

Artificial Intelligence Use Policy

From May 2026

- [1. Policy Summary](#)
- [2. Scope](#)
 - [2.1. What does this policy cover?](#)
 - [2.2. What does this policy not cover?](#)
- [3. General Principles](#)
- [4. Use of AI by Staff](#)
- [5. Use of AI by Students](#)
- [6. Potential Misuse and Risks of AI](#)
- [7. Ethical Use of AI](#)
- [8. Data Protection and Privacy](#)
- [9. Cyber Security](#)
- [10. Responsibilities](#)
- [11. Reporting and Review](#)
- [12. Glossary of terms](#)
- [13. If you need support](#)
- [14. Linked and other policies and legislation](#)
- [15. Changes since previous policy](#)
- [16. Policies superseded by this document](#)

1. Policy Summary

- 1.1. Artificial Intelligence (AI) technology has already had a broad impact across many sectors and its adoption is increasing in all levels of education provision. Generative AI, which can create new content such as text, code, images, audio, video and 3D objects, is rapidly evolving and widely available. Informed by these capabilities, OCA recognises that AI technology offers numerous opportunities for enhancing and supporting teaching, learning, and administrative processes at OCA whilst also presenting risks and challenges in relation to academic integrity, ethical application, and socio-environmental impact.
- 1.2. Our strategic vision includes exploring the adoption of AI to enhance the college's teaching and learning practices. In embracing rather than restricting the use of AI, OCA aims to improve the student experience, enhance academic outcomes and support our staff in managing their workloads, and prepare staff and students for a future where AI will be integral. We are committed to remaining at the forefront of technology developments and adapting our working methods where appropriate or necessary, informed by best-practice guidelines and industry standards.
- 1.3. In recognition that the use of AI presents risks in addition to opportunities, this policy is designed to help mitigate these risks through clear guidelines and adherence to existing policies. The safeguarding and well-being of staff and students will be at the forefront of our policy and practice. We will educate staff and students about safe, responsible, and ethical AI use.

2. Scope

2.1. What does this policy cover?

- 2.1.1. This policy covers the college's approach to using AI by its staff and students.
- 2.1.2. This policy covers the college's approach to risk and vendor management in relation to the adoption of AI tools for use by the college and its stakeholders.
- 2.1.3. This policy covers when AI may and may not be used by its staff and students, and the outcomes of misuse.
- 2.1.4. This Policy applies to all students, staff, including temporary staff, consultants, trustees, contractors, and any other individual working or volunteering for OCA.

- 2.1.5. All users of AI at OCA are required to read and understand this policy.

2.2. What does this policy not cover?

- 2.2.1. This policy does not cover the specifics of how to use AI or how not to use AI.

3. General Principles

- 3.1. OCA's approach to AI is guided by the following principles, adapted from best practices in Further and Higher Education settings:
 - 3.1.1. **AI Literacy:** OCA will support students and staff to improve their level of AI-literacy through Information Literacy training within the [Student Handbook](#).
 - 3.1.2. **Preparing Staff:** Staff will be provided with training via the [Staff Intranet](#) to assist them in supporting students to use AI effectively whilst adhering to good ethical practices and standards.
 - 3.1.3. **Adapting Practice:** OCA will adapt its teaching, learning, and methods of assessment to incorporate the safe and ethical use of AI and ensure equal access.
 - 3.1.4. **Academic Integrity:** OCA will ensure its standards of academic integrity are maintained, both in the context of formative processes and summative assessment practices.
 - 3.1.5. **Responsible and Ethical Use:** We will promote responsible, safe, and ethical AI practices.
 - 3.1.6. **Compliance:** All users will follow applicable laws, regulations, policies, and guidelines, including those governing intellectual property, copyright, and data protection.
 - 3.1.7. **Safeguarding and Data Protection:** We will prioritise the safeguarding of our students and their online safety and privacy.

