THE NATIONAL ARCHIVES

Artificial Intelligence Policy

IT Security & Assurance / IT Operations

Contents

1 Introduction 3
2 Purpose 3
3 Scope 4
4 Policy 5
4.1 General 5
4.3 Responsibility 9
4.4 Transparency 10
4.5 Responsible Use of Artificial Intelligence – Employment Impact 10
4.6 Responsible Use of Artificial Intelligence – Environmental and Sustainability 11
5 Risks 11
6 Contact 12
7 Review 12

Date	Version	Description
14/10/25	1.3	Current version post August review
30/06/25(ready for August review)	1.2	New draft being compiled with feedback from Policy Review Group and other general updates.
23/01/25	1.1	Post December 2024 review and agreement by AI Steering Group
28/06/24	0.2	Initial published version

Policy owner: Cyber Security Team
Next review by: June 2026 (or sooner if UK government policy or legislation is implemented or updated prior to this date)

1 Introduction

1.1 The broad term 'Artificial Intelligence' (AI) is used in this policy to describe various computer systems that can perform tasks previously requiring human-like intelligence. This includes Natural Language Programming, Machine Learning and Generative AI.

1.2 'Generative AI' is used to describe any type of artificial intelligence that can create new content, including text, images, video, audio, or code. Large Language Models (LLMs) are part of this category of AI and produce text outputs. The abilities of Generative AI have captured the public imagination and create potential applications within The National Archives (TNA).

1.3 AI has the potential to unlock significant productivity benefits. This document aims to help people at The National Archives understand AI, to guide anyone building AI solutions, and, most importantly, to lay out what must be taken into account to use AI safely and responsibly. It is based on a set of ten principles which should be considered in all AI projects.

1.4 Significant risks exist with the use of AI, such as bias, incorrect information, discrimination, data privacy violations. The use of AI tools in an organisation such as ours presents new challenges for our information security and data management and protection responsibilities.

2 Purpose

2.1 The purpose of this policy is to establish guidelines and best practices for the responsible use of artificial intelligence within our organisation. AI technologies have the potential to transform our business processes, enhance decision-making, and improve efficiency. However, it is essential to ensure that AI is used ethically, responsibly, transparently, and in compliance with legal and regulatory requirements.

2.2 This policy builds upon government guidance, Generative AI Framework for HMG, published 18 January 2024, and Artificial Intelligence Playbook for the UK Government, published February 2025 for the use of AI in the public sector and the National AI Strategy by the Office for AI, but adds additional controls specific to the nature of the work carried out by The National Archives. The framework has Generative AI as its focus, but TNA's policy expects staff to

apply the same principles to any use that falls within the broader definition of Artificial Intelligence. *Note: UK Government Policies, Guidance and playbooks etc. are constantly changing and being updated so it is best to refer to the UK Government AI web sites for current guidance and policies.*

2.3 We recognise that development and deployment of AI at The National Archives is at an early stage and there is activity underway to develop strategies, plans and governance.

3 Scope

3.1 This policy applies to all people using Artificial Intelligence at The National Archives. Its scope covers the use of AI tools and services for all work tasks (in any location or any platform), but also private tasks if undertaken using laptops or other equipment or logins provided by TNA. The scope also includes the potential use of any data that has been created with the help of AI.

3.2 AI tools may be used at The National Archives in accordance with this policy. Three main types of tool are anticipated:

- Ad-hoc use of AI tools and services by individuals or teams, including
  - AI tools embedded into IT applications, e.g. Microsoft Co-Pilot and it's integration with other Microsoft products.
- Tools/services/products developed by TNA, or it's sub-contractors or partners, with AI components or use of AI tools or services.
- Other general use AI services, modules or components to either existing TNA systems or new systems. This could include for example chatbots built into CRM type systems, AI functionality being developed and made available in Workday etc.

3.3 TNA's default assumption is that AI tools are insecure. Unless specifically advised otherwise, **personal data, sensitive data and bulk data must not be used with any AI tool unless an approved tool for this purpose.** Any data that is input into an AI tool must be anonymised and sanitised, for example to avoid references to individual or to TNA/The National Archives.

