

V1

AI Policy



BATH SPA
UNIVERSITY

1. Introduction

- 1.1 Artificial intelligence (AI) is defined by the Oxford Dictionary as the theory and development of computer systems to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making and translation between languages. AI can be used for task automation (macros, chatbots), content generation (images, videos, text, music), human representation (deepfakes, voice, personas), insight extraction (machine learning, analytics), decision-making (optimisation, decision trees) and human augmentation (exoskeletons, avatars).
- 1.2 Generative AI (GenAI) in particular is a rapidly evolving technology that can transform core higher education activities such as teaching and learning, individual productivity and operational efficiency. It can enable new modes of delivery, assessment and feedback, personalised, adaptive and collaborative learning, and data-driven decision making. It can also augment the capabilities of students, academic and Professional Services staff, and improve the quality and effectiveness of university processes and services.
- 1.3 AI also poses significant challenges and risks, such as ethical, legal, social, technical, and educational issues. The use of AI raises concerns about privacy, security, bias, accountability, transparency, sustainability, trust, governance and human dignity. AI can also have unintended or harmful consequences, such as displacing human roles, reducing human agency, creating digital divides, and exacerbating inequalities.
- 1.4 The purpose of this policy is to ensure the legal and ethical use of AI technology in all its guises so that it is used responsibly and beneficially at Bath Spa University.

2. Scope

- 2.1 This policy applies to, and must be adhered to, by all staff and other authorised University representatives processing data with the assistance of AI as defined in 1.1 on behalf of the University. The term 'staff' means anyone working in any context within the University at whatever level or grade and whether permanent, fixed term or temporary, including but not limited to employees, workers, and agency staff. The term "authorised University representatives" means other individuals given authorised access to Personal, sensitive or commercially sensitive data for the purposes of activities they perform for or on behalf of the University where and to the extent that this is specified in the terms of their authorisation, including but not limited to Governors, retired but active research staff, other visiting research or teaching staff, agents, volunteers, contracted service providers and external members of committees.

- 2.2 This policy also applies to students at the University when processing data with the assistance of AI on behalf of the University whether as part of research activities, group study, performance, experiments, fieldwork and case studies, and to students who are employed by the University. It does not apply to students when acting in a private or non-University capacity.
- 2.3 This policy is not part of any employee's contract of employment and should be read and complied with alongside other associated University policies and procedures.

3. Context for using AI

- 3.1 **AI** models can be used in stand-alone applications, such as ChatGPT or Bard, or incorporated into other applications such as internet search engines or word processing applications. Further information about AI can be found on the University's [SharePoint site](#).
- 3.2 **Privacy, Security and Confidentiality:** Information is shared with an AI tool, particularly GenAI tools, by user prompts, or a series of instructions or questions for the tool. Generally, providing access to information constitutes sharing data with the tool. The sharing of data potentially makes confidential or sensitive information public as the tool may train its model on the data shared. In some cases, data that has been pseudonymised can be linked to personal information and expose characteristics or behaviours about an individual. Any student or employee personal information, proprietary information or intellectual property, or otherwise commercially sensitive or confidential information entered or referenced as part of an AI prompt, may appear in other users' output. Therefore, users of this technology should avoid entering any information into a tool which they do not want to be made public or is otherwise restricted by law or policy.
- 3.3 **Governance:** The University uses a Data Protection Impact Assessment (DPIA) to help identify and mitigate risks when handling personal data. DPIAs are a legal requirement when high risk processing is planned, including when using AI. The DPIA must include an evaluation of the risks of using AI in a particular context, clearly identifying where AI processes and automated decisions may produce effects on individuals, the degree of any human involvement in the decision-making process and the stage at which this takes place.

The deployment of an AI system to process personal data must be driven by evidence that AI is a sensible and proportionate solution to an identified problem, identifying any risks to the rights and freedoms of individuals, as well as any detriment to individuals from potential bias or inaccuracy. It is also a requirement to assess whether individuals would reasonably expect AI to conduct the processing.

- 3.4 **Verification of Generative AI Output:** Outputs created by AI tools may provide fictitious answers, which are sometimes referred to as hallucinations.

Additionally, many open-source AI models are often trained on large, publicly available datasets (e.g., through data extraction of public webpages). The outputs may therefore contain copyrighted information, or others' intellectual property. While ownership in many of these cases is unclear, users should err on the side of caution and not use any output that contains material they suspect to be under copyright protection in any materials, internal or externally facing.

Users of AI tools must also be aware that they incorporate any biases of the data sets that were used to train them. This modeling bias may not always align with Bath Spa's core values of inclusivity and our commitment to diversity, equity and inclusion. Therefore, AI output may make systematic errors or favour certain groups, leading to unfair or discriminatory outcomes. Users of AI must adhere to existing review processes where AI is used to make decisions or provide analysis of information that may be subject to bias.

Using output from AI tools without reviewing it for accuracy places the University at risk and may harm Bath Spa's reputation with customers and employees.

