UNIVERSITY OF
FORWARD
THINKING
WESTMINSTER

POLICY IN RELATION TO THE SAFE USE OF GENERATIVE AI (GenAI)

1. Purpose and Scope

This policy sets out the guidelines for the use of Generative Artificial Intelligence (GenAI) systems[1] by the University of Westminster and should be read in conjunction with the University's position statement on the use of GenAI. It applies to all students, colleagues, third-party suppliers, and partners engaged in using or developing such systems within or on behalf of our institution. These guidelines support the safe and ethical use of GenAI at the University and help prepare students and colleagues for the widespread use of GenAI across industry, commerce, and the professions.

2. Definitions

For this policy, GenAI is defined as an AI system that generates new outputs in a range of possible formats such as text, images, sounds (including for example music, singing, voice narration) and video. Some specific current examples of such GenAI systems include ChatGPT, Microsoft Copilot, Gemini, and Synthesia.

3. Ethical Considerations

All users[2] of GenAI must consider the ethical and legal implications of their work. This includes being mindful that GenAI systems can generate harmful, misleading, biased, or discriminatory content. GenAI must not be used to promote discrimination, bias, or harm. The following AI ethics principles will guide the use of GenAI at the University:

3a. Fairness: GenAI should not be used to create unfair or inequitable conditions for users and participants.

3b. Transparency: The use of GenAI should be as transparent as possible in all use case scenarios[3], so that users understand how the technology and its algorithms are being deployed and if and how any of their university data is being used. Users should be made explicitly aware when GenAI is being used, for what reason and for what purpose.

[1] This relates to systems that are either accessible publicly or only through secure internal interfaces.

[2] Users may include students, colleagues, research participants, data subjects or researchers.

[3] Use case scenarios may include for example, a) Use by colleagues or students of third-party publicly facing GenAI systems such as ChatGPT; b) a researcher developing a GenAI system; c) a research participant who has been asked to interact with or whose data is being added into an in-university developed GenAI system; d) an individual staff member or student whose data is being added into a corporate GenAI system.

3c. Accountability: Those who use or deploy GenAI will act professionally and be accountable for any intentional and potential harm or misuse.

3d. Respect for privacy: The use of GenAI should respect the privacy of users and should not be used to collect, store, access or share their personal data without their consent. This includes not generating a likeness of others in images, videos, audios, or written form without consent.

3e Inclusiveness: GenAI systems and outputs should empower everyone, serving to help combat the possibility for discrimination.

3f Reliability: The output from GenAI systems should be as valid and reliable as possible.

3g Accuracy and Error Management: Users should be aware of the potential for inaccuracies and false positives in GenAI outputs. Regular audits and quality checks should be implemented by individuals to identify and mitigate such issues.

4. Data Privacy and Information Security

The University undertakes to protect the privacy of users[2] when using and training GenAI. This includes not collecting storing, accessing or sharing personal data without consent and using or ensuring appropriate security measures to protect data from unauthorised access (see below). All data used in the development and operation of GenAI systems must respect the privacy and rights of individuals involved and be securely transmitted, stored and managed in accordance with the University of Westminster’s Data Protection Policy and relevant data protection laws. In the case of the development of GenAI systems by researchers for research, and the creation of datasets to train such a system, this should also be done in accordance with the University's Research Data Management Policy. .

The University will take all reasonable steps to protect the security of its computer systems and networks when GenAI is being used through corporate systems. This includes using appropriate security measures to protect against malicious attacks and ensuring that users are aware of the risks associated with using the technology. Similarly, the University will work with third-party suppliers to ensure that services used by the University are equally safe and secure.

Any use of GenAI for automated decision-making must be explicitly approved and undergo additional data protection review. Such cases must comply with UK GDPR (see Article 22 - Automated individual decision making, including profiling) and related UK data protection laws.

5. Data Sovereignty

All use of GenAI must comply with data sovereignty rules. Information created or collected in the UK will remain under UK jurisdiction. When using internationally hosted GenAI platforms, users must consider and comply with the source country's laws regarding data use, privacy and access.

6. Usage Guidelines

GenAI must be used responsibly and not used to deliberately deceive of falsify. This includes checking as far as possible that outputs are accurate and non-biased. Inappropriate uses, such as creating malicious deepfakes[4] or generating misleading content, are strictly prohibited. All users must always clearly disclose the use of GenAI when sharing or publishing generated content. Students who use GenAI in their coursework must ensure that the use is permissible (see University Advice to Students on GenAI and Procedures Relating to Academic Misconduct and Diversity and the Dignity at Work and Study Policy). Colleagues who use GenAI in their research and/or discipline of work must ensure that the use is permissible and that they are open about the use of GenAI. The University owns all intellectual property that is created using GenAI through corporate systems (such as Microsoft Office or the Blackboard VLE) unless otherwise agreed to in writing.

7. Risk Tolerance and Ownership

The University of Westminster recognises the need to define its risk tolerance for the use of GenAI. A balanced approach will be adopted, considering both the potential benefits and the associated risks. GenAI systems that negatively affect safety or fundamental rights (see Fundamental rights in AI – What to consider) or raise significant ethical issues in research and knowledge exchange activity, will be considered high risk. Systems using GenAI considered as a high risk should not go into production without remediation. Residual risks should be escalated to the University Senior Information Risk Officer (SIRO), namely the University Secretary and Chief Operating Officer, for formal acceptance and auditing purposes following the University risk management methodology. All high-risk cases escalated to the SIRO will also be reported to the Information Compliance Team and the Data Protection Officer to ensure comprehensive oversight and compliance.

