Responsible AI Policy

Contents

1. Statement of Policy

The Open University is committed to processing and using data in an ethical manner and to using data processing technologies and the outputs and assets they create responsibly and ethically. Recognising the potential effects, both positive and negative, of large-scale data processing technologies such as Artificial Intelligence (AI) and Machine Learning (ML), the University will use such technologies in support of its mission and take deliberate action to limit the harms that may arise from their use, including through training employees on the appropriate use of AI.

2. Introduction

The Open University will explore the opportunities offered by AI to enhance students' experience and its business operations, and will navigate the challenges and risks thoughtfully.

The University collects and uses data and information through multiple routes and for numerous purposes, including the provision of timely and appropriate support to its students and staff. The collection and use of personal data is subject to data protection legislation and the University's Data Protection Policy.

The University holds significant assets in its curriculum materials, academic research, intellectual property, internal governance and commercial endeavours. All information assets are protected by the University's Information Security Policies.

Rapid development of large-scale data processing technologies such as AI means AI-based tools and services are widely available to support both everyday administrative tasks and more complex processes and problems. However, the nature of AI means that the University's use of it may create new risks. These can be risks to the security and integrity of the data itself, or risks to anyone affected by the AI use. A review and evaluation process has been created to ensure AI use is adequately scrutinised to confirm it is achieving its objectives without causing unintended risks or harms.

With significant potential for unforeseen consequences from AI use, it is incumbent on the University and its employees to ensure that use of AI within the organisation is appropriately managed to keep the risks to our students, colleagues, data and reputation within acceptable limits.

3. Purpose

The purpose of this policy is to provide guidance on the development and adoption of AI within the University and a consistent, standardised approach across the organisation. This policy and accompanying process will assist staff in procuring, designing, developing and deploying AI and similar technologies, and in identifying and mitigating risks arising from AI use. It will assist students, enquirers, members of the public and external organisations in understanding the University's approach to the use of AI.

This policy aims to:

- Support the delivery of the University's mission and goals by providing clarity over the appropriate use of AI.
- Enable staff to follow an ethical and responsible approach to procuring, developing or deploying AI-based tools and services;
- Protect the rights and interests of all stakeholders;
- Define the roles and responsibilities for responsible AI use; and
- Describe the potential consequences of non-compliance with this policy.

4. Scope

This policy applies to use of AI that does not fall within the GenAI End User Acceptable Use Policy and is not classed as prohibited or high-risk under the EU AI Act. High-risk AI will be subject to the controls required by the Act and will be managed accordingly. For relevant use cases, this policy applies to:

- Everyone working for or on behalf of the University or organisations in the OU Group, who design, develop or deploy large-scale data processing technologies, including AI and ML, during the course of their work. This includes all employees, contractors, and third parties. It also applies to anyone who accesses University systems for work purposes, including suppliers and contractors.

- All types of AI, including Generative AI (Gen AI) and General Purpose AI;
- All types of AI use, including generation of text, audio, images, animations and videos, speech recognition, data analysis, insight generation, chat bots and recommendation engines;
- AI developed by the University and third-party AI systems used in the course of University work;
- Use cases that involve data or information held by or provided by the University in any format, including raw data, text, audio and video;
- Use cases that involve personal information and use cases that don't involve personal information.

This policy does **not** apply to end-user use of AI that is compliant with the GenAI End User Acceptable Use Policy.

5. Policy principles

5.1 Assign accountability and responsibility

- As a deployer or developer of AI, the University is legally accountable for its safe and compliant use.
- In all use cases in scope, the person with overall responsibility for complying with this and other relevant University policies, plus applicable laws, must be identified and confirm that they have responsibility for the AI use. They are responsible for ensuring that there are mechanisms in place to address any unintended consequences or ethical concerns.

5.2 Adopt technically robust and safe solutions

- AI and its supporting infrastructure must be technically safe and robust to ensure the security and resilience of the AI systems.
- This includes AI systems and related computer systems, networks, digital assets and infrastructure needed to run the AI.