4. Use of AI Tools by Staff

- 4.1. Staff at OCA are permitted to explore and utilise college-approved AI-based tools and technologies to assist in managing their work and enhancing teaching and learning (see Appendix 1).
- 4.2. AI Tools, Models, Agents and associated technologies will be subjected to an Information Security Risk Assessment by the Information Security Group (ISG) prior to becoming a 'college-approved' tool for use by staff. Use of AI systems classified as 'High-Risk' under the *EU AI Act* or equivalent UK legislation requires a separate, rigorous approval

process beyond this policy. Examples of activities which may be deemed high risk in relation to the OCA include but are not limited to:

- 4.2.1. **Academic:** Admissions screening; Exam proctoring/cheat detection; Automated grading; Capability assessments.
- 4.2.2. **Operations:** Recruitment and selection (CV-parsing/applicant filtering); Employee performance evaluations.
- 4.3. As per the college's Information Security Risk Management Policy, a Risk Owner will be associated with any risk relating to AI tools and their use. The Head of Technology and Innovation will in all cases act as the Senior Information Risk Owner (SIRO) for AI tools.
- 4.4. **Permissible Uses:** Examples of tasks where AI may provide valuable support include:
 - 4.4.1. Collation of educational content and resources,
 - 4.4.2. Production of Teaching Schedules, Learning Plans or Learning Activities.
 - 4.4.3. Rewording feedback for students, supporting feedback / report writing, professional development, and administrative tasks.
 - 4.4.4. Supporting students' individual needs through rewording of content or provision of content in alternative formats.
- 4.5. **Prohibited Uses:** Activities classified as 'Unacceptable Risk' under the EU AI Act may be considered illegal and must not be carried out under any circumstances. Specifically, the following must not be engaged with at OCA:
 - 4.5.1. **Emotional Recognition:** Use of real-time facial recognition or vocal signatures to infer emotional responses, e.g. identifying lack of focus during video calls, or identifying false statements being made during interviews.
 - 4.5.2. **Exploitation of Vulnerable Individuals:** AI that exploits specific groups based on their age, disability, or socio-economic circumstances to distort their behavior and cause harm, e.g. targeting ads based on disabilities or socio-economic status.
 - 4.5.3. **Biometric Categorisation of Sensitive Traits:** Use of biometric and behavioural data to infer an individual's Protected Characteristics, such as race, political opinions, trade union membership, religious beliefs, or sexual orientation.
 - 4.5.4. **Predictive Policing Based on Profiling:** Predicting the likelihood of an individual breaking policy or law, based on personality or background rather than relevant evidence. E.g. use of HR tools that flag an individual as a risk using their socio-economic background as the basis rather than hard evidence.

- 4.6. **Professional Judgment:** AI tools should be used responsibly, ensuring they complement staff members' judgment, creativity, capabilities and skills, rather than replacing them. All staff remain accountable for any content generated with AI assistance.
- 4.7. **Accuracy and Review:** Staff must review and verify AI-generated content for accuracy, especially when evaluating subjective responses or using it for student support. Fact-checking is an essential step when using AI-generated content.
- 4.8. **Transparency:** Where staff use AI in their working practices, they should declare the context and purpose of that use, in addition to what accuracy checks and reviews have been carried out as part of a due diligence process. Documents or communications influenced by AI should include citations and references indicating AI assistance.
- 4.9. **Explanation & Justification:** Staff must not use AI for decision-making purposes unless they can *explain and justify* the outcome without solely relying on the AI. Where AI technologies have been used as part of the decision making process, affected individuals may exercise the right to request from the decision maker an explanation and/or human review of the decision. This must be made clear as part of the communication of any decision which was made with the assistance of AI tools.
- 4.10. **Training and Support:** Staff will receive general AI-use training and support, enabling them to make effective and safe use of AI in their work. Staff should identify any specific training needs with their Line Manager as part of the PDR process.
- 4.11. **Approved Tools:** Staff should only use AI technologies approved by OCA and use college-provided accounts for work purposes where available. See Appendix 1 for the list of OCA Approved AI tools.
- 4.12. **Responsible Data Handling:** All staff have a duty to use AI tools responsibly, taking care to protect data and avoiding where possible the input of sensitive information into third-party tools unless first vetted by IT Services. A DPIA must be completed prior to any new processing of personal data, as per the college's [Data Protection Policy](#). The addition of AI use to any system or process is highly likely to require a DPIA to be completed.

5. Use of AI by Students

- 5.1. **Enhancing Learning:** Students are permitted to use AI for knowledge acquisition, creative expression, research, textual analysis, accessibility support and requesting feedback on their work on the condition that such use is declared and appropriately referenced.

