

Artificial Intelligence (AI) Policy

Author: Head of IT, MIS & Exams

Equality Assessment: Head of IT, MIS & Exams

Date: 28/08/2025

Version and Date		Actions/Notes
1.0	28/08/2024	New policy
2.0	12/11/2024	Correction to Section 5. Curriculum Integration removed 'Protections should be' bullet point as added incorrectly. Changed Section 7. Responsible Use to '7. Responsible Use by Students'.
3.0	25/07/2025	Added new related act / policies including the new Data (Use and Access) Act 2025 Section 4: Added monitoring and filtering of AI. Section 9: Added Senior IT Technicians to workflow of DPIAs.

Approved by SMT: August 2025

Approved by Corporation: October 2025

Date of Next Review: August 2025

Related policies or procedures or parent policy if applicable:

- Online Safety Policy
- Information Security Policy
- Data Protection Policy
- Examinations Policy
- IT Acceptable Use Policy - Staff
- IT Acceptable Use Policy - Student

Groups/bodies consulted in the development of the policy:

- General Data Protection Regulation (GDPR) 2018
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Keeping children safe in education 2025
- Jisc
- JCQ
- Exam Awarding Bodies

To be published on College Website: Yes

To be published on Student Hub: Yes

Artificial Intelligence (AI) Policy

The purpose of this policy is to provide guidance to the Macclesfield College learning community on the use of Artificial Intelligence (AI).

Intentions

The intention to integrate AI tools into the curriculum comes from our commitment to ensure students' have the best tools available to aid learning and for tutors to enhance learning resources.

The use of AI is strategically important to our College as an additional tool to support and expand upon classroom instruction, personalised learning and increasing accessibility.

Tutors will guide and monitor students' use of AI, ensuring that it aligns with the College's curriculum objectives and learning outcomes.

Tutors will ensure their pedagogical, behavioural, and pastoral knowledge is complemented and not undermined by AI tools.

AI will not replace direct instruction or teacher interaction but will serve as an additional resource to enrich the educational experience.

Investing in AI is just one way in which the College will support the lifelong learning, further education and employment prospects of our pupils.

Integrate AI tools into Business Support teams to improve and automate workflow processes to enhance staff and student experience of administration processes.

1. Introduction

This policy provides a framework for the integration and management of AI in our college, encompassing ethical compliance, educational enhancement, workload reduction, data security, and innovation, whilst ensuring the safeguarding and protection of our students are at the heart of what we do at Macclesfield College. This policy applies to all staff, students, and stakeholders.

2. Definitions

AI: Artificial Intelligence, including machine learning, natural language processing (NLP), and large language models (LLMs).

LLM: Large language models such as ChatGPT/Bard/Claude which have Generative capabilities.

NLP: Natural language processing such as Alexa / Google Assistant / Siri - differs from the above and has fewer opportunities for bias and hallucination.

Image generation from LLM - images can be created via text prompts which can be inappropriate or subject to bias.

Stakeholders: Teachers, students, parents, administrative staff, and external partners.

3. Objectives

- Educational Enhancement: To improve teaching and learning outcomes.
- Ethical Compliance: To ensure ethical and legal use of AI.
- Data Security: To protect the privacy and data of all stakeholders.
- Workload Reduction: To utilise AI to reduce the administrative and academic workload of staff.
- Innovation: To remain at the forefront of education by integrating AI to enhance and supplement the college's mission to best support young people.

4. Ethical Use of AI

Respect for Intellectual Property

- What to Do: Ensure all AI technologies used are properly licensed and respect intellectual property laws.
- How to Do It: Before using any AI tool, consult the central record maintained by IT Support to ensure its approved for educational use.
- How to Check: Refer to the central record, kept by IT Support, for a list of approved and licensed AI tools.

Transparency and Disclosure

- What to Do: Clearly indicate where and when AI is being used in educational settings.
- How to Do It: Label AI-generated content and inform students and parents when an AI tool

is being used for educational purposes.

- How to Check: Periodic checks by the Head of IT to ensure transparency measures are consistently applied.

Avoiding Bias and Discrimination

- What to Do: Implement measures to ensure AI algorithms are free from biases.
- How to Do It: Use AI tools that have been vetted and approved by the IT Support and Safeguarding team for potential biases related to race, gender, or other factors.
- How to Check: Conduct periodic reviews and seek feedback from students and staff to identify any issues of bias.
- Who to Speak To: If concerns arise, consult with the Head of IT for further evaluation

Respect for Personal Data and Privacy

- What to Do: Comply with data protection laws, including age restrictions and parental consent, and ensure individual privacy when using AI.
- How to Do It: Use AI tools that are compliant with the Data Protection Act and Data (Use and Access) Act 2025 or other relevant data protection laws, as verified by the Head of IT and audited with the Data Protection Officer (such as not sharing any personal student data on any platform unless previously agreed by the Head of IT). Ensure monitoring and filtering of AI tools is in line with the Department for Education's 'Keeping children safe in education' guidance.
- How to Check: Regularly review updates during the Information Security Committee on data storage and handling procedures to ensure compliance. Ensure risk assessments are completed when implementing AI related tools.
- Who to Speak To: If concerns arise, consult with the Head of IT for further evaluation.

5. Curriculum Integration

- Alignment: Ensure AI tools are aligned with curriculum goals and objectives.
- Pedagogical Relevance: Evaluate the pedagogical benefits of AI tools before integration as per the 'New Software' request on the IT Helpdesk.