The responsibility for conducting actions to mitigate risks should lie with the individuals or teams directly involved in the use of the GenAI system concerned, while the responsibility for assessing novel use cases or the output of approved use cases should be designated to the appropriate oversight body (Ethics Committee for University Research and Knowledge Exchange or the relevant College Teaching Committee). In the case of using GenAI by Professional Services, ethical oversight will be provided by the Professional Services Director's Group.

8. Use Cases and Restrictions

To mitigate risks associated with GenAI use, the University of Westminster will classify use cases according to whether they are appropriate to be considered through a Self-Assessment and notification route or require more formal committee Scrutiny and Approval. Some indicative use cases covering learning and teaching and research are shown as examples in this list of GenAI Use Cases.

Risk mitigation measures for GenAI systems will be integrated with the existing Data Protection Impact Assessment (DPIA) process. Any use of GenAI involving personal data must undergo a DPIA in line with established University procedures.

It can be anticipated that most proposed uses conducted in internal facing, secured corporate tools and systems will likely be categorised within the Self-Assessment and Notification category. It is also intended that going forward, the GenAI Use Case table will be regularly updated as new low risk use cases emerge. However, it can also be anticipated that some use cases, even if they use internal facing systems, may necessitate scrutiny by the relevant ethics body.

[4] A malicious deepfake may be defined as a video of a person in which their face or body has been digitally altered so that they appear to be someone else, typically used maliciously or to spread false information.

9. Authority for Decision Making

The authority to make decisions regarding the uses of GenAI that require formal scrutiny rests with the relevant Ethics Group. These groups, comprising representatives from relevant departments and key stakeholders, will consider ethical concerns related to GenAI. For teaching and learning the relevant group is the University Teaching Committee, for research is the relevant Research Ethics group and for Professional Services it is the Professional Services Director's Group. A central record of all approved GenAI use cases requiring formal scrutiny across all areas of activity will be maintained and available to the Information Governance Advisory Group (IGAG) for review.

10. Information Sharing

9a. Disclosure to Students, Employees, and Third Parties: The University of Westminster recognises the importance of transparency and open communication. Therefore, information about the use of GenAI should be disclosed to students, employees, and relevant third parties. Such disclosure should include the nature of the GenAI system being used, the purpose for which it is being used, and any potential impact on individuals' data or privacy. All users can find information about university approved systems via the university's AI blog.

9b. Disclosure Requirements: Students and employees who use GenAI to generate content through systems or software that they would not be expected to be using within their subject context and the guidance of their tutors, must disclose this fact when submitting or sharing the generated content. They should clearly indicate that GenAI was involved in the creation process. For further information please Guidance for Students and Code of Practice for Academic Colleagues.

9c. Employee Monitoring: The University reserves the right to monitor the use of GenAI by employees to ensure compliance with this policy. Employees and students should be aware that the use of GenAI, and particularly external public facing systems, without due consideration of the legal and ethical implications of their work, may result in disciplinary action. Any suspected misuse of GenAI should be reported in the first instance by email to GenAI@westminster.ac.uk

11. Training and Awareness

The University of Westminster is committed to promoting the use of GenAI in ethical ways through training and awareness programs. All users of GenAI are required to complete a training program on the ethical use of AI. This training program will cover topics such as the responsible use of GenAI, ethical considerations, privacy, data protection, and compliance with this policy. The University of Westminster will ensure that its users are aware when any system it supports uses GenAI.

12. Monitoring and Auditing

The University of Westminster will periodically monitor the use of GenAI to ensure compliance with this policy. Audits will also be carried out by relevant departments (e.g., Learning Innovation and Digital Engagement for the virtual learning environment and Information Systems and Services for Microsoft Office 365) to assess adherence to ethical guidelines and identify areas for improvement.

13. Review and Updates

This policy will be reviewed at least bi-annually, or more frequently, if necessary, to ensure it remains relevant and up to date with technological advancements and legislative changes. Recommendations for updates or improvements to the policy may be submitted to either the Ethics

Committee for University Research and Knowledge Exchange (for research or knowledge exchange linked suggestions) or the relevant College Teaching Committee (for teaching related matters) or the Professional Services Director's Group (for corporate services matters).

14. Policy Approval and Implementation

This policy is approved by the University Executive Board (UEB) and will be implemented by the schools and professional services departments, working closely with relevant support services.

15. Related Policies

This policy forms part of the information security management system (ISMS) at the University of Westminster.

The Policy for the safe and ethical use of generative GenAI should be read in conjunction with all other University information management policies, which are reviewed and updated as necessary to maintain an effective Information Security Management System to meet the University's business needs and legal obligations. These include: The Acceptable Use Policy, Information Security Policy, Research Data Management Policy, Student Code of Conduct and Code of Practice Governing the Ethical Conduct of Research.

16. Compliance with the Policy

Failure to meet the requirements detailed within this Policy and the Framework in protecting University information (or that entrusted tr us by a third party) puts the University at risk of reputational damage, financial penalty, breach of legal, contractual or regulatory requirement. It may lead to disciplinary action that will be dealt with under the appropriate disciplinary code or procedures. Additionally, where it is suspected that an offence has occurred under UK law, it may also be reported to the police or other appropriate authorities.

17. Publishing Policies

This policy is published on the University website at https://www.westminster.ac.uk/about-us/ouruniversity/corporate-information/policies-and-documents-a-z and can be requested in a range of formats e.g. Word, PDF, plain text and alternative formats such as large print or Braille.

Last updated: 23/09/2024

Next review date: 01/4/2025