Artificial Intelligence Usage Policy

Version 1.1

1. Introduction

1.1. Artificial Intelligence (AI) is a new and emerging area of technology. AI tools are transforming the way we work. NILGOSC recognises the potential AI has to automate tasks, create efficiency, improve decision-making, and provide valuable insights into business operations.

1.2. NILGOSC seek to encourage a pro innovation approach to the use of AI in the organisation.

1.3. However, the use of AI tools also presents new challenges in terms of information security, data protection and misinformation. NILGOSC is committed to protecting the confidentiality, integrity, and availability of the data we hold.

1.4. This policy requires that AI tools be used in a manner consistent with these values.

1.5. The policy sets out NILGOSC's position in terms of AI usage and also acts as a guide for employees on how to be safe and secure when using AI tools, particularly in relation to the sharing of potentially sensitive information.

1.6. The policy has been developed in accordance with the Artificial Intelligence Playbook for the UK Government and the 10 principles contained therein.

1.7. The Artificial Intelligence Usage Policy applies to:

- All NILGOSC Staff
- All NILGOSC Committee Members
- The staff and agents of other organisations who directly or indirectly have been given permission to access NILGOSC IT Systems or information assets, including AI tools or platforms, or who provide information to NILGOSC.

1.8. This policy should be read in conjunction with the following NILGOSC Policies and Procedures:

- IT Information Security Policy
- Software Policy
- Data Protection Policy & Procedures.

2. Policy Updates

2.1. This policy is managed by the Head of Information Technology (IT).

2.2. The policy will be revised from time to time in response to changing circumstances. AI is a rapidly emerging and changing technology. Changes will be made as new technologies develop, and in response to operational and legislative requirements, with a full review occurring at least every three years.

3. Background

3.1. There are two main types of AI: extractive AI and generative AI. Extractive AI extracts data from a given dataset (e.g. a search engine which provides an answer to a specific question by extracting the relevant section of a web article), generative AI generates new outputs based on a given dataset (i.e. it creates new content, unlike extractive AI)

3.2. This policy relates primarily to the use of Generative AI. Generative AI Systems include Large Language Models (LLM), Image Generation applications, Neural networks etc.

3.3. Several Generative AI models exist, including ChatGPT, Google Gemini, DALL-E and others. The policy applies equally to all Generative AI applications.

3.4. NILGOSC's IT Team are constantly looking at ways to improve IT efficiency and security, and the usage of AI forms part of this. When exploring the roll out of an AI service, the IT team will seek to utilise existing platforms where data privacy and licencing terms are well understood and under regular review.

3.5. The use of any new AI service within NILGOSC is permitted only with the express pre-approval of the Head of IT, where the request has been made in accordance with Section 5.

4. Approved AI Use Model

4.1. NILGOSC operates a controlled model for the use of Artificial Intelligence, designed to ensure that usage is secure, proportionate, and aligned with organisational, legal and regulatory requirements.

4.2. The use of AI within NILGOSC is restricted to approved platforms and services, as determined by the IT team. These will typically include enterprise-grade tools where data handling, security, and contractual terms have been reviewed and are subject to ongoing assurance.

4.3. The use of AI is limited to internal business activities only. AI tools must not be used to provide information or responses directly to members of the public, scheme members, or external stakeholders without appropriate human review and approval.

4.4. AI tools are intended to support staff in the performance of their duties and may be used for activities such as:

- Drafting internal documents and communications;
- Summarising information;
- Analysing data or identifying trends;
- Assisting with locating and retrieving information within authorised systems

4.5. AI services must operate within existing NILGOSC identity, access control, and information governance frameworks. AI must not be used to access, infer, or expose information that a user is not already authorised to view.

4.6. All outputs generated by AI systems must be treated as advisory only. Responsibility for the accuracy, appropriateness, and use of any output remains with the user.

5. Requesting Approval to use AI

5.1. Requests for access to or use of AI services must be made in accordance with the Software Policy and IT Service Desk procedures.

5.2. Staff should raise a request on the IT Service Desk by completing the web form located under User Services > Software Request or my emailing help.me@nilgosc.org.uk, where a request will be created for you.

5.3. The request should include details of the AI application you wish to use and it's intended business purpose. When requesting approval be mindful that the use of AI to enter,

upload or share any data that is confidential, proprietary, or protected by regulation is explicitly prohibited.

6. Approval Process

6.1. Requests made to the IT Service Desk will be reviewed by the Head of IT.

6.2. Approval will be based on:

- Alignment with the Approved AI Use Model;
- Use of an approved or approvable platform;
- Compliance with security, data protection, and governance requirements.

6.3. A decision will be communicated to the requester via the Service Desk request. If a request is rejected, reasons for doing so will be recorded. All Service Desk requests are retained.

6.4. If a request is approved, a member of the IT team will assist in signing up for the application or service.

7. Security

7.1. If the use of an AI web application or service is approved under the software policy, a NILGOSC email account must be used to sign up. The account must conform to all security considerations listed in the IT Information Security Policy, including password complexity.

7.2. AI services must operate within NILGOSC's existing identity and access management controls. Users must only access information they are already authorised to view.

7.3. AI services must not be used to bypass, extend, or infer access to restricted or sensitive information.

7.4. Where integration with internal systems is enabled (e.g. through connectors or agents), such integrations must:

- Be approved and configured by the IT team;
- Operate on a least-privilege basis;

- Be read-only by default;
- Reflect underlying system permissions at all times.

7.5. AI services are subject to the requirements of the Software Policy, including licensing, supplier assurance, and approval controls.

7.6. The IT Team will ensure that any AI service is configured in line with generally accepted best practice and in compliance with both NILGOSC IT procedures and in line with UK Government guidance on the implementation of AI.

