



*served by One Team*

South & East Lincolnshire Councils Partnership

# Information Security Policy Artificial Intelligence

May 2024

# 1. Document Control

## Version Control

Issue Number	Issue Author	Issue Date	Reason for Issue
1.0	J Wright/C Gooch		Draft and release of new policy
1.1	C Gooch	22-04-2024	PFH Feedback and Review

## Approval Control

Issue Number	Approval Authority	Names	Approval Date	Due for Review
1.0	ELDC/BBC/SHDC	James Gilbert	May 24	May 2025
1.1	SLT	Senior Leadership Team	May 24	May 2025

## Policy Governance

<b>Responsible</b>	Business Intelligence and Change Manager
<b>Accountable</b>	Assistant Director Corporate (ELDC/BBC/SHDC)
<b>Consulted</b>	Data Protection Officers, Head of ICT and Digital, ICT Security Lead, Members Working Groups, PFHs
<b>Informed</b>	Employees/Members

## Contents

1. Document Control .....	2
Version Control.....	2
Approval Control.....	2
Policy Governance .....	2
2. Policy Overview .....	4
Policy Aim .....	4
Introduction .....	4
Policy Commitment.....	5
Responsibilities .....	5
3. Scope .....	5
Governance.....	6
Vendors.....	6
Copyright.....	7
Accuracy .....	7
Confidentiality.....	8
Ethical Use .....	8
Disclosure .....	8
Security .....	9
Integration with other tools.....	9
4. Risks.....	9
Legal compliance .....	9
Bias and discrimination.....	10
Security .....	10
Data sovereignty and protection .....	10
5. Compliance.....	10
Record keeping for Compliance.....	10
6. Review.....	11
7. Policy Compliance .....	11
8. Related Policies .....	11
9. Glossary of Acronyms.....	11

## 2. Policy Overview

### Policy Aim

2.1 The aim of this Policy is to define the broad mechanisms and roles through which the Organisation will be able to demonstrate accountability and compliance with regards to the use of Artificial Intelligence – Artificial Intelligence (AI) is defined as the science of making machines that can think like humans. It can do things that are considered "smart." AI technology can process large amounts of data in ways, unlike humans. The goal for AI is to be able to do things such as recognise patterns, make decisions, and judge like humans.

### Introduction

2.2 This is a joint Artificial Intelligence Policy. Where “The Organisation” is referenced, this refers to either Public Sector Partnership Services or its Client Councils: South Holland District Council, East Lindsey District Council, or Boston Borough Council.

2.3 The purpose of this policy document is to provide a framework for the use of Generative Artificial Intelligence Large Language Models (GenAI) such as ChatGPT, CoPilot, Bard, Bing, or other similar tools by council employees, contractors, developers, vendors, temporary staff, consultants, or other third parties, hereinafter referred to as ‘users’.

- This policy is designed to ensure that the use of AI is ethical, complies with all applicable laws, regulations, and council policies, and complements the council’s existing information and security policies.
- The pace of development and application of AI is such that this policy will be in a constant state of development.

2.4 This policy applies to Councillors, employees, contractors, consultants, temporaries, and other workers at the Organisation, including all personnel affiliated with third parties.

### Cost and Efficiency Benefits

2.5 The implementation of AI tools offers significant cost and efficiency benefits, enhancing productivity and operational effectiveness across the Organisation:

- **Increased Productivity:** AI tools can automate routine tasks, allowing staff to focus on more complex and value-added activities. This leads to improved efficiency and faster turnaround times for various processes.
- **Cost Savings:** By reducing the time and resources required for manual tasks, AI tools help lower operational costs. This includes savings on training, as AI can provide real-time assistance and guidance, reducing the need for extensive training programs.
- **Consistency and Accuracy:** AI ensures that outputs are consistent and accurate, minimising errors and the need for rework. This is particularly beneficial in areas such as data entry, report generation, and customer service.
- **Enhanced Decision-Making:** With advanced data analysis capabilities, AI can provide insights and recommendations that support better decision-making. This leads to more informed and effective strategies and policies.