4 Policy

General

4.1.1 TNA will follow government policy and guidance on the use of AI.

4.1.2 All users of AI tools should be aware of and follow, where appropriate, the ten common principles in the government Generative AI Framework for HMG for safe, responsible and effective use of generative AI in government organisations. The white paper A pro-innovation approach to AI regulation, sets out five principles to guide and inform AI development in all sectors. This framework builds on those principles to create ten core principles for generative AI use in government and public sector organisations:

- **Principle 1**: You know what AI is and what its limitations are
- **Principle 2**: You use AI lawfully, ethically and responsibly
- **Principle 3**: You know how to use AI securely
- **Principle 4**: You have meaningful human control at the right stages
- **Principle 5**: You understand how to manage the full AI lifecycle
- **Principle 6**: You use the right tool for the job
- **Principle 7**: You are open and collaborative
- **Principle 8**: You work with commercial colleagues from the start
- **Principle 9**: You have the skills and expertise needed to implement and use AI
- **Principle 10**: You use these principles alongside your organisation's policies and have the right assurance in place

Note: **Principle 4** includes ensuring that all AI-assisted processes, TNA commit to upholding the primacy of human judgment and ensuring full transparency and openness with our colleagues and trade unions.

The latest UK Government guidelines, principles, standards and legislation must also be used and referenced, especially as the field of AI is moving quickly and standards and guidelines are being updated often. It is planned that the UK will introduce its first AI-specific legislation in 2025. The latest UK Government papers on AI that should be referred to when dealing with AI includes:

- AI Cyber Security Code of Practice: This voluntary code advocates a ***secure-by-design*** approach to AI cyber security. It aims to build resilience into AI systems throughout their lifecycle to prevent data loss and breaches[1]
- Software Security Code of Practice This code ensures that organizations selling software prioritize security and resilience in their product design. It helps businesses manage risks throughout their supply chains[2]

4.1.3 Where available, corporately provided and approved tools must be used. If this is not possible and a login is required, staff must authenticate ideally via Single Sign On and / or Multi-Factor Authentication. If this is not possible using their TNA email address together with a unique password that follows our password policy.

4.1.4 Outputs from an AI tool must not be used without reviewing it first and must contain a reference to the output has been generated, in part or in full, via AI with the source of the AI used and the date. This is a requirement under Article 22 UK GDPR, i.e. "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."
— Article 22(1), UK GDPR

4.1.5 TNA must lodge the use of AI with the UK Government "**Algorithmic Transparency Recording Standard Hub"** which is mandated by UK Government. See https://www.gov.uk/government/collections/algorithmic-transparency-recording-standard-hub

4.1.5.1. This site has a template that needs to be completed and details on how to submit.

4.1.5.2. It is proposed that all lodgings are highlighted to the AI Steering Group

1.1 _____

1.2

[1] Cyber security codes of practice - GOV.UK
[2] A Code of Practice for Software Vendors: call for views - GOV.UK

4.1.6 Use of AI Transcription Tools in Meetings

4.1.6.1. Ensuring the security of our virtual meetings is a collective responsibility; here's an essential guide to help us all navigate the use of third-party transcription tools in meetings

4.1.6.2. The Government Security Group has identified security risks linked to the proliferation of third-party AI tools capable of transcribing virtual meetings which may result in the unintended disclosure or compromise of HMG information.[3]

4.1.6.3. Recent cyber-attacks on government showcase the need to defend against a broad range of threat actors who would profit off a transcript of a meeting discussing sensitive HMG information. Alongside improving our cyber resilience, from a personnel security and insider risk perspective it is critical for HMG employees to mitigate the risks of (un)intentional third-party unauthorised access to government information, systems, assets, and infrastructure.