- 3.5 **Transparency:** The University aims to provide our employees, third parties, and customers with transparency regarding how we use AI to support our work. All content generated using AI must be clearly identified on any outward-facing content.
- 3.6 **Third-party risk:** Data sent by Bath Spa University to third parties could be used in the third party's use of AI tools. Uses include training new AI models, providing updated information for existing AI models, and improving the user experience. Sensitive information input into unapproved AI applications may appear as output for individuals outside of the University. Not using AI in accordance with this policy may violate Bath Spa University's contractual obligations with customers or vendors or, in some cases, violate applicable law.
- 3.7 **Sustainability:** AI systems require vast quantities of processing power; as AI platforms continue to develop in terms of sophistication, this energy requirement will continue to increase, leading to huge demand from energy systems and water for cooling. Estimates suggest that a search driven by generative AI consumes four to five times the energy of a conventional web search. AI systems can also be used to help tackle climate change.

4. Policy Principles

- 4.1 The Policy is based on the following principles, aligned with the university's values and informed by best practice and standards in AI ethics and governance.

- We will provide our students/learners with the skills they need to make appropriate use of AI tools in their studies and thrive in an AI-enabled workplace.
- We will ensure staff have the skills to maximise the value of AI, to help reduce workload and support effective learning, teaching and administration.
- We will ensure academic integrity is maintained, whilst allowing students/learners to develop the skills they need.
- We will ensure the use of AI is lawful, safe, ethical and responsible.
- We will aim to ensure all learners have access to the AI tools that they need.

5. Policy Guidelines

The following guidelines must be adhered to in using Gen AI applications:

- 5.1 To maintain the **security of our data and IT systems**, you must not attempt to gain access to unapproved AI applications when using University systems or networks, conducting business on behalf of the University, or when using the University's data. To avoid potential data leaks or security incidents:

Do not use University credentials, email addresses, or telephone numbers as a login to unapproved versions of publicly available AI applications where no data protection arrangement exists.

Do not install non-approved Application Programming Interfaces (APIs), plugins, connectors, or software related to AI systems.

- 5.2 To maintain the **confidentiality of the University's sensitive information**, including but not limited to employee and customer personal information, our intellectual property and copyrighted material, you must only share information with approved personnel and only input sensitive information into approved AI systems. To maintain confidentiality:

Do not input, or provide as a reference, University intellectual property into non-approved generative AI applications.

Do not enter personal information of employees, customers, or other third parties into any non-approved AI application. Treat the application as you would an external contact with whom we have no formal relationship.

Do contact your manager, or email dataprotection@bathspa.ac.uk if you are unsure whether information you are planning to input falls into any of the above categories.

Do review the University's [Data Protection Policy](#)

- 5.3 To **maintain transparency** with customers and employees and protect the University from **claims against copyright infringement** and/or theft of

intellectual property, all AI-generated content must be cited and reviewed if used for work purposes. To protect the University:

Do clearly attribute any output used for work purposes to the AI application that created it through a footnote or other means visible to the reader.

Do maintain an updated record of AI use for work purposes and be able to share those records with your manager or other authorised University personnel upon request.

- 5.4 To protect our **employees and customers from harm, and to protect the University from reputational damage**, employees must use AI in alignment with Bath Spa University's [Equality Policy](#). AI-created content that is inappropriate, discriminatory or otherwise harmful to our employees or clients/customers must not be used for work purposes. Such use will result in disciplinary action. To protect our employees, customers, and the University:

Do review output of AI applications to make sure it meets the University's standards for principles of equality, ethics, and appropriateness.

Do not use any output that discriminates against individuals based on race, colour, religion, sex, national origin, age, disability, marital status, political affiliation or sexual orientation.

Do not use AI applications to create text, audio, or visual content for purposes of committing fraud or to misrepresent an individual's identity.

- 5.5 All employees and contractors are expected to comply with applicable laws, regulations, or company policies regarding the use or development of AI content or tools.

- 5.6 All employees are expected to report instances of non-compliance with this policy to the compliance team at dataprotection@bathspa.ac.uk. Employees are encouraged to speak up when they witness misconduct. Employees who report misconduct or concerns in good faith will not be retaliated against. For more information, see the [Whistleblowing Policy](#)

6. Acceptable Use

- 6.1 The adoption of specific AI tools by Bath Spa University will be considered on a use case basis to identify, assess and manage the risk factors and opportunities presented by that particular use case.

- 6.2 The use case is the specific application or scenario of AI in higher education, such as using AI for grading, tutoring, or scheduling. Alternatives to the use of AI will need to have been considered and evaluated before determining whether AI is the best solution.

- 6.3 The risk factors are the potential sources of harm or uncertainty associated with the use case, such as privacy, security, bias, or reliability; these are used to calculate a risk score. Depending on the associated risk factors, their likelihood and therefore their risk scores, some use cases for AI may not be appropriate for use at Bath Spa University.

7. Monitoring and Compliance

- 7.1 Bath Spa University reserves the right to access and monitor the use of AI applications on University-issued devices to ensure compliant use of these systems. Users who fail to comply with this Policy may be subject to disciplinary action. Any AI-related activities which appear to violate applicable laws will be reported to the relevant law enforcement agency.
- 7.2 In the event that monitoring systems detect a possible policy violation, or if a user reports a possible policy violation, the event should be processed using appropriate security incident response processes.

Document Details

Responsible Office: Governance, Legal and Compliance

Responsible Officer: University Secretary

Approving Authority: Senior Leadership Group

Date of latest approval: November 2024

Effective Date: November 2024

Related Policies and Procedures: [Data Protection Policy](#)

[Regulations for using computer facilities](#)

[BYOD Policy](#)

[Whistleblowing Policy](#)

[Equality Policy](#)

Supersedes: N/A

Next review due: November 2026