- **Scalability:** AI tools can easily scale to meet the demands of the Organisation, handling increased workloads without a proportional increase in costs or resources.

By leveraging these benefits, the Organisation can achieve greater efficiency, reduce costs, and enhance the overall quality of services provided to the community.

## Policy Commitment

2.5 Artificial Intelligence has become an umbrella term for the use of Machine Learning (ML), Robotics (RPA), Large Language Models (LLM), Intelligent Automation (IA) and Artificial Intelligence (AI). This policy underpins the use of any such technology.

2.6 The rise of Artificial Intelligence has the ability to transform the way we work, with the ability to automate tasks, improve decision making and provide valuable insights into our operations. However, the use of AI presents new challenges. It raises technical and ethical questions on its use and brings to the forefront again the subject of data and information sharing.

2.7 This policy is to ensure all colleagues use AI in a secure, responsible, and confidential manner.

## Responsibilities

Role	Responsibility
The Organisation's Chief Executive	Supporting Company/Authority compliance with the policy
Senior Management Team / SIRO (Senior Information Risk Owner)	Ensuring the policy adheres to statutory legislation & guidance and that it is embedded in the workforce and ensuring managers and Team Leaders show compliance with the policy and it is understood.
Procurement Team	Ensuring that due diligence to policy alignment is made as point of procuring a solution
Managers & Team Leaders	Understanding and complying with the policy, ensuring it is available to team members, and advising on it. Ensuring Information Asset Registers are updated as necessary
All Staff/Members	Understanding and complying with the policy.

## 3. Scope

3.1 This policy applies to all users with access to Artificial Intelligence (AI) or any associated technology discussed in the previous section, whether through council-owned devices or BYOD (bring your own device) in pursuit of required activities.

3.2 Use of AI must be in a manner that promotes fairness and avoids bias to prevent discrimination and promote equal treatment and be in such a way as to contribute positively to the organisation's goals and values.

3.3 Users may use AI for work-related purposes subject to adherence to the following policy. This includes tasks such as generating text or content for reports, emails, presentations, images, and customer service communications.

3.4 Particular attention should be given to Governance, Vendor practices, Copyright, Accuracy, Confidentiality, Disclosure, and Integration with other tools.

## Governance

3.5 To ensure data protection by design, before accessing AI technology, users must first request advice and guidance from the Organisation's ICT and Data Protection teams.

3.5.1 The ICT and Data protection teams will review the tools security features, terms of service and privacy policy. This information will allow the SIRO to make a balanced risk-based decision on whether to adopt a solution.

3.5.2 The requestor should have clear documentation detailing their intention to use, the reason for use, and the expected information to be input as well as the generated output and distribution of content.

3.5.3 The use of AI is likely to require a DPIA (Data Protection Impact Assessment) to be completed. Please refer to the relevant Data Protection Officer.

## Ownership and Vendor Accountability

3.6 Any use of AI technology in pursuit of the Organisation's activities should be done with full acknowledgement of the policies, practices, terms, and conditions of developers/vendors.

3.6.1 Ownership of AI Technology: To ensure transparency and accountability, it is crucial to establish and clarify the ownership of any AI technology used by the Organisation. This includes identifying the companies that supply AI systems to the Council and understanding their ownership structures and motives. The Organisations Information Governance Team will maintain a register of all AI vendors, detailing their ownership and any relevant affiliations. This register will be reviewed and updated regularly to ensure it reflects the most current information.

3.6.2 Vendor Assessment: Before procuring or implementing any AI technology, the Organisation will conduct a thorough assessment of the vendor. This assessment will include:

- Ownership Verification: Confirming the ownership of the vendor and any parent companies.
- Motives and Objectives: Understanding the vendor's business motives and objectives to ensure alignment with the Organisation's values and goals.
- Reputation and Compliance: Evaluating the vendor's reputation and compliance with relevant laws and ethical standards.

