

Acceptable Use Policy for Artificial Intelligence (AI)

Positional Statement

At GOsC we embrace innovation and the use of AI to inform our work. All AI-generated content undergoes human review to ensure accuracy, quality and accountability.

Use of AI within the General Osteopathic Council (GOsC)

When you are using these tools for work-related activities, we want to support you in using these tools safely and in a manner that does not compromise the organisation or its reputation.

AI can be defined in many different ways but is essentially a software-based system that is designed to perform tasks that typically require human intelligence, such as learning, reasoning and decision making.

We have committed in our strategic plan to embracing innovation and want to embrace any opportunities that AI has to offer and ensure that we are able to use it to improve what we do. At the same time, we need to ensure that when using AI, we carefully balance the opportunities against the potential risks that may arise.

1. Policy Objectives

The purpose of this policy is to outline the acceptable use by employees of AI systems within the General Osteopathic Council (GOsC). It aims to ensure AI is used in line with our organisational values as well as responsibly, ethically and in compliance with legal, regulatory and societal expectations.

This policy aims to:

- Promote transparency, fairness, and accountability in AI use.
 - Ensure AI is only used in accordance with this Policy.
 - Safeguard data privacy, public trust, and institutional integrity.
 - Ensure compliance with organisational values and expectations around behaviour and conduct in the workplace as well as legal and ethical obligations.
-



2. Scope of AI Use

This policy applies to anyone working for us. This includes employees and contractors.

GOsC has decided to use Microsoft 365 Copilot (M365 Copilot) as its approved AI system because, as with other large AI providers like Open AI and Google, Microsoft faces higher regulatory scrutiny and has the following in place:

1. Stronger security and compliance controls: they invest heavily in security compliance and data protection. They have robust infrastructure, encryption and access controls that smaller AI models may lack.
2. Clear data handling policies: Reputable AI providers have well defined policies for data protection, data retention, data encryption and processing.
3. Predictable and audited AI behaviour: They have transparency reports, ethical guidelines and accountability mechanisms. Their models are tested for biases, adversarial vulnerabilities and security risks and they have the resources in place to support these essential functions.

You are therefore asked to use M365 Copilot as this is covered by [Enterprise Data Protection](#) and all data that is inputted remains within our own secure system.

If you wish to use any other AI system in your work please discuss with your Line Manager and seek agreement **before** using.

If you are using another type of AI technology approved by your Manager, the same policy applies. This includes (but is not exhaustive):

- Other types of generative AI (e.g. text, image, audio generation) in addition to Microsoft Co-pilot
- Case management and workflow automation systems
- Document analysis and information extraction tools
- Predictive analytics tools
- Natural language processing tools

3. Acceptable Use

Individuals using AI technologies are responsible for their actions and must use AI in a responsible and ethical manner.



It is important to only ask AI to produce something that you could do anyway as then you will be confident that you can quality assure the output. The types of things you could use AI for are:

- brainstorming ideas.
- basic research.
- developing a project plan.
- critically analysing a piece of work.
- redrafting text to fit different audiences; and/or
- proofreading.

Principles of Acceptable Use:

- Only use approved AI systems for tasks relating to your work that support the GOsC's values, existing policies and objectives as a regulator.
- Be open about when AI is used in your work. Discuss with your Line Manager and the Communications Team if using AI-generated content in public communications or reports.

Where appropriate add the following statement as a footnote on documents and /or emails :

'All content has been reviewed by humans, and GOsC takes full responsibility for its accuracy and quality.'

- Ensure you have been sufficiently trained to use the AI system competently and are aware of the potential risks that it poses.
- Always check the accuracy of AI outputs before using them in your work. Involve others in the checking process if you are unsure.
- Report any concerns about AI system outputs (e.g. incorrect or biased results) to your Line Manager.

4. Where AI Should Not be Used :

- In any manner that undermines public confidence or impartiality in our statutory functions.
- In any work related to Fitness to Practise.
- To make decisions.
- In ways that introduces or could potentially amplify bias, discrimination, or unfair treatment.
- To generate misleading, discriminatory, or harmful content.
- For any activity that does not support the GOsC's values, its existing policies and objectives.



- To attempt to circumvent established data protection, cybersecurity, or ethical review processes.
- To undertake any task where you do not have sufficient experience and expertise to ensure accuracy, quality, and accountability.
- To carry out any part of a grievance and/or disciplinary procedure (for example to decide a grievance outcome or appropriate disciplinary penalty).
- To carry out any task that requires you to input the organisation's confidential information and/or personal employee data (for example for financial forecasting).

What is acceptable and what is prohibited will depend on your job and the nature of the task that you are engaged in. If you are unsure about using AI for a task that you are undertaking, you should speak to your Line Manager for further advice.

5. Common Risks and other points for consideration

Bias & Fairness	AI models may reflect or amplify societal biases, leading to unfair outcomes.
Privacy & Data Protection	Inputting personal data into AI systems can violate data protection laws. Use anonymised data and comply with GDPR or relevant laws.
Misinformation	Generative AI may produce information that sounds plausible but is factually inaccurate or misleading.
Security Vulnerabilities	AI systems may be exploited if not properly secured or monitored.
Loss of Accountability	Overreliance on AI can obscure responsibility for decisions.
Environmental impact	Use of AI systems can involve a large amount of energy consumption. Employees should be mindful of this when deciding to use any AI system in their work.

6. Governance & Oversight

- All AI systems must be approved by SMT under guidance from the IT Manager.
 - Regular reviews and audits will be conducted to assess performance, fairness, and risk.
 - All employees must complete mandatory training on ethical AI use and data protection if using AI systems.
-

7. Reporting & Enforcement

- You must speak with your Line Manager if you have any concerns about AI outputs or notice any misuse of AI systems. They will work with you to help address the issue, including liaising with SMT.
- Where misuse occurs, this may need to be addressed in line with GOsC's Disciplinary Policy and Procedure.
- Employees of GOsC have a responsibility to protect and maintain confidentiality of GOsC's information and the personal data that is held as part of its statutory duties. Any data breaches should be reported in line with the Employee Handbook.
- Whistleblower protections apply to those reporting misuse in good faith.

Data protection

You are strictly prohibited from sharing any personal data and special categories of personal data with any AI **outside of the organisation i.e. with AI that has not been approved for GOsC use and does not have the appropriate controls in place. If in any doubt speak to your Line Manager.**

Personal data is any information that relates to a living individual who can be identified from that information.

Special categories of personal data means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

Any personal data and special categories of personal data, must be handled in accordance with our data protection policy / policy on processing special categories of personal data.



General
Osteopathic
Council

Breach of policy

Employees are encouraged to use AI in supporting their work. They are reminded to refer to this policy and, if in any doubt, to their Line Manager to support data security and organisational and personal credibility. Such actions will avoid a breach which may be addressed in line with GOsC's Disciplinary Policy and Procedure.

Further guidance

If you need further guidance or support on this policy, you can contact The IT Manager or Governance Manager.

8. Policy Changes and Review

This policy will be reviewed on a 3 monthly basis and in response to significant changes in law, technology, operational risk or internal processes.

As these tools continue to advance and develop, we will carry on assessing and navigating the risks associated with using them to ensure that our policy remains current and effective. If there are any changes to this policy, we will notify you accordingly.

The policy does not form part of your contract of employment and we reserve the right to amend it at any time.

Date of Policy Review	Changes Made	Version Control	New Review Date
15 Jan 2026	New Policy	V1	15 April 2026