



Artificial Intelligence (AI) Policy

1. Purpose

This policy sets out how West Herts College Group will use artificial intelligence (AI), including generative AI tools, safely, ethically and lawfully to support teaching, learning, assessment, business operations and student support.

The policy aims to:

- enable innovation while managing risk
- protect students, staff and the college
- ensure compliance with safeguarding, data protection and digital safety requirements
- establish expectations and provide clarity on acceptable and unacceptable use of AI

This policy aligns with Department for Education (DfE) guidance on the use of generative AI in education, statutory safeguarding requirements, and sector principles for FE colleges.

The College will adopt a proportionate, risk-based approach to the use of AI and will ensure that appropriate governance, oversight and assurance arrangements are in place.

2. Scope

This policy applies to:

- all staff (including agency staff and contractors)
- all students
- governors and volunteers where relevant
- any AI systems or tools used on college-owned or personal devices where the use relates to college activity

3. Definition of Artificial Intelligence

For the purposes of this policy, artificial intelligence refers to computer systems that can perform tasks normally requiring human intelligence. These tasks include learning from data, recognising patterns, understanding language, making predictions, supporting decision-making and solving problems. This includes generative AI, (for example, large language models such as chat-based tools) which can create text, images, audio, video or code

Large Language Model (LLM)

A Large Language Model is a type of AI trained on large collections of text so it can generate and process human language. LLMs can answer questions, summarise information, draft written content and support a wide range of language-based tasks.

Machine Learning (ML)

Machine Learning is a branch of AI in which computer systems learn from data to identify patterns and make predictions or decisions without being explicitly programmed for every task. ML underpins many AI applications, including predictive analytics, image classification and automated recommendations.

Agentic AI

Agentic AI refers to AI systems designed to operate with a degree of autonomy. These systems can set or pursue goals, take actions, or make decisions within defined boundaries, sometimes without continuous human instruction. Agentic AI may coordinate tasks, automate workflows or interact with digital systems on behalf of the user. These systems must always operate under appropriate human oversight within the College.

Generative AI

Generative AI is a type of AI that can create new content, such as text, images, audio, video, code, or other digital materials, in response to user prompts or instructions. These include tools such as Microsoft Copilot, ChatGPT, Google Gemini, Claude, DALL·E, Midjourney, Adobe Firefly, Sora and Runway. In the Education setting these tools can support with drafting lesson plans, creating teaching resources and quizzes, creating presentations and summarising reports or policies

4. Principles for the Use of AI

The College adopts the following principles, informed by the Department for Education (DfE) and Joint Information Systems Committee (Jisc) guidance:

- Human oversight: AI supports decision-making but does not replace professional judgement. Users remain responsible for reviewing AI outputs and seek support if they do not have the skills or expertise to do so
- Safety first: Safeguarding and student wellbeing take precedence over innovation.
- Transparency: Staff and students should understand when and how AI is being used and be open about their use of AI.
- Data protection: Personal data must be protected and handled lawfully. Only essential information should be entered into AI tools. Personal, confidential or sensitive data must not be used in unapproved or public systems. This could include names of staff and students; attendance and assessment records; additional learning support details.
- Fairness and integrity: AI must support equitable outcomes, avoid bias and not undermine academic integrity or equality of opportunity.

5. Safeguarding and Student Protection

The use of AI at the College complies with Keeping Children Safe in Education (KCSIE) and the College's safeguarding and child protection policies.

In particular:

- AI tools must not expose learners to harmful, inappropriate or misleading content.
- Any safeguarding concern arising from AI use must be reported in line with the college's safeguarding procedures.
- Staff must remain alert to risks such as over-reliance on AI, exposure to biased content, or inappropriate interactions.

Safeguarding obligations apply equally to digital and AI-enabled activity.

6. Ethical Use of Artificial Intelligence

AI must be used in ways that are consistent with the college's values, public sector responsibilities and duties to students, staff and the wider community.

Ethical use of AI at the college is guided by the following principles:

- Human-centred use: AI is used to support people, not replace professional judgement, teaching expertise or learner effort.
- Fairness and inclusion: AI use must not disadvantage individuals or groups, including those with protected characteristics or additional learning needs.
- Transparency: Where AI meaningfully contributes to content, decisions or processes, this should be clear to those affected.
- Accountability: Humans remain responsible for decisions and outcomes, even where AI tools are used, and for the quality (including accuracy and appropriateness) of any work prepared using AI tools
- Proportionality: AI should only be used where it offers a clear benefit and where risks can be managed appropriately.

7. Acceptable Use of AI by Staff

Staff may use AI tools to support their work where this:

- improves efficiency or quality
- does not involve entering personal, confidential or sensitive data
- complies with data protection, safeguarding and intellectual property requirements
- aligns with professional standards.

