ARTIFICIAL INTELLIGENCE POLICY 2026-2027

Overall responsibility:	Principal
Implementation:	Assistant Principal Teaching, Learning & Quality Head of ICT Services
Date issued:	July 2026
Date for review:	July 2027

Endorsed and approved by The Senior Leadership Team

Date: July 2026

Jason Lancaster

Principal and CEO



Contents

1. Introduction 3
2. Responsibility 3
3. Core principles 3
4. Guidelines for staff 4
5. Guidelines for students 6
6. Risk Management 7
6. Future skills development 7
9. Conclusion 8
10. Linked Policies 8

1. Introduction

At Northampton College, we recognise the potential for Artificial Intelligence (AI), particularly Generative AI (e.g., ChatGPT, Claude), to transform how our College is managed and how students learn. This policy outlines our approach to integrating AI responsibly into how we run our College and how we deliver learning, enabling everyone to benefit from new technologies, educating them about safe, responsible and ethical AI use.

We recognise the guidance set out in the Department for Education's Statement on Generative Artificial Intelligence in Education[1]. This policy has been informed by that guidance along with documents such as JISC's 'Principles for the use of AI in FE Colleges'[2].

All users of generative AI will comply with relevant laws, regulations, policies and guidelines governing Keeping Children Safe in Education[3], intellectual property, copyright, data protection and other relevant areas. We will prioritise the safeguarding of our students and will not knowingly use any AI technology that puts them at greater risk. Staff will not provide intellectual property, including students' work, to be used to train Generative AI models without appropriate consents or exemptions in place.

2. Responsibility

Overall responsibility: Principal and CEO

Implementation: Assistant Principal Teaching, Learning and Quality and Head of ICT Services

3. Core principles

When we invest in, implement and use AI in our college we follow these key principles:

- **Equity and inclusion:** We recognise the diversity of our College community and are committed to ensuring that AI tools are accessible and beneficial to students and staff of all backgrounds, abilities, and identities. We commit to deploying AI technologies in a way that is equitable and promotes inclusion, addressing biases and ensuring fair access to educational opportunities for all staff and students, for example where appropriate, AI tools will be used to enhance accessibility—for example, by offering real-time transcription, providing materials in multiple languages, supporting neurodiverse students, providing accessible formats based on individual student needs, language support, or personalised learning pathways for students with additional learning needs. Where staff and students experience overlapping forms of potential bias or exclusion, the College will monitor and address such issues proactively.
- **Transparency:** We prioritise transparency in AI usage, ensuring that students, families, and staff understand how and where it is used and the effects on teaching and learning.
- **Privacy:** We apply strict data protection standards, including safeguarding student and staff data used in AI applications. Our full data protection policy can be found here – link to Data Protection Policy 2026-27
- **Accountability:** We hold ourselves accountable for the ethical design, development, and implementation of AI systems, regularly reviewing their impact and efficacy.
- **Educational value:** We consider how AI applications align with the curriculum scope and objectives and serve to improve teaching and learning experiences and outcomes for students.

[1] https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education/generative-artificial-intelligence-ai-in-education
[2] https://www.jisc.ac.uk/further-education-and-skills/principles-for-the-use-of-ai-in-fe-colleges
[3] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

- **Alignment with skills needs:** where appropriate, the use of AI will be aligned to local, regional and national skills as identified through Local Skills Improvement Plans, and emerging sector needs to support progression and employability.
- **Safeguarding:** All AI tools used with students will be age appropriate and comply with Keeping Children Safe in Education (KCSIE). Staff will report any safeguarding concerns arising from AI use to the Designated Safeguarding Lead.
- **Procurement:** the procurement of any AI tools will be subject to the same checks as any other IT resources such as data security and compliance with the appropriate accessibility standards.

We use AI as an administrative and educational tool and actively develop staff and students' AI literacy and skills. We use AI to help tutors manage their workload rather than add to it, and to improve and streamline operations to maximise time and resource available for teaching and learning.

4. Guidelines for staff

Staff are permitted to explore and use AI-based tools and technologies to support their work where no proprietary or personal information is shared with the AI tool. AI tools will be used responsibly, ensuring they complement expertise but do not create a substitute for professional judgement. Staff remain professionally responsible and accountable for the quality and content of any output they have generated using AI. The preferred general use AI tools for staff are College-licenced Copilot and FEAI Knowledgeflow Teachers may use College-licenced Teachermatic for supporting planning and delivery of teaching, learning and assessment.