## Data Protection Impact Assessment (DPIA)

3.7 DPIA Requirement: When reviewing the feasibility of a new AI system, a Data Protection Impact Assessment (DPIA) will be conducted to ensure that all data and content points are thoroughly evaluated and addressed. The DPIA will cover the following aspects:

- Data Ownership and Control: Identifying who owns the data processed by the AI system and ensuring that data control remains with the Organisation.
- Data Security and Privacy: Assessing the security measures in place to protect data from unauthorized access, breaches, and misuse.
- Compliance with Data Protection Laws: Ensuring that the AI system complies with all applicable data protection laws and regulations, including the General Data Protection Regulation (GDPR).
- Risk Mitigation: Identifying potential risks associated with the use of the AI system and implementing measures to mitigate these risks.
- Transparency and Accountability: Ensuring that the use of AI is transparent and that there is accountability for decisions made by or with the assistance of AI systems.

3.7.1 Documentation and Review: The DPIA process will be documented, and the findings will be reviewed by the ICT and Data Protection teams. The Senior Information Risk Owner (SIRO) will make the final decision on whether to proceed with the implementation of the AI system based on the DPIA findings.

## Copyright

3.7 Users must adhere to copyright laws when utilising AI, especially when using LLM's. It is prohibited to use any AI to generate content that infringes upon the intellectual property rights of others, including but not limited to copyrighted material. If a user is unsure whether a particular use of AI constitutes copyright infringement, they should contact the Data Protection Officer or the relevant legal team.

## Accuracy

3.8 One of the incentives of automated decision-making through artificial intelligence (AI) and machine learning (ML) lies in their ability to generate decisions that are consistent, easily traceable, and replicable, marking a significant advancement over the variability inherent in human judgment. However, this technological promise is accompanied by a critical caveat: the potential for these systems to perpetuate or even exacerbate biases, resulting in discriminatory outcomes. The essence of ensuring fair use of AI while

acknowledging its inherent biases rests on understanding that while AI/ML systems hold the potential to revolutionise decision-making processes by eliminating human error and subjectivity, they are not free from the prejudices existing in the data they are trained on or the algorithms that drive them. These biases, if unchecked, can lead to decisions that unfairly disadvantage certain groups or individuals, thereby underscoring the importance of vigilance and ethical responsibility in the deployment of AI technologies. It is paramount that as we harness the efficiencies and accuracies offered by AI/ML systems, we also implement rigorous measures to identify, understand, and mitigate the biases within them to ensure that the advancements they bring about are equitably accessible and beneficial to all.

3.8.1 All information generated by AI must be reviewed and edited for accuracy prior to use. Users of AI are responsible for reviewing output and are accountable for ensuring the accuracy of AI generated output before use/release.

3.8.2 If a user has any doubt about the accuracy of information generated by AI, they should not use AI.

## Confidentiality

3.9 Confidential, proprietary, protected, and personal information must not be entered into a publicly available AI tool, as information may enter the public domain.

3.9.1 Confidential, proprietary, protected, and personal information must not be entered into any available AI tool without appropriate approval from the relevant Head of Service. This includes data relating to customers, employees, or partners. Users must follow all applicable data privacy laws and organisational policies when using AI. This approval should be logged in the Information Asset Register.

3.9.2 Users must not give access to AI tools outside the Organisation without prior approval from the relevant Head of Service

3.9.3 If a user has any doubt about the confidentiality of information, they should not use AI.

## Ethical Use

3.10 AI must be used ethically and in compliance with all applicable legislation, regulations, and organisational policies. Users must not use AI to generate content that is discriminatory, offensive, or inappropriate.

3.11 If there are any doubts about the appropriateness of using AI in a particular situation, users should consult with their line manager or the Data Protection Officer.

## Disclosure

3.12 Content produced via AI must be identified and disclosed as containing AI-generated information.

Footnote example: **Note:** *This document contains content generated by Artificial Intelligence (AI). AI generated content has been reviewed by the author for accuracy and edited/revised where necessary. The author takes responsibility for this content.*

## Security

3.13 Users must apply the same security best practices we use for all organisational and customer data. This includes using strong passwords, keeping software up to date and following data retention and disposal policies.

