LONDON METROPOLITAN UNIVERSITY

Artificial Intelligence (AI) Usage Policy

London Metropolitan University

Version control	1.0
Owned by:	Executive Director of Digital and Information Services
Latest amendment on:	September 2026
Approved by:	University Executive Board
Approved on:	23-09-26
Coming into effect on:	01-10-26
Next Planned Review date:	By 31st March 2027

LONDON METROPOLITAN UNIVERSITY

1. Purpose and Scope

This policy sets out how London Metropolitan University expects all users to use Artificial Intelligence (AI) tools in university work and study. It applies to the use of AI tools across all University activities, accessed through university-approved accounts, personal accounts used for university purposes, and AI features embedded in third-party software used on the University's behalf. It also provides the accountability and governance that support the University's responsible and ethical use of AI.

It forms part of the University's wider Information Management Policy Framework and restates those principles specifically for the use of AI across the institution. It should be read alongside the University's IT Acceptable Use Policy, which sets out the general standards expected when using University IT systems, networks, and accounts.

The policy is not intended to prohibit the use of AI. It provides clarity on responsible use and on which tools are approved in different contexts. AI use should be enabled where it advances learning, inclusion, creativity, research or service quality; restricted where risk cannot be managed proportionately; and never allowed to obscure human accountability, widen inequality or weaken the evidence on which academic and institutional decisions depend. AI tools can improve productivity, quality and decision-making when used responsibly. This policy sets clear boundaries on where AI can be used freely, where its use must be disclosed, and where its use is not permitted, so that users can adopt these tools with confidence. It is an overarching usage policy that provides general principles and guidance; it does not replace more specific policies or guidance for areas such as research, teaching, learning or assessment.

AI is a fast-evolving technological area. In addition to ad-hoc updates where required, this policy will be reviewed at least termly to reflect the latest developments and ensure it remains fit for purpose.

For the purposes of this policy:

- **AI tools** include systems or software features that generate, summarise, classify, recommend, translate, analyse, automate or otherwise assist with teaching, learning, research, content, data, decisions or workflows using artificial intelligence techniques.

- **University information** includes confidential, commercially sensitive or non-public institutional information, and any information that could identify individual staff, students, applicants, partners or other individuals.

2. Guiding Principles

Trust with accountability: all users are trusted to use AI sensibly, provided they remain personally accountable for anything produced with its assistance.

Transparency: where AI has materially shaped a piece of work, its use should be declared.

Human oversight: AI output is a draft or a suggestion, not a finished, verified answer. A person must review, correct, and take responsibility for the final result.

Data protection first: no confidential, personal, or commercially sensitive data should be entered into a public or non-approved AI tool.

Proportionate risk: the level of scrutiny and permission required should scale with the sensitivity and impact of the task.

Inclusion: AI should be used to promote accessibility, participation and equitable outcomes, and its use

should not create or reinforce barriers or disadvantage any staff or student group

3. Roles and Responsibilities

- Individual staff: responsible for using AI in line with this policy and for the accuracy and appropriateness of anything they produce with AI assistance.

- Students: responsible for using AI in accordance with this policy, the University principles on student use of AI, and any local assessment requirements. Students must maintain academic integrity, declare AI use where required, and remain responsible for the accuracy and originality of their work. The library student hub provides more information https://libguides.londonmet.ac.uk/collection-ai

- Line managers: responsible for clarifying any team or role-specific restrictions and for raising concerns about inappropriate use.

- AI Governance Committee: responsible for overseeing and recommending usage of AI across the University – see committee Terms of Reference

- Centre for Teaching Enhancement: responsible for providing guidance and support on the educational use of AI across teaching, learning and assessment, and working through the Generative AI in Teaching and Learning Steering group to monitor emerging risks and opportunities and make recommendations to the AI Governance Committee.

- Centre for Equity and Inclusion: when proportionate to the impact, review and provide guidance where proposed AI use or policy changes may materially affect equity, inclusion or accessibility.

- Digital and Information Services: responsible for maintaining the list of approved tools, data processing agreements, and technical access controls as well as ensuring that AI-related demand is managed through the University's existing Digital demand process and passed to the AI Governance Committee where required.

- Legal/Compliance and HR: responsible for advising on data protection, IP, and employment implications, and for handling any misuse investigations.

- Marketing and Communications: responsible for setting and maintaining guidelines for the use of AI-generated and AI-assisted content and assets that represent the University, including copy, imagery, video, audio and other creative materials. This includes establishing appropriate standards for brand representation, authenticity, transparency and quality, and providing guidance on when and how AI-generated content may be used across university marketing and communications channels.

4. Accountability and Governance

- All requests for new AI-enabled digital services must be submitted through the University's Digital Demand process, to ensure alignment with institutional requirements and appropriate value for

money.

