Artificial Intelligence Policy

V1.3

10 Sep 2026

Document Title	**Artificial Intelligence Policy**		
Issue Status	V1.3	**Issue Date**	12/12/2023
Author	Daniel Glennie	**Title**	Security Manager
Tel:		**E-Mail**	Daniel.glennie@improvementservice.org.uk
Security Classification	OFFICIAL	**Retention Period**	Per policy
Review Period	Annual	**Last Reviewed**	**10/09/2026**

Version No	Date	Summary of changes
0.1 DRAFT	11/12/2023	Initial release for comment
0.2 DRAFT	12/12/2023	Revised to align with ISO 27001
0..9 DRAFT	14/12/2023	Revised after initial release
1.0	15/12/2023	Approved by ISMS Board
1.1	15/12/2024	Annual review
1.2	16/09/2025	Updated to reflect changes (Copilot)
1.3	10/09/2026	Updates on licensed vs unlicensed Copilot use

Review

Name	Organisation

Daniel Glennie	Improvement Service		
ISMS Board	Improvement Service		

Authorisation

Document Approvals

Document Authorisation	Title/Organisation	Signature	Date
ISMS Board			tbc

Introduction

As we continue to embrace technological advancements, the use of Artificial Intelligence (AI) tools in the workplace has become increasingly prevalent. This policy provides clear guidelines on the responsible and secure use of AI tools, ensuring productivity and innovation while safeguarding sensitive information and compliance with applicable standards and legislation.

The policy's primary goal is to protect the Improvement Service's information assets from external and internal threats, whether deliberate or accidental, and to ensure compliance with ISO 27001:2022, GDPR, and UK Government security requirements.

Aim

This policy aims to:

- Prevent unwanted sharing of sensitive information.
- Encourage consistent, professional, and ethical use of AI tools.
- Ensure that staff are clear about their responsibilities when using AI.
- Protect the organisation from reputational, financial, and legal risks.
- Protect the organisation from legal liability and the inappropriate use of AI tools.
- Ensure compliance with information security and data protection standards.

Scope

This AI Policy applies to:

- All employees, contractors, third parties, and agents of the Improvement Service.
- All devices (organisation-owned or personal) used for conducting all IS work.
- All AI-related activities, whether for official use or general productivity.

Terms and Definitions

Term	Definition
Sensitive Information	Any data that could compromise security, privacy, or compliance if disclosed. Examples include: personally identifiable information (PII), financial data, system configurations, intellectual property, council data, confidential business information, audit findings, employee records, health information, government data, contractual details, and any data classified as "Restricted" or "Confidential" under the Information Security Policy.
Generative AI	AI models that create text, images, or other content, such as Microsoft Copilot, OpenAI ChatGPT, Google Gemini, Perplexity, or similar.
Asset	Anything that has value to the organisation
Control	Means of managing risk, including policies, procedures, guidelines, practices
Guideline	A description that clarifies what should be done and how
Information Security	Preservation of confidentiality, integrity and availability of information
Incident	An event that affects the confidentiality, integrity or availability of information
Policy	Overall intention and direction as formally expressed by management
Risk	Combination of the probability of an event and its consequence
Third Party	Person or body that is recognised as being independent

Risks

The use of Artificial Intelligence (AI) tools presents several risks that, if unmanaged, could compromise the confidentiality, integrity, and availability of information assets within the Improvement Service. A primary concern is the **potential loss or leakage of sensitive information**. When sensitive data such as personally identifiable information (PII), council data, financial information, or system configurations are entered into unauthorised AI tools, it may be stored, reused, or exposed in ways that fall outside the organisation's control. This could lead to data breaches, identity theft, or reputational harm to the organisation.

Another significant risk is the **inaccuracy and unreliability of AI generated content**. AI models are prone to producing flawed, biased, or misleading information. If staff rely on such outputs without adequate verification, it could result in poor decision-making, the spread of misinformation, or operational inefficiencies. In critical scenarios, this could even lead to financial loss, compliance violations, or damage to the organisation's credibility.

The organisation is also exposed to **legal and regulatory risks**. Misuse of AI tools may lead to breaches of laws such as the UK GDPR, the Data Protection Act 2018, or contractual confidentiality obligations. Failure to comply with international standards such as ISO 27001:2022 or sector specific regulations could result in penalties, loss of certification, and diminished trust among stakeholders and partner councils.

There are further risks related to **insufficient staff education, lack of awareness, or inadequate training**. Data and information may be put at risk when employees misuse AI tools, fail to recognise security warnings, or breach established controls. Poor understanding of acceptable use guidelines increases the likelihood of accidental disclosure, data mishandling, or unauthorised sharing of sensitive information.

Additionally, **data collected, analysed, stored, communicated, and reported upon by the organisation may be subject to theft, misuse, loss, or even exploitation for AI training purposes** by third-party providers. Many commercial AI platforms reserve the right to use user input as training data unless explicitly disabled, which poses a direct threat to confidentiality and intellectual property rights if sensitive information is entered into unapproved systems.