5.3 Make privacy and data governance standard

- Personal data in AI must be used in compliance with data protection laws, including managing access to the data and supporting individuals' rights over their data.
- All data used in AI must be properly governed to ensure an appropriate level of accuracy and data quality.
- These requirements apply in design and development of the AI system, and to data generated by the AI use.

5.4 Design for transparency and explicability

- The use of AI must be openly communicated in a timely way to those interacting with it, provided with the output from it, or affected by its use.
- Transparency should be designed into the AI lifecycle to support the monitoring and traceability of data and decisions at all stages.
- AI systems should be designed with explicability in mind. This is especially important for systems that inform decisions or perform actions that can cause harm or restrict an individual's rights.

5.5 Build in human agency and oversight

- Decisions made by AI systems should not replace or diminish the role of humans in critical decision-making processes. Individuals must retain **agency**, that is, the capacity to make intentional and informed decisions and exercise control.
- AI systems must be overseen by humans using supervision, monitoring, safeguards and accountability mechanisms. Human **oversight** is crucial to prevent unintended consequences, biases, and potential harms that AI systems might cause. Effective oversight depends on humans in the human-AI partnership understanding the AI and its limitations.

5.6 Incorporate diversity, inclusion, non-discrimination and fairness

The following points should take account of characteristics that are protected under the Equality Act 2010 or under University policy, namely sex, gender reassignment, disability, race, maternity and pregnancy, age, marriage and civil partnership, religion or belief and sexual orientation, as well as caring and dependents, political opinion and socio-economic background. Characteristics that are not protected under legislation or policy should also be accounted for.

- The benefits and costs (financial or other) of AI should be fairly distributed.
- The use of AI should not result in the discrimination and marginalisation of certain groups.

- A diverse range of users and perspectives must be represented throughout the entire lifecycle of the AI to prevent bias and ensure that the AI can fairly and accurately represent and serve a broad user base.
- Access to digital infrastructure and services must be considered, both in data used in AI and in end use, so that biases caused by limited digital access can be mitigated.
- AI should not perpetuate or amplify existing prejudices or biases, either in how it operates, how it is deployed or sold, or who has access to it. This applies to exclusion of under-represented groups from datasets, as well as digital poverty and e-exclusion affecting access to digital resources.
- Decisions, actions, and processes of AI should be impartial and unbiased, and should provide equal opportunities and equitable outcomes. The diverse needs, circumstances, and rights of all parties involved should be considered and any risks to fairness mitigated.

5.7 Promote individual, societal and environmental wellbeing

- AI systems should contribute to, and not harm, individual wellbeing, the quality and functioning of society, and the quality of the environment.
- The principle of diversity, inclusion, non-discrimination and fairness must be followed, to mitigate biases that might negatively affect individual wellbeing.

- Impacts on society and the environment must be considered across the AI supply chain.
- The accountability principle must be followed, to ensure that the University takes responsibility for the impact of its AI use.

5.8 Keep AI use proportionate

- Proposed AI uses must be impartially assessed to evaluate whether, taking the other principles into account, AI use is necessary, appropriate, and the best solution to achieve the desired outcome.
- AI should be used where its deployment is proportionate to the nature of the objective, as the nature and size of the risks associated with AI can be significant.

6. Responsibilities

All employees using or planning to use AI in a way that is not covered by the GenAI End User Acceptable Use Policy must comply with the principles of this Policy and the requirements in the Responsible AI Standard.

The **Senior Information Risk Owner** (SIRO) has overall responsibility and authority for risk management relating to AI use in the University. The SIRO is responsible for understanding the impact of risks relating to AI use on the University's strategic objectives, and authorising appropriate mitigations or acceptance of risk. The SIRO is the University's strategic risk owner for information-related risks.

The University Secretary is the University's SIRO.

The **Director, Information Rights and Compliance** is responsible for assessing or arranging the assessment of the risks arising from AI use, and advising the SIRO and colleagues on risks and issues.

The **Information Rights team** is responsible for operating the University's AI governance processes, including maintaining and communicating policies, managing records and documentation, reviewing Responsible AI Assessments and advising colleagues on responsible and compliant use of AI.