- 5.1.1. AI tools may be incorporated into tasks, exercises and assignments or may be encouraged as part of research tasks and creative processes where the use is relevant to declared outcomes and proportionate to the task.
- 5.2. **AI Literacy Education:** AI education will be incorporated into programmes and course units where relevant and appropriate to provide students with an understanding of AI's abilities, limitations, direction of travel, and ethical implications. The college will provide training and guidance on information literacy, inclusive of the identification and verification of AI-generated misinformation (fake news.) Students will be engaged in discourse around data privacy, safeguarding, model biases, and the socio-environmental impact of AI.
- 5.3. **Responsible Use and Academic Integrity:** Students are provided with training on ethical and responsible AI use. Awareness of risks inherent in reliance on AI tools will be communicated. OCA staff will emphasise the importance of original, critical and creative thinking in the creation of student work, whilst discouraging misuse of AI as tools of plagiarism, academic malpractice or dishonesty. Students should be clear and transparent about where their work has been created with the assistance of AI. While AI may assist in the creative process, the assessment of student work, particularly in a portfolio context, focuses on evaluating the student's understanding, critical thinking, and creative journey.
- 5.4. **Avoiding Misuse:** Students are provided with training within the Student Handbook both on the potential benefits and what constitutes misuse of AI, including those seeking to deceive or trick them (e.g., deepfake and impersonation materials). Any staff suspecting a student of misusing AI should refer to the [Academic Misconduct Policy](#).
- 5.5. **Data Privacy for Students:** Students should not enter any personal, sensitive, copyrighted or confidential data into AI prompts, as some generative AI models may not be private or data-secure.

6. Potential Misuse and Risks of AI

OCA is aware of potential misuses and risks associated with AI and will implement measures to mitigate them.

- 6.1. **Academic Misconduct and Plagiarism:** Using AI tools to complete projects, tasks and assignments without appropriate transparency or attribution constitutes academic misconduct. Students must understand guidelines on the appropriate use of AI during assessment and ensure their work reflects their own efforts, even if it is informed by interaction with AI models as part of the creative process. AI can present

information created by others as being unique, leading to plagiarism or copyright infringement, including in artwork.

- 6.2. **Bias and Discrimination:** AI outputs can reflect inherent biases in the data they were trained on, potentially leading to unethical or discriminatory content based on protected characteristics (age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation) and factors such as socioeconomic background or profession. OCA will take steps to highlight and/or address issues if they arise through college-approved AI tools (see Appendix 1).
- 6.3. **Inaccuracy and Misinformation:** AI-generated information may be inaccurate, fictitious, poorly referenced, or out-of-date. Both staff and students must fact-check and critically evaluate AI outputs. AI can be used to create or spread harmful or misleading content.
- 6.4. **Harmful Content:** AI may expose students to harmful or unsuitable content. Mitigation includes the pre-testing and vetting of AI tools as part of Vendor Management processes, provision of reporting mechanisms, monitoring, and human oversight.
- 6.5. **Emotional Manipulation and Mental Health Impacts:** AI tools could negatively affect student mental health through biased or harmful content, or overuse of AI tools could cause stress, anxiety, or dependency. Through training and guidance materials, the college will raise awareness of these potential risks.
- 6.6. **Data Protection and Privacy Breaches:** As noted in Sections 4 and 8, entering personal or sensitive data into AI tools poses significant risks and should be avoided.
- 6.7. **Cyber Security Threats:** AI can be involved in cyber-crime, including generating deepfakes or facilitating impersonation and fraud. Staff and students must be aware of these risks and the form they may take.
- 6.8. **Digital Divide:** All students will have equal access to college-approved AI tools to ensure equitable access to their potential benefits (see Appendix 1 for the list of OCA Approved AI tools).
- 6.9. **Ethics and Environmental Impact Awareness:** The college is committed to monitoring and, wherever possible, reducing its impact on the environment. Training will be provided on these aspects of AI use to improve awareness.
- 6.10. **Assessment models:** OCA is aware that the potential for AI misuse by students poses challenges in regards to the development of Assessment models and techniques which can withstand the potential for AI use to jeopardise the rigour and fairness of Summative Assessment.

- 6.10.1. Regular risk assessments must be conducted, as part of curriculum reviews and following each assessment event, to assess the vulnerability of Summative Assessment models and techniques to AI-related malpractice.
- 6.10.2. In addressing any vulnerability of Summative Assessment models and techniques, it must be ensured that no student groups are unfairly disadvantaged through the implementation of restrictions, e.g. restricting accessibility of submission procedures.
- 6.10.3. In recognition of the low success rate of AI detection software, addressing the vulnerability of Assessment models and techniques to malpractice through the use of AI must not solely rely on such autonomous methods of malpractice detection.

7. Ethical Use of AI

The use of AI systems, particularly Generative AI by staff and students, must be carried out with caution and an awareness of the AI systems ' limitations and any ethical considerations.