8. Data Protection

8.1. The use of any AI service must be compliant with UK GDPR and the Data Protection Act 2018 (DPA 2018).

8.2. AI services operate by processing data in response to user prompts. Users must be mindful that information entered into AI tools should be limited to what is necessary for the task.

8.3. Staff should be mindful at all times of the data they enter into an AI model. Users must avoid including personal or sensitive data in prompts unless it is necessary, proportionate, and within the scope of their authorised access and duties.

8.4. Where AI services are provided under enterprise agreements, NILGOSC data will not be used for model training. Users must not assume this applies to unapproved tools, where data entered may be used to train AI models in accordance with the developers privacy policy

8.5. If an option is available on the platform to disable data sharing for AI learning, this should be selected.

8.6. Users must not rely on AI outputs as complete or authoritative. Outputs must be reviewed and validated prior to use, particularly where they may influence internal decision-making or documentation. Users should be aware at all times that the information generated by AI, particularly LLM, is not guaranteed to be free from errors, omissions or factual inaccuracies. AI systems can have bias embedded into them which can manifest in various ways.

8.7. The ownership of output including text and images generated by AI must also be considered. Generative AI tools can output written, visual, aural, or audio-visual works that can mimic the style of specific human creators if their works are present in the datasets. This raises implications for intellectual property rights, regardless of whether companies are transparent with datasets or not. Users should be aware of this and seek advice from Governance or Legal where doubt exists and where appropriate.

8.8. Encryption and secure transmission using TLS and Data at Rest Encryption (D@RE) should be employed whenever available.

9. User Responsibilities

9.1. Users must ensure that their use of AI aligns with the Approved AI Use Model and all relevant NILGOSC policies.

9.2. AI-generated content must be treated as advisory only, and users remain fully responsible for verifying its accuracy, completeness, and appropriateness.

9.3. AI must not be used to make, support, or automate decisions affecting members or staff without appropriate review and application of existing decision-making processes.

9.4. Where AI is used to assist in producing internal documentation, users must ensure that outputs meet NILGOSC standards for accuracy, clarity, and governance.

9.5. NILGOSC will take reasonable steps to ensure that staff are provided with appropriate guidance, awareness, and training in relation to the responsible use of Artificial Intelligence.

9.6. Training may include a combination of general awareness material and more targeted guidance for users of approved AI services.

9.7. Users are expected to:

- Familiarise themselves with any training or guidance provided;
- Apply the requirements of this policy when using AI tools;
- Seek advice from the IT department where they are unsure about appropriate use.

9.8. The level and form of training provided will be proportionate to the nature of AI use within NILGOSC and will be reviewed as adoption evolves.

10. Change Management

10.1. AI services and their use within NILGOSC will be kept under periodic review to ensure they remain aligned with organisational, security, and data protection requirements.

10.2. Where there are material changes to an AI service or its use are expected to be identified through ongoing monitoring, management and operational oversight. This might include:

- Significant changes to supplier terms or data handling practices;
- Introduction of new functionality or features that change how the service is used;
- Integration with additional data sources or systems;
- Expansion of use into new business areas.

10.3. Changes should not be progressed where they would:

- Significantly alter how personal data is used or accessed;
- Introduce new or unmanaged risks to information security or confidentiality;
- Enable automated decision-making or external-facing use without appropriate oversight.

10.4. The use of AI within NILGOSC may be expanded over time. Any such expansion must remain consistent with the Approved AI Use Model and is subject to appropriate review and authorisation prior to implementation.

10.5. The IT Team are responsible for the configuration, testing, deployment, and ongoing management of any NILGOSC developed or configured AI capabilities, including custom agents and integrations.

11. Auditing

11.1. The IT team will maintain a register of approved AI services available within NILGOSC and the use to which these services are put.

11.2. The IT team reserves the right to restrict, suspend, or withdraw access to any AI service where continued use presents a risk to security or compliance.

11.3. Approved AI services and their configuration will be subject to periodic review to ensure continued compliance with organisational, legal, and security requirements.

11.4. The Senior Information Risk Owner (SIRO) will receive a quarterly summary of any AI applications or services approved and in use and will consider these specifically against any information governance and data protection implications.

12. Prohibited Use of AI

12.1. The following activities are strictly prohibited:

- Use of unapproved AI tools or services for NILGOSC business;
- Uploading or sharing NILGOSC data with public or consumer AI platforms
- Using AI to make automated decisions that produce legal or similarly significant effects;
- Using AI to generate communications issued directly to members, the public, or external stakeholders without review and approval;
- Circumventing established information security, access control, or data protection requirements.

13. Use of AI by Members and Suppliers

13.1. Staff should be aware that members may be using AI to provide them with advice used as a basis for queries to NILGOSC. Members may therefore be misinformed and also have compromised the security of their data by using an AI tool.

13.2. NILGOSC staff who are contract managers should consider the services provided by the respective supplier. If the service makes use of NILGOSC data the contract manager should ensure this policy is applied. If the supplier provides information to NILGOSC used for decision making, the supplier must disclose if AI has been used in the generation of that information.

14. Review

14.1. Published: 01/05/2024

14.2. Last Review Date: 01/06/2026

14.3. Next Review Due: 01/06/2029

15. Compliance and Acknowledgement

15.1. All staff are required to comply with the requirements outlined in this policy. AI tools must be used in a manner consistent with the guidance set out above, and any security or data protection incidents or concerns must be reported to the Head of IT and Head of Governance and HR.

15.2. Use of NILGOSC IT systems and AI services constitutes acceptance of, and agreement to adhere to, the provisions of this policy.