Examples of acceptable use may include:

- developing learning materials and resources
- summarising information
- supporting administrative tasks

Staff must:

- critically evaluate AI-generated outputs – these can be inaccurate, biased or misleading and must always be checked
- not present AI-generated content as fact without verification
- provide clear guidance for students on when AI use is permitted
- remain accountable for all work produced using AI
- ensure student work submitted for assessment is demonstrably their own and in-line with Awarding Body and Joint Council for Qualifications (JCQ) guidance

Staff must not

- use AI to mark student work or make assessment decisions
- use AI to generate feedback for students

8. Use of AI by Students

Students may use AI tools where permitted by the college and their programme of study.

The College will:

- set clear expectations about when AI use is allowed and when it is not
- ensure learners understand how AI can support learning without undermining assessment integrity
- treat misuse of AI in assessments in line with the managing student behaviour policy

Students must not:

- submit AI-generated work as their own where this is prohibited
- use AI to bypass learning or assessment requirements
- use AI in ways that breach safeguarding or acceptable use policies, including appropriate referencing of AI in their work

9. Data Protection and Privacy

AI use must comply with UK General Data Protection Regulations (GDPR) and the Data Protection Act 2018.

Staff and students must not:

- enter personal data about students, staff or third parties into public AI tools
- upload confidential or sensitive information or enter such information into AI tools in the form of questions or instructions, unless the tool has been formally approved by the college and is accessed through the college IT system.

Staff and students must:

- only use AI tools that have been formally assessed, approved through College IT processes, and authorised by the College
- comply with any conditions, restrictions or guidance attached to the use of an approved tool
- access approved AI tools only through College-approved systems, platforms, or channels where required

AI systems must only be used where appropriate data protection and security controls are in place. Data protection risks associated with AI use are highlighted by national cyber security guidance and must be considered at all times.

10. Branding and Content Creation

Staff must not use AI tools to generate branded content that uses West Herts College Group's identity, likeness, or brand assets - this includes images, posters, leaflets, or other branded materials.

While AI may be used to support the creation of teaching and learning materials, it must not be used to produce branded content on behalf of the College unless that content has been reviewed by a member of the College's marketing team and confirmed to adhere fully to the College's brand guidelines (including approved logos, colours, typography, tone of voice, and imagery).

AI-generated visuals and copy frequently misrepresent or distort brand assets, and staff are not authorised to publish such content without this check. If you are unsure whether a piece of AI-generated content is appropriate or brand-compliant, contact a member of the Marketing team before use or publication.

11. Cyber Security, Filtering and Monitoring

The College will ensure that:

- AI tools accessed through college systems are subject to appropriate filtering and monitoring
- cyber security risks associated with AI are considered as part of the college's wider security arrangements.

This aligns with DfE expectations on filtering and monitoring standards and National Cyber Security Centre guidance on the risks associated with large language models.

12. Procurement and Approval of AI Tools

AI tools must not be introduced for college use without appropriate approval through Technical Services.

When selecting AI products, the college will consider:

- intended purpose and educational use
- age appropriateness
- safeguarding features
- data protection and security
- supplier terms, data use and retention

An approved AI tool is an AI-enabled system, application or service that has been formally assessed and authorised for College use through the College's agreed approval process.

Approval of a tool does not mean that it is approved for every purpose or every type of information. Users must comply with any conditions or restrictions attached to its approval.

The College will maintain an appropriate record of AI tools approved for use and any conditions or restrictions applying to them.

The DfE generative AI product safety standards provide a good reference point for assessing suitability.

13. Training and Awareness

The College will ensure that:

- staff receive appropriate guidance and training on the safe and effective use of AI
- students are supported to develop digital and AI literacy skills including how AI is used in employment sectors related to their programmes of study.

14. Monitoring, Review and Breaches

Compliance with this policy will be monitored through existing governance, safeguarding and quality assurance arrangements.

15. Roles and Responsibilities

The Senior Management Team is responsible for ensuring appropriate governance and oversight of AI use across the College.

Relevant College managers, including Data Protection, Safeguarding, IT/Information Security and Curriculum/Quality, are responsible for providing advice and oversight within their areas of responsibility.

Managers are responsible for ensuring staff understand and comply with this policy.

All staff and students are responsible for using AI in accordance with this policy and for reporting concerns or incidents through the appropriate College procedures.

16. Related Policies

Data Protection Policy

IT Policy

Malpractice, Maladministration and Plagiarism Policy

Safeguarding and Child Protection Policy

Staff Code of Conduct

This policy is reviewed annually to ensure compliance with current regulations.

Authorised by CLG	Date September 2026
--------------------------	----------------------------