4.1.6.4. **Key points**

- Departments should ensure the 'lobby' or 'waiting room' settings are enabled in HMG video conferencing providers (e.g. MS Teams, Google Meets) to prevent certain types of participants from joining a call by default until the meeting chair admits them.
- HMG employees chairing virtual meetings should verify the identity of all participants on the call and remove participants that have not been successfully identified.
- Meeting chairs may wish to positively confirm whether or not AI transcription tools offered natively by government video conferencing providers are allowed to be used - and confirm participants are content prior to any transcription feature being enabled. *TNA Note: Within TNA the only supported AI transcription is the built in MS Teams Transcription which is secure and any / all content is kept within the TNA Microsoft tenant.*
    - Meeting chairs positively confirm third party AI enabled transcribing software is **not allowed**. If there remain concerns undisclosed third-party

1.1 _____

1.2

[3] See 2024-06-25 -GSG-SRN 079 - AI Transcription Services.pdf

AI transcription tools are in operation, it is recommended to terminate the meeting and report it to the Departmental security team.

When using transcription in Microsoft teams within The National Archives Microsoft tenant:

- The recordings remain within our secure environment.
- You can safely record the meeting using our Microsoft Teams' built-in recording feature if any content in the meeting is not classified as Sensitive. If any Sensitive content is to be used or discussed, then transcription services should NOT be used (and the normal protocol on ensuring sufficient levels of security clearance of all attendees)
- Using Microsoft 365 Copilot when signed into your TNA Microsoft account: It's integrated into our system and is not considered an external third-party application. It respects our internal security protocols, ensuring that our data and communications remain protected.
- All recordings are subject to FOI and Subject Access requests and therefore any recording must be stored / saved in a relevant secure TNA storage area that supports the relevant protections and data retention policies.
- If any TNA member of staff is uncomfortable with the meeting being recorded then the meeting should not be recorded or that person should leave the meeting.

When external parties are involved:

- If an external participant joins a TNA hosted meeting or if we're invited to an externally hosted meeting, be cautious.
- If a third party hosted meeting, then before the meeting, ask if any third-party AI transcription tools will be used.
- If a third-party tool is proposed, clarify it is <u>not</u> to be used during the call.
- If you're unsure about the security of a third-party tool, it's best to avoid using it and stick to Microsoft Teams' native features.

4.2 At The National Archives, the security of our meetings hinges on the integrity of the service, proper configuration, and the security of the devices used by participants. We can only be assured of meeting our security standards when all attendees are TNA staff or when external participants belong to entities with equivalent security measures and governance. It's vital that we all contribute to maintaining this security posture during virtual meetings.

4.2.1 Use of AI built into software and upgrades / updates

To help mitigate the risk of existing software introducing AI features and functionality then any/all updates, patches and upgrades which involve the use of AI must also go through the aforementioned approval process.

A significant example of this is TNA's Workday product where there is requirement to ensure AI is NOT used for any form of HR processes or processing without due consideration and consultation with the Unions.

Responsibility

4.2.2 All TNA staff are expected to adhere to security best practices when using AI systems. This includes the following:

- **Evaluation of AI tools and Services:** TNA's Cyber Security team in conjunction with the Data Protection team will evaluate the security of any AI tool before proposing to the AI Steering Group its use and seek the permission from their department Information Asset Owner.
- **Protection of confidential data:** TNA users must not upload or share any data that is confidential, proprietary, or protected by regulation.
- **Access control:** TNA users must use their TNA credentials, ideally via Single Sign on and / or Multi Factor Authentication (MFA) for any work-related AI use and must not share login credentials, use any generic login or share other sensitive information with un-approved third parties.
- **Use of reputable AI tools:** Only accredited AI tools will be considered for use in the TNA and staff must not use AI tools or services developed by individuals or companies without TNA Cyber Security team and AI Steering Committee's approval.
    - **Compliance with security policies:** Staff must apply the same security best practices we use for all company and customer data.
    - **Compliance with wider legal framework as appropriate ;** for example Employment law or Business law may need to be considered.
- **Data privacy:** Even when approval for a tool has been given staff must exercise discretion when sharing information publicly.