Staff can use AI technologies:

- As a starting point to generate schemes of work, lesson plans and assessment materials. These should then be adapted to better reflect the specific needs of students and must meet the needs of awarding organisations or validating institutions.
- To develop course materials such as handouts and presentations to support streamlining workflows and reducing workloads.
- To support development of business documentation and materials to support streamlining workflows and reducing workloads.
- In business support roles to assist in streaming workflows and improving efficiency.
- In College-approved pilots and projects e.g. the use of AI tools in assessment and feedback. Where such pilots or projects are being undertaken, consent to participate should be obtained from staff and students involved. Guidance on this can be obtained from the Quality Office.

For transparency, staff should indicate when AI has been used to support the creation of all materials. Within the footer of all materials, you should include the following: “AI has been used to support the creation of this content”

Staff cannot:

- Currently use AI technologies to assess and provide feedback to students on formative and summative assessment unless as part of an approved College project or trial. If a member of staff would like to trial using an AI tool for assessment and feedback, they should contact the Quality Office to discuss.
- Upload data that is protected by data protection laws pertaining to identifiable individuals to any AI tool other than the College licenced Copilot or Knowledgeflow. The uploading of such information to any other AI tool will be classed as a GDPR breach and must be reported to

the Data Protection Officer (dataprotection@northamptoncollege.ac.uk). This information includes:

  - Basic identity information
  - Health and genetic data
  - Biometric data
  - Racial or ethnic data
  - Political opinions
  - Sexual orientation / identity
  - Any information that relates to an identified or identifiable living individual.

- Upload any business or commercially sensitive information belonging to Northampton College or any of its stakeholders to any AI tool other than the College licenced Copilot or Knowledgeflow.
- Use AI tools that the College have taken the considered decision not to allow the use of on College devices and through the College network. These decisions are based on consideration of concerns such as data and privacy management. Specific tools that are not to be used are listed below.
  - DeepSeek (confirmed 30/1/25)
  - To protect the privacy, confidentiality, safeguarding, and security of all staff, students, visitors, and College information, the use or wearing of Artificial Intelligence (AI) enabled smart glasses, smart eyewear, or any wearable device capable of recording, transmitting, analysing, or storing audio, video, images, or other data is strictly prohibited on College premises and during College activities. (confirmed 25/8/26)
  - NOTE: specific guidance may be given to individuals using College piloted tools.

Staff will receive training to:

- Understand Generative AI: Staff will receive training on the capabilities and limitations of Generative AI tools like Knowledgeflow, Copilot and ChatGPT. This will include checking for bias, accuracy and currency. They will learn to quality-assure and fact-check the results and use AI-generated content responsibly in teaching materials and other business documentation.
- Use professional judgement: Staff will exercise professional judgement in checking AI-generated content for accuracy, relevance, and appropriateness before use in educational settings. They are expected to provide context, and supplement AI-generated materials with their expertise.
- Use AI to personalise learning: Staff must promote equity in education by considering use of AI to address learning gaps and provide personalised support, preparing all students for a future in which AI technology will be an integral part, being mindful of disparities in opportunities for different students.
- Meet data protection and Intellectual Property legislation and policies: Staff will be trained to protect personal and sensitive data, ensuring compliance with data protection legislation and other college policies, recognising the risks posed by AI. Staff also need to respect students' intellectual property rights, ensuring that original work (including homework) is not used to train AI models without appropriate consent or exemption to copyright.

Teaching staff will emphasise to students the importance of critical thinking, creativity, and originality in their work. Clear guidelines and expectations will be communicated to students regarding the appropriate use of generative AI tools for homework and during assessments, ensuring that their work reflects their own efforts and understanding and meets the

requirements of awarding organisations. Teachers can use information from sources such as the JCQ (for example – https://www.jcq.org.uk/wp-content/uploads/2024/02/JCQ-AI-poster-for-students-2.pdf) to ensure that students are clear about how they can use AI appropriately in assessment and the consequences of its misuse – see the Malpractice, Maladministration and Plagiarism Policy.

All staff, including senior leaders, are responsible for reading and understanding this policy before using any AI technology. Staff must report any suspected breaches of this policy to the Quality Office (qualityteam@northamptoncollege.ac.uk).

Staff must ensure that any potential new use of AI tools is assessed to consider if a Data Protection Impact Assessment is required.

5. Guidelines for students

Throughout their programmes of study, students will be guided to:

- Understand generative AI: Students will be given information on the capabilities and limitations of the most widely available, age-appropriate, Generative AI tools, enabling them to critically evaluate AI-generated content. They will learn to discern between reliable and unreliable information and use AI tools responsibly.
- Use AI responsibly: Students are encouraged to use AI tools as aids to supplement their understanding rather than relying on AI-generated content. They will be taught to quality-assure and fact-check information and get help from teaching and support staff when needed. Students will be taught not to enter personal details or sensitive information into generative AI tools.
- Develop their digital citizenship: Students will be trained in digital citizenship and online safety, including understanding the implications of sharing personal data and intellectual property online. They will learn to protect their privacy and respect the intellectual property rights of others in digital environments.

