

Artificial Intelligence (AI) Policy

Contents

1. Definitions of AI.....	1
2. Statements.....	1
3. Risks (Reputational)	2
3.1 AI and plagiarism.....	2
3.2. AI and environmental impact.....	2
3.3. AI and social responsibility.....	2
4. Risks (Data Protection).....	2
5. Responsible use – what is appropriate	2
6. Security and monitoring.....	3

Purpose

The purpose of this policy is to ensure that staff, Trustees, volunteers, and anyone else working on the Society's behalf are clear about the principles of AI use and to ensure that the Society has guidelines and procedures in place which are consistently followed.

As AI is a rapidly developing field, this policy is subject to change and should be monitored regularly.

1. Definitions of AI

Artificial intelligence (AI) refers to the theory and development of computer systems capable of performing tasks that normally require human intelligence.

Generative AI (sometimes called Gen AI) is artificial intelligence that can create original content – such as text, images, video, audio, or software code – in response to a user's prompt or request.

A (Large) Language model (LLM) is a model trained on textual data. The most common use case of a LM is text generation. The term “LLM” is used to designate multi-billion parameter LMs, but this is a moving definition.

This policy focuses primarily on the use of generative AI systems such as ChatGPT, Claude, Copilot, and Gemini. Many other generative AI tools are available, and the number continues to grow as more software companies integrate AI into their platforms.

Note: Microsoft CoPilot is encrypted and operates under Microsoft privacy commitments. The Society is currently exploring the use of CoPilot licenses for non-generative tasks (such as spreadsheet automation).

2. Statements

- Staff must not upload any personal data to unencrypted AI systems.
- AI must not be used to generate content for the Society; including but not limited to text, image, and audio/visual content.
- Generative AI can and does provide incorrect information and should never be relied upon without manually verifying the information given.

- Staff, trustees, and volunteers must be transparent in their use of AI tools and defer to the Data Protection Officer's guidance.

3. Risks (Reputational)

The following elements of AI constitute a reputational risk to the Society and should be closely monitored:

- Plagiarism
- Dissemination of fabricated or incorrect information
- Environmental impact
- Social responsibility

3.1 AI and plagiarism

The use of generative AI includes but is not limited to; image creation from text prompts, sound/music creation, code generation, and text and content creation. While generative AI can be a useful tool, it has a problematic history of facilitating plagiarism and fabricating content (known as 'AI hallucinations').

LLMs scrape data from the web without verifying sources or obtaining consent from authors. Using generative AI for content creation risks engaging in plagiarism and disseminating incorrect information. This is a severe reputational risk for the Society. As a learned authority on Egypt and the Sudan, we cannot be seen to validate fabricated or generally incorrect information.

Generative AI should never be used to create text content for the Society, and any research done using AI must be manually verified before it is included in Society outputs.

3.2. AI and environmental impact

The use of AI is associated with significant environmental impact. AI data centres require massive amounts of water and electricity and contribute to air and noise pollution. The Society is committed to reducing our energy consumption and carbon footprint in a practical and cost-effective manner.

3.3. AI and social responsibility

The Society should not be seen to be using generative AI instead of paying for work from, for example, typesetters and graphic designers.

4. Risks (Data Protection)

Unencrypted LLMs scrape the web for data and regurgitate information given to it by other users. Therefore, sensitive information, especially member and donor records, should never be fed into an LLM. While there is currently no UK legislation that directly refers to the use of AI, where an AI system is using or collecting personal data, it will fall within the scope of the UKGDPR and Data Protection Act 2018 (DPA).

Staff, trustees, and volunteers should always comply with the Society's Data Protection Policy and contact the Data Protection Officer for queries.

5. Responsible use – what is appropriate

While AI should never be used to generate content, AI tools may be used to edit and check work, manage personal diaries, and perform basic automated tasks, with the permission of the Data Protection Officer.

Examples include:

- Using an AI system such as Reclaim or Notion to manage calendars and personal diaries.
- Using spellcheck software such as Grammarly to edit existing work.
- Using Microsoft CoPilot (with an appropriate encrypted user license) on spreadsheets.
- Editing or 'touching up' photos.
- Handwritten text recognition or language translation (which should then be verified).

6. Security and monitoring

This policy will be reviewed regularly and updated as necessary to reflect the rapid development of the AI field.

Document Revision Record

Date issued	Version no.	Summary of changes	Drafted by	Approved by
July 2026	First version		Adelaide Robinsmith	Board of Trustees, 11 th September 2026