There are also risks associated with the **over-reliance on AI systems without human oversight**. Excessive dependence on AI tools may reduce critical thinking and professional judgement among staff. This over-reliance could cause employees to overlook errors or fail to challenge inappropriate outputs, thereby undermining accountability and organisational resilience.

Finally, the use of AI can introduce **emerging cybersecurity risks**. Some AI tools may operate from third-party environments with unknown or insufficient security practices, increasing exposure to threats such as data harvesting, unauthorised access, or malicious manipulation of AI models (e.g., prompt injection or data poisoning attacks). These risks highlight the importance of adopting a controlled, risk-based approach to AI tool usage, supported by regular risk assessments, staff training, and the application of security controls that are proportionate to the threat landscape.

Acceptable Use of AI

Employees are encouraged to leverage AI tools to enhance productivity, creativity, and problem-solving in their daily tasks. However, use must be consistent with this policy, with particular care taken not to expose sensitive or confidential information in unauthorised platforms. Staff are expected to exercise professional judgement at all times, considering the appropriateness of the tool for the task at hand.

The following rules apply:

1. **Microsoft Copilot – Official Use** ○ Microsoft Copilot is the only approved AI tool for use with **sensitive information** (e.g. personal data, council information, financial details, employee records, security configurations, audit findings, or any information classified as Confidential or Restricted under the Information Classification Policy).
    - Copilot must only be used in its organisation-managed and secured environment (e.g., Microsoft 365). This means **you may only use Copilot for sensitive purposes if you have a Copilot licence.** Unlicensed use of Copilot is not secure as it does not stay within our 365 tenant.
    - Only Copilot is acceptable for use in minuting meetings as these often include sensitive information.
    - Copilot agents developed by providers other than Microsoft (i.e. 3rd party agents) are **not suitable** for use with sensitive information

2. **Other AI Tools – General Purposes Only** ○ Other reputable AI tools such as ChatGPT, Google Gemini, Anthropic Claude, Perplexity AI, or 3rd party agents within Copilot may be used for **non-sensitive tasks only**, such as:
    - Drafting general emails or communications.
    - Producing articles, blogs, or summaries that do not contain confidential data.
    - Brainstorming ideas, creating outlines, or gathering general knowledge.
    - ○ These tools **must not** be used for inputting or processing any sensitive information, including meeting minutes.
3. **Sensitive Information Prohibition** ○ Employees must never input data that includes personal identifiers, confidential council information, financial data, intellectual property, audit results, system configurations, or contractual/legal details into unauthorised AI platforms. ○ Staff must also avoid entering meeting minutes, strategic project details, or system vulnerabilities, as these may be stored or used to train third-party AI models without the organisation's consent.
4. **Verification and Oversight**
    a. AI-generated outputs should never be accepted as fact without review. Employees are required to check all outputs for accuracy, bias, and compliance with organisational standards.
    b. Staff must apply the same level of proofreading, quality control, and accountability as they would when drafting their own work.

5. **Escalation of Doubts**

a. If an employee is uncertain about the appropriateness, security, or compliance of using a particular AI tool or entering specific data, they must consult the **IT Security Team or the Security Manager** before proceeding. This ensures risks are identified and mitigated before any potential exposure occurs. By adhering to these principles, staff can benefit from AI-enabled efficiency while ensuring that the organisation remains compliant with information security standards, legal requirements, and data protection obligations.

Video Calls

The use of AI tools for video calls (e.g. MS Teams meetings/calls), other than Copilot, is prohibited due to data privacy concerns. Video calls often involve the sharing of visual and auditory information that may compromise the privacy of individuals and sensitive business discussions. AI assistants are increasingly popular for tasks such as minuting, but the risks to information security are too broad to justify this.

Email Drafting

AI tools for email drafting are generally acceptable, provided they do not compromise the confidentiality of sensitive information. Employees should use AI assistance responsibly and be aware of the content they generate, ensuring it aligns with company policies and values

Consultation with IT Security Team

If an employee is uncertain about the appropriateness, security, or compliance of using a particular AI tool or entering specific data, they must consult the **IT Security Team or the Security Manager** before proceeding. This ensures risks are identified and mitigated before any potential exposure occurs. The IT security team is here to provide guidance, assess potential risks, and ensure the protection of company data

Privacy and Compliance

All employees must adhere to data privacy regulations and comply with company policies when using AI tools. Avoid using AI tools that may compromise the confidentiality, integrity, or availability of sensitive information.

Training and Awareness

Employees will be provided with training and resources to enhance their understanding of AI tools, including their benefits, risks, and proper usage

Reporting Security Incidents

In the event of any security incidents or concerns related to the use of AI tools, employees are required to promptly report them to the IT security team. Timely reporting is crucial to address and mitigate potential risks.

Authority

Staff, contractors, consultants, visitors and guests who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary action, contract termination, or legal consequences.

Review

The Security Manager will monitor the effectiveness of this policy and carry out regular reviews of all reported breaches.

This policy will be reviewed annually.