- All requests for changes or enhancements to existing AI-enabled services must follow the IT Services Change Request process.
- IT Services will maintain a comprehensive Service Catalogue, ensuring that all instances of software utilising AI are accurately documented.
- Instances of technology using AI within a broader platform will also be identified and recorded in a central register, maintained by IT Services, so that users can understand where AI-enabled processes, generated content, recommendations or summaries are used and the University can maintain appropriate oversight.
- Risks relating to the security or technical use of AI are tracked in the IT Services Risk Register. Risks relating to data protection sit within the DPO's risk register. Other risks relating to the use or effect of AI on services should be captured in departmental risk registers.
- All purchases of IT software and services must include an assessment of both current and intended use of AI, critically considering data protection, cybersecurity, and ethical implications.

5. AI tools

Microsoft Copilot is currently the only generative AI chat tool approved for use with university data and information – other tools can be used if no university information is given to them. All university users have access to Copilot as part of our institutional Microsoft 365 licence. Further guidance on how to use Copilot effectively is available here:

Copilot Chat for Work

Examples of other AI tools and guidance on their use are available:

AI-Tools.aspx

Only tools marked as “Internal and Confidential” are approved for use with university information; use of university information in other tools is prohibited. For this purpose, **university information** means any confidential or commercially sensitive content or data, any information that could identify staff or students, information relating to university initiatives that are not already in the public domain, or content created by someone within the institution where permission has not been given for use outside the University.

Beyond the tools approved for university information, the list is not exhaustive and is intended to illustrate the existing breadth of positive usage across the University and provide clarity on different use cases. It will continue to be updated to reflect our evolving usage of AI-specific tools.

6. Acceptable AI Use

The following categories are intended to help users make practical decisions about AI use. Where there is uncertainty, users should take the more cautious approach and seek advice from their line manager, module leader, IT Services, the Data Protection Officer, Legal or the AI Governance Committee as appropriate.

6.1 Freely Permitted (within the boundaries of this policy)

The activities below are permitted only when the tool is approved for the information being used and any

relevant assessment, research, copyright and disclosure requirements are met:

- Drafting or improving emails, reports, presentations, and internal documentation.
- Creation of media including images, moving image and sound
- Use of tools embedded in approved platforms such as Weblearn
- Summarising publicly available or already-internal, non-sensitive documents, provided that any copyright, licensing, contractual or other restrictions relating to the use of the content are followed
- Brainstorming, outlining, and idea generation.
- Writing, explaining, or debugging code, subject to the organisation's standard code review process.
- Using AI as a study or explanatory aid to understand a topic, tool, or process.
- Using AI to support learning, study and research activities, including understanding concepts, exploring topics, generating search terms, identifying sources and creating revision materials.
- Producing first drafts of external-facing material (e.g. client communications, policies, marketing copy), provided that the author reviews and edits it for accuracy and takes responsibility for the content.
- Improving the accessibility and inclusivity of communications, with human review of the final content, for example plain language drafts, alternative formats and checking readability.

6.2 Permitted with Disclosure

- The use of AI to assist with the production or editing of genuine photography, video and audio, provided its use does not materially alter or misrepresent the people, places, events or experiences depicted.
- Using AI to analyse datasets or produce figures used in decision-making documents. The method and tool used should be noted.
- Using AI notetakers or meeting summarisation tools. Attendees should be informed when a meeting is being recorded or summarised by AI.
- For students, using AI in assessments, dissertations or research activities where University regulations or module requirements require its use to be declared, for example the ‘AI in Assessment’ policy

6.3 Not Permitted

- Entering personal data, financial data, credentials, or any confidential/commercially sensitive information into a non-approved or public AI tool.
- Using AI agents or AI browsers to log into university systems or sharing login credentials with an AI tool or agent.
- Presenting AI-generated or AI-manipulated output as entirely your own original work without review or disclosure where disclosure is required by this policy.
- Using AI to generate content that misrepresents or could be interpreted as misrepresenting facts, fabricates data or sources, or impersonates a real person.
- The use of AI to recreate, modify, distort or generate variations of the University logo or other

protected brand assets.

- Relying on AI output for final decisions in high-risk areas (legal, financial, HR, safety) without qualified human review.

Where users are uncertain whether a proposed use of AI is permitted, they should not proceed until they have sought appropriate advice. Staff should normally consult their line manager, IT Services, the Data Protection Officer, Legal or the AI Governance Committee, depending on the nature of the proposed use. Students should consult their module leader, supervisor or the relevant student support service where the question relates to assessment, research or reasonable adjustments.

7. Data Protection and Confidentiality

Users must not input personal data (as defined under UK GDPR), client-confidential information, or commercially sensitive material into any AI tool that has not been contractually approved for such use by IT Services and Legal. Where an approved enterprise tool is used, staff should still apply a 'need to know' principle and avoid pasting more information than the task requires.