- **Risks:** All users should be aware of the risks, benefits and general characteristics of AI tools before using them. All users of these tools must use them safely and ethically.

4.2.3 Governance for AI follows the principles of the TNA Cloud Services Policy:

4.2.4 Information Asset Owners (IAOs) are responsible for ensuring AI tools are used safely within their department IAOs should record their department's use of AI tools, for example in IAO reporting.

Transparency

4.2.5 All users must be open and honest in their use of AI systems, the purposes they are used for and how they are applied, particularly where AI has contributed to their work. Any outputs produced using AI must be clearly marked.

4.2.6 IAOs are responsible for publishing under the Algorithmic Recording Transparency Standard

Responsible Use of Artificial Intelligence – Employment Impact

4.2.7 The organisation is committed to the ethical and responsible use of Artificial Intelligence (AI) technologies. In deploying AI systems, we will actively consider their potential impact on employment and livelihoods, particularly in roles traditionally performed by human professionals.

4.2.8 Where AI is used to generate creative outputs—such as images, videos, or written content—that may previously have been produced by skilled professionals (e.g., photographers, designers, writers), we will:

4.2.8.1.1. Assess the impact on existing roles and employment opportunities.
4.2.8.1.2. Engage with affected stakeholders, including employees, contractors, and industry representatives, to understand the implications.
4.2.8.1.3. Prioritise human-centred approaches where feasible, including hybrid models that combine AI tools with human expertise.
4.2.8.1.4. Provide transparency about when and how AI-generated content is used.
4.2.8.1.5. Explore opportunities for reskilling and redeployment of affected individuals, supporting a just transition to new roles enabled by AI.

4.2.9 This clause aligns with our broader commitment to fairness, transparency, and social responsibility in the adoption of emerging technologies.

Responsible Use of Artificial Intelligence – Environmental and Sustainability

4.2.10 The organisation is committed to the ethical and responsible use of Artificial Intelligence (AI) technologies. In deploying AI systems, we will actively consider their potential impact on employment and livelihoods, particularly in roles traditionally performed by human professionals.

4.2.11 Where AI is used to generate creative outputs—such as images, videos, or written content—that may previously have been produced by skilled professionals (e.g., photographers, designers, writers), we will:

4.2.11.1. Assess the impact on existing roles and employment opportunities.
4.2.11.2. Engage with affected stakeholders, including employees, contractors, and industry representatives, to understand the implications.
4.2.11.3. Prioritise human-centred approaches where feasible, including hybrid models that combine AI tools with human expertise.
4.2.11.4. Provide transparency about when and how AI-generated content is used.
4.2.11.5. Explore opportunities for reskilling and redeployment of affected individuals, supporting a just transition to new roles enabled by AI.

4.2.12 This clause aligns with our broader commitment to fairness, transparency, and social responsibility in the adoption of emerging technologies.

5 Risks

5.1 AI systems we develop must be safe and secure. They must be designed to prevent harm to individuals and organisations.

5.2 All users should be aware of the risks and problems in using AI tools and in the responses they give.

5.3 Risks from inputting data:

5.3.1 An AI tool may use any prompt or input in its own learning and repeat it to any other user of that tool. As such, any data given to an AI tool must not be sensitive and be suitable for public access.

5.4 Risks of AI outputs:

5.4.1 AI outputs may be wrong or misleading, fictitious, biased or in an improper style (e.g. US English).

5.4.2 AI outputs may be out of date or imply that past activities are current.

5.4.3 AI outputs may present facts out of context in a misleading way.

5.4.4 Sensitive data could emerge unexpectedly in AI output.

6 Contact

6.1 Users or IAOs with any doubts about an AI tool should contact the IT Security team via the IT Service Desk.

6.2 All incidents or suspected incidents related to AI must be reported as soon as possible following IT security reporting procedures:

7 Review

This policy will be reviewed and updated on a regular basis to ensure that it remains current and effective.

Appendix I – List of reference sites / links

Incubator for Artificial Intelligence - GOV.UK

Using AI for digital selection in government - The National Archives