6. Workload Reduction

- AI should enhance, not replace, human creativity. Examples include but are not limited to lesson planning, quiz creation, and flashcard generation. Teachers must verify the suitability, accuracy, and curriculum alignment of any AI-generated materials.

7. Responsible Use by Students

AI misuse is when you take something made using AI and say it's your own work. This will be classed as plagiarism and follow our usual plagiarism processes.

You're not allowed to use AI tools when you're in an exam.

Your teachers will tell you if you're allowed to use AI tools when doing your coursework - the rules will depend on your qualification.

Even if you're allowed to use AI tools, you can't get marks for content just produced by AI - your marks come from showing your own understanding and producing your own work.

Ensure that AI-generated content is accurate and factually correct.

Refencing AI

- Name the AI tool you used
- Add the date you generated the content
- Explain how you used it
- Save a screenshot of the questions you asked and the answers you got.

Declare it's all your own work

When you hand in your assessment, you have to sign a declaration. Anything without a reference must be all your own work. If you've used an AI tool, don't sign the declaration until you're sure you've added all the references.

If you've misused AI, you could lose your marks for the assessment – you could even be disqualified from the subject.

Compliance with Laws and Regulations

- Adhere to all local and international laws regarding the use of AI and data protection. If in doubt, speak with your line manager or a member of the IT Support team. Ensure usage also complies with the IT Acceptable Use Policies.

8. Safeguarding

- Take a proactive stance about AI-related safeguarding risks, including but not limited to:
 - deep fakes and impersonation;
 - harassment and bullying;
 - criminality, coercion, grooming and exploitation.
- Note that AI may be an aggravating factor in safeguarding and child protection cases.

9. Data Management

All data used in AI applications is treated in the same way as any other data in our college and must be documented in the College Information Asset Register and reviewed by the Information Security Committee bi-annually.

New systems must have an appropriate Data Protection Impact Assessment (DPIA) conducted by the Head of IT or a Senior IT Technician and the requester, which should be approved by the Head of IT and then sent to the DPO for audit purposes.

Data stored within AI applications must adhere to the College's Data Retention schedule.

Any personal data must be encrypted/password protected in line with the College's Information Security policy.

10. Implementation Plan

In terms of implementing AI tools, these should follow the same as any other resource or software following the IT Support 'Implementing or Improving an IT System' which is outlined below:

- **Explain the need.** The reason for the change should be clear. We're changing because there is a need, whether it's efficiency, simplification, merging, staying current, meeting customer needs, or other reasons.
- **Involve those impacted by the change.** They know things that you don't and can help identify roadblocks, work around possible problems to find a solution or reach out to contacts/companies who have implemented what we're working towards.
- **Protect data.** Any new systems or improvements to existing systems that involve personal/sensitive data should also involve the Data Protection Officer and have a Data Protection Impact Assessment (risk assessment) completed and data agreements in-place with any third parties that process/store our college data. Ensure the new system follows the College's complex password policy and data minimisation and retention are in line with policy.
- **Make a plan.** Create a timeline of events to manage expectations on the project - include some buffer room in your timeline for the unexpected (e.g. key staff leave the project).
- **Decide on a measure of success.** Work with the team to establish what would be considered success and how can that be measured.
- **Communicate.** Share good news or bad news as the project develops, this will ensure people are kept informed and allows them to adjust to changes. Listen and address any concerns users have with the new system.
- **Train and document.** Ensure end users and IT Technicians have the correct training provided and document any roles/responsibilities, training materials, access keys, server/network changes, bespoke configurations, scheduled tasks you have to implement with the system. The system must be documented in the IT Systems register.
- **Testing.** Conduct user and security testing with the system and make improvements based on this feedback.
- **Backup and recovery.** Ensure the new system is integrated with the current backup procedure and can be recovered in a timely manner.
- **Measure results.** Is the system working in line with the original measures of success agreed? Are people happy? Document any areas for improvement for the next development iteration?

11. Accountability

The Information Security Committee oversees and implements the Data Protection and Information Security policies.

The Data Protection Officer (DPO) audits the information held and processed at the College.

12. Levels of responsibility

- Programme Leads, Centre Principals and Line Managers: The responsibility for initial approval lies within the relevant department leads. Check for use against the central record. If required complete the 'New Software' request on the IT Helpdesk.
- Programme Leads should define the tools used in their curriculum areas and the assessment methods for their curriculum area. Programme Leads should reflect on what tools and approaches best fit their curriculum, being mindful of AI and how it can (and may) be used by both students and staff alike.
- SMT Approval: The Senior Management Team must give final approval for any AI initiatives.
- Governance Approval: The governing body must also approve any major AI initiatives.
- Technical/Data Protection Approval should be given by the Head of IT and reviewed by the Information Security Committee.

13. Review and Monitoring

The effectiveness and impact of AI on pupil learning and attainment will be regularly evaluated and reviewed through the usual curriculum review meetings.

Feedback from students, teachers, and parents will be gathered to assess the benefits and limitations of AI in enhancing the curriculum and discussed in the IT Strategy Working Group.

Adjustments and improvements will be made based on evaluation findings to ensure the optimal integration and utilisation of AI in line with the college's aims and the evolving needs of the curriculum.

References

Anderson, M., Knight, L. (2023) Free resource: Use of artificial intelligence (AI) in Education School Policy Template, ICTEvangelist. Available at: <https://ictevangelist.com/free-resource-use-of-artificial-intelligence-ai-in-education-school-policy-template> (Accessed: 28 August 2024)