The use of university information in any AI system beyond those already approved is not permitted without a completed Data Protection Impact Assessment (DPIA) and security review. The use of copyrighted material with AI systems must comply with applicable copyright law, licence agreements, contractual terms and University policies. Users remain responsible for ensuring that they have the appropriate rights, permissions or licences to use content with AI tools and should seek advice where there is uncertainty.

All data used in the development, training, testing, or deployment of AI systems must be accurate, relevant, representative, and obtained through ethical and lawful means. Data sources must be documented, and reasonable steps taken to assess data quality and reliability with particular attention to mitigating bias, ensuring that data appropriately represents the populations and contexts in which the system will be used, and avoiding misleading, outdated, or incomplete information. Datasets should be regularly audited, especially where outcomes may affect individuals or groups.

AI outputs that reference or appear to reproduce real individuals' personal data should be treated with caution and verified before any further use or distribution. Extra care, including regular reviews and impact assessments, is required for systems handling student records, health data, biometric data, or other highly sensitive information.

8. Accuracy, Bias, and Human Oversight

AI tools can produce plausible sounding but incorrect, outdated or biased content, often referred to as “hallucinations.” Users remain fully responsible for verifying factual claims, checking calculations, and confirming that any code, figures or citations produced by AI are correct before they are used or shared.

AI-generated citations, references, quotations or summaries must be checked against the original source material before being relied upon or included in any document.

Decisions influenced or made by AI systems must be explainable, traceable and subject to human oversight,

especially in high-stakes areas such as assessment, admissions and research integrity.

9. Security

All centrally supported IT services using AI, whether new services or enhancements to existing ones, must undergo a security review to ensure any cyber security risks are understood, documented, and, where possible, mitigated.

The University will deploy responsible AI-based tooling to help defend against AI-enabled cyber-attacks.

All incidents relating to the use of AI must be reported through the IT Service Management portal and managed in line with standard IT incident management processes.

10. Academic Integrity, Teaching, and Research

The University supports responsible academic inquiry, pedagogic innovation and critical engagement with AI. Restrictions will be proportionate to the risk and will not unnecessarily limit legitimate teaching, scholarship, research or academic debate. The following requirements apply to all staff engaged in teaching, research, and administrative tasks involving AI:

- Your Responsibilities: it is your responsibility to ensure your use of AI is ethical and within the policies stated above.
- Your Responsibilities to Others: if you have supervisory responsibilities (academic or managerial), you must ensure those working with you are aware of the University's current guidance on AI use.
- Academic Integrity: all work presented for assessment, or representing the results of research, must comply with the University's Academic Integrity regulations.
- Teaching and Learning: staff developing or using AI in any learning activity must ensure it is used responsibly and conforms to university regulations.
- Research: staff using AI in research must ensure it is ethical and compliant with university regulations, including obtaining research ethics committee authorisation where necessary.
- Communication: presenting AI-assisted work (e.g. for conferences, publications) must follow the guidelines of the relevant funder, conference organiser, or publisher, as well as University policy.
- Values: the use of AI must remain consistent with the University's values of collaboration, compassion, inclusivity, and integrity.

This will be supplemented by the University providing AI literacy and ongoing training and development opportunities.

11. AI for Public Good

All new AI-enabled services for corporate, academic or research purposes involving University information must first be reviewed by the AI Governance Committee or DSSG. The review will consider whether the proposed AI model, tool or process presents risks of bias, unfairness, misinformation, exclusion or other outcomes contrary to the University's values. When selecting or deploying AI at scale, the University will consider environmental and social impacts alongside educational value, accessibility, cost, security and legal

compliance, where relevant and reasonably assessable

Any AI model provided by the University should be made equitably and accessibly available to the groups for whom it is intended.

All content produced using AI must be effectively reviewed and labelled to combat misinformation related to AI-generated content.

12. Accessibility and Reasonable Adjustments

AI tools may be used to meet an accessibility need or as part of a reasonable adjustment, for example through text-to-speech, summarisation or writing support, provided their use meets data protection and any relevant assessment requirements. Staff should seek advice through HR or line management where appropriate. Students should seek advice through the University's Disability and Dyslexia Service (DDS) where appropriate.

13. Breach of Policy

Use of AI that breaches this policy, particularly entering confidential data into unapproved tools, failing to disclose AI use where required, or misrepresenting AI-generated work as verified fact, will be handled under the University's normal disciplinary, academic misconduct, information security or other relevant procedures.

14. Review

This policy will be reviewed at least termly, and sooner if there is a material change in the AI tools available, applicable law, or organisational risk appetite. Feedback from staff is welcomed and should be directed to IT Services.