

Artificial Intelligence (AI) Acceptable Use Policy for students



**Resilience
Multi Academy
Trust**

Summary	AI Acceptable Use of AI Policy for students		
Responsible Person/Author:	Adam Marham - COO		
Applies to: (please circle/delete as appropriate)	Colleagues ☒	Student ☒	Community ☐
Ratifying Committee(s) and Date of Final Approval:	Trust Board – 20.08.26		
Available On:	SharePoint and on demand, Websites		
Effective from:	21.08.26		
Date of Next Formal Review:	August 2027		
Review Period	1 Year		
Status	Non-statutory		
Owner	RMAT		
Version:	1		

DOCUMENT CONTROL

Date	Version	Action	Amendments
1	1	Policy created	

Contents

DOCUMENT CONTROL	2
Aims and application	4
Purpose	4
Scope	4
Policy statement	Error! Bookmark not defined.
Data Protection implications of using AI	Error! Bookmark not defined.
Ethical use of AI	5
Appendix 1 – Permitted and Prohibited AI tools and Prohibited uses	7

Aims and application.

1. RMAT recognises that AI is becoming an important part of education, employment, and everyday life. Students should develop the skills to use AI safely, ethically, critically, and responsibly.
2. This policy sets out expectations for student use of AI and supports academic integrity, safeguarding, and responsible digital citizenship.

Purpose

3. The purpose of this policy is to:
 - Support safe and responsible use of AI.
 - Promote academic integrity.
 - Protect students and staff.
 - Ensure fairness in assessment.
 - Encourage students to use technology appropriately and critically.

Scope

4. This policy applies to all students. It covers:
 - RMAT provided AI systems.
 - AI systems accessed through RMAT accounts.
 - AI functions embedded within software and digital services used for educational purposes.

AI Principles

5. Students must follow these principles whenever using AI.
 - **Responsibility**
Students remain responsible for all work submitted in their name.
 - **Academic Integrity**
Work submitted for assessment must accurately reflect the student's own knowledge, understanding, and skills.
 - **Transparency**
Students must disclose and reference AI use where required by teachers, examination boards, or assessment instructions.
 - **Critical Thinking**
Students should question and verify information produced by AI rather than accepting it without challenge.
 - **Respect**
AI must not be used to harm, embarrass, deceive, bully, or exploit others.

Appropriate use

6. Students may use approved AI systems to:

- Explain concepts.
- Support revision.
- Generate ideas.
- Improve understanding.
- Create revision materials.
- Support planning and organisation.
- Improve accessibility.

Academic integrity

7. Students are responsible for ensuring their work represents their own learning, understanding, and skills.
8. AI may support learning but must not replace it.
9. AI must not be used to:
 - Complete assessments on a student's behalf.
 - Produce final work that is presented as wholly the student's own.
 - Circumvent learning objectives.
 - Gain an unfair advantage over other students.
10. Where AI is used, students may be required to:
 - Explain how it was used.
 - Show draft versions of their work.
 - Provide screenshots or records of AI interactions.
 - Demonstrate authorship of submitted work.

Formal assessments

11. RMAAT will follow current JCQ and awarding body requirements.
12. Where assessment instructions allow AI use:
 - Students must follow the instructions provided.
 - Students must acknowledge AI use. E.g. Microsoft Copilot used on 4 September 2026 to generate initial ideas for essay structure. All final content independently researched, verified and written by the student.
 - Students must verify information provided by AI.
 - Students remain responsible for submitted work.

Authenticity of Work

13. Teachers will use professional judgement when considering the authenticity of student work. This may include:
 - Classroom performance.
 - Previous work.
 - Discussion with the student.
 - Drafting history.

- Supporting evidence.
- Understanding demonstrated by the student.

RMAT will not rely solely on AI detection tools due to known reliability issues

Approved AI systems

14. Students may only use AI systems approved by RMAT through RMAT-managed platforms and accounts.
15. RMAT will maintain an approved systems register which may be updated without amendment to this policy. The current edition of the register appears at appendix 1.
16. Questions regarding approved tools should be raised with a teacher, tutor, Head of Year, or academy leadership team.

Safeguarding and Online Safety

17. Students must not:
 - Use AI to bully, threaten, harass, or humiliate others.
 - Create fake content about staff or students.
 - Generate or share inappropriate content.
 - Create or distribute deepfakes.
 - Use AI to deceive others.
 - Share personal or confidential information through non-approved systems.

Relationships with other policies

18. Use of AI does not replace or override:
 - Safeguarding and Child Protection Policy.
 - Anti-Bullying Policy.
 - Positive Discipline Policy.
 - Exams policies.
 - ICT Acceptable Use Agreement.

Breaches

19. Breaches of this policy will be addressed through relevant academy procedures, including:
 - Safeguarding procedures.
 - Examination malpractice procedures.
 - Positive Discipline Policy.

Review

20. Due to the pace of AI development, RMAT may update guidance, approved system registers, procedures, and implementation guidance between formal reviews.

Appendix 1 – Permitted and Prohibited AI tools and Prohibited uses.

Permitted Generative AI tools.

Name of Tool	Purposes
Copilot for Microsoft 365	Support learning by explaining topics, summarising content, generating ideas for assignments, helping structure written work, and developing study or revision materials.
Canva	Create and enhance presentations, infographics, and other visual materials to support learning, revision, and the communication of ideas.

Prohibited AI tools.

Name of Tool	Reasons for prohibition
Character.AI	High safeguarding risk, no educational controls
Claude	No guaranteed data isolation, risk of sharing sensitive contact.
DeepSeek	Global concern regarding user security and access to inputs by the Chinese Government
Discord bots with AI features	Minimal safeguarding controls. Data stored outside education contracts
FaceApp	Unclear data retention. No educational purpose.
Midjourney	Public prompt history by default. No safeguarding controls.
Personal Chat GPT accounts	Individual users who sign up to Chat GPT sign up to the terms provided by Open AI for individual users. These terms do not contain suitable data processing terms and require individual users to proactively opt out of their content being used to train the models. These terms are therefore not suitable for use for school purposes.
Replika	No professional use case.
Snapchat My AI	Safeguarding concerns.
TikTok AI tools	No enterprise safeguards.
Unvetted chrome extensions	Data scraping risk.
Voice cloning tools	Fraud and safeguarding concerns
WhatsApp AI tools	No control over data flow. No compliance guarantee.

The above list is not exhaustive and if you have any questions about the suitability of use of an AI product, you should contact the IT Director or Data Protection Officer.

Prohibited uses.

The following uses of AI are prohibited:

- Submitting work created fully or partly by AI as your own, where this has not been authorised by your teacher.
- Using AI in assessments, homework, or coursework where it has been specifically prohibited by the teacher.
- Using AI to create harmful, offensive, or inappropriate content, including content used to bully, threaten, or embarrass others.
- AI systems designed to deceive, coerce, or influence human behaviour in harmful ways.
- Using AI to target or take advantage of someone's age, needs, or personal circumstances in a harmful way.
- Using AI to judge, rank, or label people in ways that could affect how they are treated.
- Inputting confidential, personal, or sensitive school data (including pupil or staff details) into AI tools that are not approved by the Trust.
- Using AI to impersonate another person (e.g. staff or students), including creating fake messages, images, audio, or video.