## Integration with other tools

3.14 API (Application Programming Interface) and plugin tools enable access to AI and extended functionality for other services to improve automation and productivity outputs.

3.14.1 Users should discuss integration of API/Plugin with the ICT Department who will follow OpenAI's [Safety Best Practices](#) to consider its appropriateness.

3.14.2 API and plugin tools must be rigorously tested for:

- Moderation – to ensure the model properly handles hate, discriminatory, threatening, etc. inputs appropriately.
- Factual responses – provide a ground of truth for the API and review responses accordingly.
- 

## 4. Risks

4.1 Use of AI carry inherent risks. A comprehensive risk assessment should be conducted for any project or process where use of AI is proposed. The risk assessment should consider potential impacts including legal compliance; bias and discrimination; security (including technical protections and security certifications); and data sovereignty and protection.

## Legal compliance

4.2 Data entered into AI may enter the public domain. This can release non-public information and breach regulatory requirements, customer, or vendor contracts, or compromise intellectual property.

4.2.1 Any release of private/personal information without the authorisation of the information's owner could result in a breach of relevant data protection laws.

4.2.2 Use of AI to compile content may also infringe on regulations for the protection of intellectual property rights, specifically the use of AI to reattribute personal data without lawful basis is an offence under DPA 2018 (section 171(1))

4.2.3 Users should ensure that their use of any AI complies with all applicable laws and regulations and with council policies.

## Bias and discrimination

4.3 AI may make use of and generate biased, discriminatory, or offensive content.

4.3.1 Users should use AI responsibly and ethically, in compliance with Organisation's policies and applicable laws and regulations.

## Security

4.4 AI may store sensitive data and information, which could be at risk of being breached or hacked.

4.4.1 The Organisation must assess technical protections and security certification of AI before use.

4.4.2 If a user has any doubt about the security of information input into AI, they should not use AI.

## Data sovereignty and protection

4.5 While an AI platform may be hosted internationally, under data sovereignty rules information created or collected in the originating country will remain under jurisdiction of that country's laws. The reverse also applies. If information is sourced from AI hosted overseas, the laws of the source country regarding its use and access may apply, for this purpose we discourage using AI platforms that are not UK hosted.

4.6 AI service providers should be assessed for data sovereignty practice by any organisation wishing to use their AI.

# 5. Compliance

## Record keeping for Compliance.

5.1 Records of requests to use any kind of AI must be kept, along with guidance issued. This should be available for reference by the ICT security team and the Information Governance team.

5.2 Any use of AI should have a clear Information Owner that has accountability for the use of that AI tool.

5.3 The decommissioning of any AI tool should be recorded in a register, identifying what assurances have been made in respect to the disposal of information that may have been collected.

5.4 Transparency arrangements should be in place for any use of AI where the processing affects or uses personal data.

5.5 Changes to the register are reported regularly to the Senior Leadership Team and/or ICT Strategy Board.

## 6. Review

6.1 It is recommended that this Policy be reviewed every 1 year to ensure it remains effective, appropriate and in parallel with the pace at which AI continues to develop.

## 7. Policy Compliance

7.1 If any user is found to have breached this policy, they will be subject to the Organisation's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

7.1.1 If you do not understand the implications of this policy or how it may apply to you, seek advice from the ICT Department.

## 8. Related Policies

Data Protection Standard

Employers Code of Conduct

Employers Disciplinary Policy

## 9. Glossary of Acronyms

- AI - Artificial Intelligence
- BBC - Boston Borough Council
- BYOD - Bring Your Own Device
- DPIA - Data Protection Impact Assessment
- ELDC - East Lindsey District Council
- GenAI - Generative Artificial Intelligence

- IA - Intelligent Automation
- ICT - Information and Communication Technology
- LLM - Large Language Models
- ML - Machine Learning
- PFH - Portfolio Holder
- RPA - Robotics Process Automation
- SHDC - South Holland District Council
- SIRO - Senior Information Risk Owner
- SLT - Senior Leadership Team