Students must:

- Only use AI technologies where advised by teachers and support staff that they can – this will depend on the assessment guidance linked to the qualifications they are studying.
- Not use AI tools that the College have taken the considered decision not to allow the use of on College devices and through the College network. These decisions are based on consideration of concerns such as data and privacy management. Specific tools that are not to be used are listed below.
    - DeepSeek (confirmed 30/1/25)
    - To protect the privacy, confidentiality, safeguarding, and security of all staff, students, visitors, and College information, the use or wearing of Artificial Intelligence (AI) enabled smart glasses, smart eyewear, or any wearable device capable of recording, transmitting, analysing, or storing audio, video, images, or other data is strictly prohibited on College premises and during College activities. (confirmed 25/8/26)
- Be clear and transparent where work has been generated with the help of AI.
- Clearly reference the use of AI tools in any homework, classwork or formal assessment by including the following at the end of the work:
    - The name of the AI tool used
    - The date the content was generated
    - An explanation of how the tool was used e.g. what prompts were used to generate the content
    - Save a screen shot of the questions/prompts asked and the responses received

- Sign any declarations required to confirm that any work without references is your own. If an AI tool has been used, the declaration should not be signed until all the references have been added.

NOTE: apprentices and work-based learners will be provided with specific guidance on the appropriate use of AI in the workplace by their employer.

If a student misuses an AI tool, for example by not including appropriate references, they are likely to have committed malpractice, and this may attract severe sanctions; for example, they may be disqualified from the assessment or even the whole qualification. More details of this can be found in the Malpractice, Maladministration and Plagiarism Policy - see the Malpractice, Maladministration and Plagiarism Policy and the Student Behaviour and Intervention Policy.

6. Risk Management

Bias and discrimination: We are committed to fairness and equality; we will reduce the risk of unfair outcomes by upskilling our staff to understand the potential for bias in AI-generated content and to monitor AI outputs for fairness and equality.

Data security: Cybersecurity measures are implemented to prevent data breaches and unauthorised access to sensitive information, including AI-generated content. (see ICT Security Policy FINAL 2026-2027.docx).

Educational integrity: Measures are taken to prevent misuse of AI in assessments and safeguard the integrity of qualifications. (see the Malpractice, Maladministration and Plagiarism Policy).

Online safety: Guidance is provided to protect against harmful or inappropriate content online, including content generated by AI. (See E-Safety Policy).

Monitoring and Review of AI use: the Assistant Principal TLQ and the Head of ICT Services will agree regular checks to carry out on the appropriate use of AI tools, for example review the access to commonly used AI tools. Outcomes from review will be linked to the planning of professional development activities.

6. Future skills development

Knowledge-rich curriculum: Students are equipped with foundational knowledge and critical thinking skills to effectively use emerging technologies like Generative AI, built into digital skills, study skills and academic and vocational delivery.

7. Feedback, evaluation and continuous improvement

We gather feedback from students, families, staff and other stakeholders, and engage in ongoing research to refine our use of generative AI, address concerns, and adapt to evolving educational needs, the College will actively seek feedback from underrepresented groups to ensure that the implementation of AI technologies meets the needs of all members of the college community. For example:

Students	Staff	Parents and Carers	Stakeholders
• Feedback on assessments	• CPD activity • The EdTech Development Team & the	• Parents and carers events • College website and social media	• College website and social media

• Digital skills and study skills lessons • Focus groups and student surveys • The Digital and Academic Resources Centre (DARC)	Digital and Academic Resources Centre (DARC) • College policies and procedures		• Stakeholder briefings and information events

8. AI governance

Key staff at Northampton College who are responsible for this policy's content and implementation:

- The Assistant Principal Teaching, Learning and Quality is the lead for use of generative AI technology. They monitor compliance and work with the wider college community to communicate, promote and regulate AI use, including providing or arranging training where needed.
- Our Data Protection Officer (dataprotection@northamptoncollege.ac.uk) is responsible for advising the college about our data protection obligations in relation to AI use.
- Our IT lead (Head of ICT Services) provides technical support and guidance on the use of AI. Our Digital and Academic Resource Centre Manager and team will provide support around the use of AI.

9. Conclusion

At Northampton College we are committed to harnessing AI technologies responsibly where they can improve teaching and learning outcomes. By applying ethical principles, promoting transparency, and implementing measures to safeguard students, we aim to use AI effectively for the benefit of our college community.

This policy was updated 24th June 2026and will be reviewed in July 2027 or when there are relevant changes to statutory guidance, whichever happens soonest.

10. Linked Policies

- Malpractice, Maladministration and Plagiarism Policy
- E-Safety Policy
- Data Protection Policy
- ICT Security Policy