The **Chief Information Security Officer** is responsible for managing the cyber security risks to the organisation.

Business owners of AI projects, initiatives or use cases have overall responsibility for the AI use and for monitoring compliance within their area of responsibility. They are responsible for ensuring that all staff, volunteers, consultants, research students and individuals associated with the project or initiative are aware of this and related policies and processes and have the necessary resources to comply with them. They are also responsible for ensuring that people developing, deploying or using the AI are appropriately trained.

7. Non-compliance

Any deliberate or persistent infringement of this policy will be treated seriously by the University and may result in disciplinary action according to the Disciplinary Policy. If infringement of this policy represents misconduct in research, it will be investigated accordingly and may result in notification to external bodies including funders or publishers.

8. Useful references

The following resources contain information relevant to the responsible use of AI.

8.1 University policies and guidelines

- GenAI End User Acceptable Use Policy
- Data Protection Policy
- Data Protection Standard
- Information Security Policies
- Content, licensing and intellectual property (Library Services)
- Equality, Diversity and Inclusion
- Accessibility Standard
- Guidance on Generative AI in Learning, Teaching and Assessment

8.2 Laws

The following laws are relevant to the use of AI in the University:

- The UK Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- The EU General Data Protection Regulation (EU GDPR)
- The EU Artificial Intelligence Act 2024
- The Computer Misuse Act 1990

- The European Convention on Human Rights
- The Equality Act 2010 and Public Sector Equality Duty (PSED)
- Equality legislation for Northern Ireland
- The Copyrights, Designs and Patents Act 1988
- Accessibility requirements for public sector bodies
- Waste Regulations 2011
- Waste Electrical and Electronic Equipment (WEEE) Regulations 2018
- UK government principles for AI

8.3 Other references

- Jisc: Exploring digital carbon footprints
- Scope 3 Calculation Guidance: GHG Protocol
- ICO guidance on artificial intelligence
- Government Digital Service (2020). Data Ethics Framework
- High-Level Expert Group on Artificial Intelligence AI HLEG (2018). Ethics Guidelines for Trustworthy AI. European Commission
- Leslie, D. (2019). Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. The Alan Turing Institute
- Wright, D (2010). A framework for the ethical impact assessment of information technology. Springer Science + Business Media

9. Glossary

- **'Artificial Intelligence'** does not have a single agreed definition but the definition provided by the UK government in 2019 is useful, as follows.

  "AI can be defined as the use of digital technology to create systems capable of performing tasks commonly thought to require [human] intelligence.

  AI is constantly evolving, but generally it:

  - involves machines using statistics to find patterns in large amounts of data;
  - is the ability to perform repetitive tasks with data without the need for constant human guidance."

- **'AI system'** is used as defined in the EU AI Act, meaning a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

- **'AI tool'** as used in this document refers to a functionality or service that an end user might interact with that is run or supported by AI.

- **'Personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This is in accordance with the definition of personal data in the EU and UK GDPR.

10. Version control

10.1 Summary of significant changes since the last version

This Policy replaces the Data Ethics Policy. Key differences from the Data Ethics Policy are:

- A wider scope to encompass the use of data technologies rather than just the use of data held by the University;
- Revised principles to reflect the broader scope and the evolving field of responsible AI use.
- Specific recognition of the human and societal impacts of AI, particularly on equality, diversity, non-discrimination and inclusion.
- Acknowledgement that the processing and use of data, AI, ML and related technologies have an increasing digital carbon footprint.
- Better alignment to the United Nations Sustainable Development Goals.

10.2 Current version

Version number: V1.3 minor amendments to wording, template changes and restructuring to separate requirements into a Responsible AI Standard. Amendments to reflect the changes of scope in relation to the GenAI End User Acceptable Use Policy.

Approved by and date: University Secretary, October 2025

Publication date: January 2026

Review date: November 2026

Document owner: Director, Information Rights and Compliance

Department: Information Rights

Author: Rebecca Ward