- 7.1. Users should be mindful of, and students should be instructed about, potential bias, ensuring generated data does not discriminate (also see 7.1.6).
- 7.2. Users must check the accuracy and currency of AI-generated information.
- 7.3. Users should be aware that AI tools may not follow ethical codes, or their adherence to any ethical code of conduct may not be verifiable.
- 7.4. AI tools should not be used in ways that could lead to exploitation, such as that potentially involved in the development of some AI models through human training.
- 7.5. Human oversight is essential; AI should assist human decision-making, not replace it, especially for decisions affecting individuals.
- 7.6. AI systems should align with principles of equity, diversity, inclusivity and fairness in education (see 7.1).
- 7.7. Transparency about AI use is essential - acknowledge and cite any use of AI in work produced.
- 7.8. The environmental impact of AI models (especially those involved with the generation of media) must be considered prior to engaging with those models.
- 7.9. In relation to 7.8, it is the policy of OCA that AI-generated visual or audio media should not be used in marketing materials, unless the use meets a specific and well-defined purpose.

8. Data Protection and Privacy

Protecting personal and sensitive data is paramount when using AI tools.

- 8.1. **Data Privacy Risk:** Staff and students must be aware that any information entered into a Generative AI model may no longer be private or secure.
- 8.2. **Prohibited Data:** Staff and students must not enter any personal information (personal data), intellectual property, or private/commercially sensitive information into any Generative AI model unless explicitly approved for that use by OCA.
- 8.3. **Compliance:** Staff must ensure any AI tools comply with UK GDPR and other data protection regulations, as per the requirements of OCA's [Data Protection Policy](#).
- 8.4. **Data Protection Impact Assessments (DPIAs):**
 - 8.4.1. Potential new uses of AI tools will require assessment to determine if a DPIA is needed, following OCA's Data Protection Policy and Procedures.
 - 8.4.2. A DPIA must consider the lawful basis for processing data with AI, including the fairness and proportionality of processing, potential harms (including bias), accuracy, security threats, and necessary safeguards.
 - 8.4.3. Processing involving vulnerable data subjects, such as children or individuals with protected characteristics is likely to be considered high risk and will trigger a DPIA.
- 8.5. **Training Data:** Care must be taken to avoid intellectual property, including students' work, being used to train Generative AI models without appropriate consent or exemption.
- 8.6. **Transparency:** Staff should inform students about the data collection, storage, and usage practices associated with AI technologies.

9. Cyber Security

- 9.1. **Security Protocols:** Rigorous cybersecurity protocols, access controls, encryption, security patches, and secure storage will be implemented.
- 9.2. **Incident Reporting:** Suspected or confirmed security incidents involving AI must be reported promptly through [OCA's IT Helpdesk](#).
- 9.3. **Tool Evaluation:** The security of any AI tool must be evaluated in terms of its security and privacy before use as part of existing Vendor Management processes, which make up part of OCA's [Information Security Management System](#). Ethical considerations around model

training and environmental sustainability must also be considered as part of any evaluation process.

- 9.4. **Awareness:** Staff and students will be provided with training trained to promote awareness of the importance of Cyber- and Information Security when using AI tools and the associated risks, e.g. through advanced phishing and spear-phishing techniques of impersonation to extract personal and sensitive data.

10. Responsibilities

All OCA stakeholders have responsibilities regarding the use of AI.

- 10.1. **Trustees:** Provide oversight on the college's responsible use and promotion of the use of AI.
- 10.2. **Senior Leadership / Directors:** Responsible for strategic planning, policy establishment, and ensuring staff receive training and understand the policy.
- 10.3. **Relevant Leads (e.g., Head of Quality and Academic Support, Head of Student Services, Head of Technology and Innovation, Data Protection Officer etc.):** Act as leads for AI use, monitor compliance, communicate policy, provide training or technical support, advise on data protection obligations, and handle security incidents.
- 10.4. **Staff:** Responsible for adhering to this policy and using AI responsibly within guidelines, reporting incidents, challenging inappropriate behaviour, ensuring sensitive data is secure, and educating students on safe/ethical AI use.
- 10.5. **Students:** Responsible for understanding their responsibilities, using AI appropriately, transparently declaring its use in their work, reporting concerns, and adhering to relevant Policies and Standards.

