples such as lesson planning, quizzes and flashcards.
39. Staff must verify the suitability, accuracy, and curriculum alignment of any AI-generated materials.

ACCURACY, DATA INTEGRITY AND FACT CHECKING

40. Ensure that AI content is accurate and factually correct.
41. Adhere to all legislation regarding the use of AI, data protection and safeguarding. If in doubt, speak with a member of the AI Evaluation Team.

SAFEGUARDING

42. Ensure that a proactive stance about AI-related safeguarding risks is taken, including examples such as deep fakes and impersonation, harassment and bullying, criminality, and exposure of private and sensitive data.

STUDENT GUIDELINES

43. The use of AI is recommended for Key Stage 3 and above students only.

USE OF AI FOR ACADEMIC PURPOSES

44. AI can be used as an aid for academic purposes, such as research, homework, and assignments. However, it is essential to note that students should not solely rely on AI to complete their work. The use of AI must be in line with academic integrity guidelines, and students must cite the sources used.

PROHIBITION

45. The use of AI must not result in plagiarism or copyright infringement. Students must understand the concept of plagiarism and be able to use AI ethically. Teachers and staff must educate students on how to use AI without violating plagiarism guidelines and copyright laws.

RESPONSIBLE USE

46. Students must use AI in a responsible and ethical manner. They must safeguard their privacy and avoid sharing personal information with AI tools. Teachers and staff must educate students on how to use AI safely.

INAPPROPRIATE USE

47. Inappropriate usage of AI will be dealt with in line with the school's behaviour and IT Acceptable Use policies.

REVIEW

48. The application and outcomes of this policy will be monitored to ensure it is working effectively by:

- Monitoring student learning and attainment
- Obtaining feedback from staff, students, and parents to gauge the benefits and limitations of AI.

49. This policy is reviewed annually by SNMAT in consultation with recognised trade unions.

APPENDIX 1 – VENDOR AI GUIDANCE

Microsoft – AI Safely & Responsibly – Classroom Toolkit

<https://learn.microsoft.com/en-us/training/educator-center/instructor-materials/classroom-toolkit-unlock-generative-ai-safely-responsibly>

Microsoft – Responsible AI

<https://www.microsoft.com/en-us/ai/responsible-ai>

Google – Future of Education

<https://edu.google.com/future-of-education/>

APPENDIX 2 – RECOMMENDED MICROSOFT TRAINING COURSES

Enhance Teaching & Learning with Microsoft Copilot

<https://learn.microsoft.com/en-us/training/modules/enhance-teaching-learning-bing-chat/>

Empower educators to explore the potential of artificial intelligence.

<https://learn.microsoft.com/en-us/training/modules/empower-educators-explore-potential-artificial-intelligence/?ns-enrollment-type=Collection&ns-enrollment-id=zxga837jwj00n>

A quick guide to Bing Chat for educators

<https://edudownloads.azureedge.net/msdownloads/Bing-Chat.pdf>

Enhancing teaching and learning with Bing Chat

<https://learn.microsoft.com/en-us/training/modules/enhance-teaching-learning-bing-chat/>

APPENDIX 3 – DfE GUIDANCE – SLT RESPONSIBLE FOR DIGITAL TECHNOLOGY

In January 2024, the Department for Education (DfE) expanded its Meeting Digital and Technology Standards in Schools guidance to include digital leadership and governance. The guidance recommends that schools assign a member of its Senior Leadership Team (SLT) to be responsible for digital technology.

<https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/digital-leadership-and-governance-standards>

APPENDIX 4 - DfE GUIDANCE – USING GENERATIVE AI IN EDUCATION

This guidance sets out the position of the DfE on the use of generative artificial intelligence (AI), including large language models like ChatGPT or Google Bard, in the education sector.

<https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education/generative-artificial-intelligence-ai-in-education>

APPENDIX 5 - NATIONAL CYBER SECURITY CENTRE (NCSC) – CHATGPT MODELS: WHAT’S THE RISK

This blog from the NCSC considers some cyber security aspects of ChatGPT and Large Language Models.

<https://www.ncsc.gov.uk/blog-post/chatgpt-and-large-language-models-whats-the-risk>

APPENDIX 6 – EUROPEAN UNION AI ACT – FIRST REGULATION

The use of artificial intelligence in the EU will be regulated by the AI Act, the world’s first comprehensive AI law.

<https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>

APPENDIX 7 – EXAMPLE USAGE RISKS

Content and Safety Risks

Exposure to harmful, inaccurate, biased or misleading content, including hallucinations.
Deepfakes and AI-generated media that mislead or impersonate others.
Creation and sharing of AI-generated child sexual abuse material.
Avatars and chatbots used for grooming.
Extremist propaganda generated or spread using AI.
AI content framed as credible, encouraging misplaced trust.
Risk of anthropomorphising AI and over-trusting its output.

Data Protection Risks

Breach of personal data through use of AI tools.
Use of AI without lawful basis or proper safeguards.
Lack of clarity with students on data use.
AI systems accessing publicly exposed or outdated data.
Risks from using free or personal AI tools not GDPR-compliant.

Intellectual Property (IP) Risks

Student work used without permission.
Copyrighted material uploaded into AI tools.
AI outputs that replicate copyrighted content.
Lack of clarity about what data AI models train on.
Safeguarding and Online Safety Risks
Social media profiling via personalisation algorithms.
Grooming through AI avatars or bots.
More credible cyber threats enabled by AI.
Access to blocked or harmful content through AI.
Students oversharing personal info via AI tools.

Academic Integrity Risks

Students bypassing learning with AI-generated work.
AI output hard to distinguish from student work.
Detection tools unreliable, may flag false positives.
Confusion about what counts as cheating.
Over-reliance on AI for homework and assessments.
Uploading student work to tools without consent.

Bias and Inclusion Risks

Bias in AI output reflecting flawed training data.
Neurodiverse students excluded by typical AI outputs.
Inaccessible or inappropriate content for some pupils.
Over-trust in seemingly authoritative AI output.

Professional Judgement Risks

Outsourcing thinking and judgement to AI.
Missing legal nuance or context in AI-generated content.

System and Policy Risks

Use of non-approved or insecure AI tools.
Outdated AI or safeguarding policies.
Inadequate staff training on AI risks.
No DPIAs for AI tools.
Lack of clear student guidance on appropriate AI use.