11. Reporting and Review

- 11.1. **Reporting Incidents:** Reporting systems are available for staff, students, and parents/carers to report concerns or incidents involving AI misuse, data breaches, or inappropriate outputs. All reports will be handled appropriately.
- 11.2. **Policy Review:** This policy will be reviewed regularly, at least annually, or whenever new AI technologies or significant developments arise. Policies and guidance will be evaluated for effectiveness, fairness, and ethical implications.

12. AI Use Declaration

- 12.1. The *Google Gemini 2.5 Deep Research* AI tool was used to research and gather relevant material for the production of this policy.

- 12.2. The *Google NotebookLM* AI tool was used to cross-reference this policy against existing policies to identify areas of potential conflict or omission.

13. Glossary of terms

- 13.1. **Artificial Intelligence (AI):** Technology that can support and improve teaching, learning, and administrative tasks.
- 13.2. **Generative AI:** A type of AI that can produce content such as text, images, audio, or video.
- 13.3. **AI Literacy:** Having the knowledge to understand how AI works, what it can and can't do, and the ethical issues it raises.
- 13.4. **Academic Integrity:** Maintaining honesty in your academic work. Using AI tools without proper acknowledgment is considered dishonest.
- 13.5. **Deepfake:** Fake images, videos, or audio created by AI to mislead or impersonate people.
- 13.6. **Data Protection Impact Assessments (DPIAs):** Reviews carried out before using AI in new ways, to check for privacy and data protection risks.
- 13.7. **UK GDPR:** The UK's rules for protecting personal data, based on the General Data Protection Regulation.
- 13.8. **Intellectual Property:** Original ideas or creations. You should not submit them to AI tools unless you have permission.
- 13.9. **Copyright:** A legal right that protects creators' work. Using AI can accidentally break these rules.
- 13.10. **Bias (in AI):** When AI results are unfair or unbalanced because of the data it was trained on.
- 13.11. **Misinformation:** False or misleading information that can be produced by AI tools (sometimes referred to as 'hallucinations').
- 13.12. **Cyber Security:** Keeping systems and data safe from digital threats, including those involving AI.
- 13.13. **Digital Divide:** Unequal access to AI technologies and tools, which can lead to disadvantages for some people.

14. If you need support

- 14.1. Technical support: techsupport@oca.ac.uk
- 14.2. Support in relation to this Policy: paulvincent@oca.ac.uk
- 14.3. Support in relation to referencing and citation of AI sources: library@oca.ac.uk

15. Linked and other policies and legislation

- 15.1. [Academic misconduct Policy](#)

- 15.2. [Data Protection Policy](#)
- 15.3. [Information Security Policy](#)

16. Changes since previous policy

- 16.1. This is the first version of this Policy Document.

17. Policies superseded by this document

- 17.1. This is the first version of this Policy Document.

Appendix 1: OCA Approved AI tools

Compliance Indicator	Google (Vertex AI / Workspace Gemini)	OpenAI (API / Enterprise)	Anthropic (API / Enterprise)	Mistral AI (La Plateforme)
No-Training Commitment	Yes, explicit in Business and Cloud Terms	Yes, explicit in Business (API) Terms	Yes, explicit in Commercial Terms	Yes, explicit in Paid Tiers
Zero Data Retention (ZDR)	Yes, via configuration and request (done)	Yes, by request for eligible endpoints *requested, awaiting response from baa@openai.com	Yes, via separate agreement *requested	Yes, by request for legitimate reasons
Default API Data Retention	Up to 24-hour cache; up to 55 days for abuse logs (exempted by request)	Up to 30 days for abuse monitoring	Up to 30 days for API calls	30 days for abuse monitoring

DPA Integration	Manual opt-in required via Admin Console (done)	Separate DPA form to be executed	Automatically incorporated in Commercial ToS	Automatically incorporated in ToS
Intl. Transfer Mechanism	DPF & SCCs in CDPA	SCCs in DPA; DPF status to be verified	SCCs in DPA	UK-EEA Adequacy & SCCs for sub-processors
Key Security Certifications	SOC 2 Type 2, ISO 27001 series	SOC 2 Type 2	SOC 2 Type 2	ISO 27701, SOC 2 Type 2
Legal Doc. Clarity	Fragmented; requires navigation of multiple portals	Clear structure but multiple documents	High clarity; unified commercial terms	High clarity; GDPR-native structure
Overall UK GDPR Readiness	High (with high administrative burden)	High	Very High	Very High
Suitable for General Staff/Student Use (outside of APIs)	Yes	No	No*	No*

* Pending Retention and Use Limitation Agreements.