

Artificial Intelligence policy

2025 - 2028

1. Introduction

This policy provides a framework for the use of Artificial Intelligence (AI) at Hart District Council. At the heart of the policy is the intention to help our staff and contractors use AI in a responsible and ethical way. We must comply with all applicable laws and regulations, complementing the Council's existing information and security policies.

2. AI principles

Our approach to AI has been informed from a range of sources, including [Socitm](#), [Local Government Association](#), good practice from across the public and private sector and [Artificial Intelligence Playbook for the UK Government](#).

We have adapted the Government playbook principles and commit to:

- using AI lawfully, ethically and responsibly
- ensuring that AI supports, rather than replaces, officer decision making with clear accountability
- keeping AI secure and compliant with data protection, cyber security and regulatory policies
- focussing on enhancing our skills and expertise to develop AI, learning from the sector and beyond.

This, in turn, will allow us to:

- improve service delivery as we will offer faster and more accurate responses to resident and other enquiries
- provide better value for money as we will save time and resources and be smarter how we design our services.

3. Definition and scope

The [LGA define AI](#) as “machines that perform tasks normally requiring human intelligence, especially when the machines learn from data how to do those tasks.”

This policy applies to the use of Microsoft Copilot 365 included as part of the Council's Microsoft suite of applications. The use of Copilot within the tenancy owned by the Council allows essential safeguards to be put in place around the type of data entered and ensure complete oversight of its use.

The policy also applies to AI procured by the Council for a specific use as part of a standalone licensed product or included as a module or feature within an existing platform.

AI tools, embedded in existing known business applications and platforms (licensed or subscription based), and accessed by staff are included in this policy. These rules apply when using corporate-owned devices used for Council business. The policy

covers all Council staff who have access to these tools. [Appendix 1](#) provides a definition of AI related terms to help officers gain a shared understanding.

4. Responsibilities around use of AI

4.1 Governance

There is currently no legislation in place that directly refers to the use of AI in the UK. Regulators such as the [Information Commissioner's Office](#), [Financial Conduct Authority](#) and [Ofcom](#) oversee AI through their existing powers, requiring organisations to meet current standards on data protection, fairness, and accountability. The Local Government Association has collaborated with the [Equality and Human Rights Commission](#) to develop guidance for local authorities that [supports compliance with the public sector equality duty and data protection law when deploying AI](#).

Good governance at Hart provides a framework for decision-making, accountability, and transparency, mitigating potential risks and maximising the benefits of AI. It will help to foster public trust, promote proportionate deployment and safeguard staff. The Council's AI governance is considered in more detail in section 4.5 Accountability.

4.2 Data protection

Where an AI system is using or collecting personal data, it will fall within the scope of the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA). This includes personal data being used to train or test AI, or in the live deployment of the technology and refers to any personal data held by the Council.

GDPR and DPA gives individuals certain rights where their personal data is being used or created, particularly for automated decision-making. As such, the use of AI carries significant risks, and these must be carefully considered in the development and deployment of AI.

When undertaking any new project involving the use of AI, staff will need to complete:

- [Integrated Impact Assessment](#) (AI tab) to review and consider all potential impacts of the use of AI
- AI Data Protection Impact Assessment ([Appendix 2](#)) should be used to review the project and consider GDPR and DPA implications

In the majority of cases, the use of AI will involve a type of processing likely to result in a risk to individuals' rights and will trigger the legal requirement for staff to undertake a full DPIA. It would be good practice to involve the Data Protection Officer from the outset of any AI project for advice and guidance. [The ICO website has further guidance](#) that staff should familiarise themselves with.

4.3 Data quality

It is essential that any [effective use of AI relies on good quality data](#). Any use of AI should consider these components of quality data:

1. Accuracy: Accurate data is crucial for AI algorithms, enabling them to produce correct and reliable outcomes
2. Consistency: data should follow a standard format and structure, enabling the efficient processing and analysis of the data
3. Completeness: Incomplete data can cause AI to miss essential patterns and correlations, leading to incomplete or biased results
4. Confidentiality: data should be secure and stored following GDPR procedures
5. Timeliness: Up to date data plays a significant role in AI performance and provide staff with current information
6. Relevance: Relevant data contributes directly to the problem at hand, helping AI to focus on the most important aspect of the query.

4.4 Copyright

Staff must comply with copyright laws when using AI. Staff must also understand the licensing terms of any AI tools they use. This includes verifying whether the generated content can be used, edited, or distributed, depending on the licensing conditions of the AI service provider.

If staff are unsure whether a particular use of AI constitutes copyright infringement, they should contact Legal Shared Service before using it.

4.5 Accountability

There are a number of roles in the Council that will help in the development and ongoing review of this AI policy:

- The Executive Director for Corporate Services acts as the organisation lead regarding the use of AI and delegates responsibility to staff to monitor compliance with and enforce the policy
- Corporate Project Board will consider all major projects relating to AI
- Operational Management Group will be updated of the use of AI across the services
- The Change and Digital Manager will communicate and promote AI use
- The Data Protection Officer is responsible for providing advice on data protection obligations in relation to AI use
- IT will provide technical support on the use of Copilot and advisory for security, safety and, procurement of AI
- The AI governance and working group will be responsible for the review and monitoring of this policy and [Appendix 3 use of AI across the Council](#). This group will:
 - Be chaired by Change and Digital Manager

- Involve interested staff from across the Council, reflecting the full range of grades and services including the Monitoring Officer
- reflect diversity of perspectives on AI, requiring active recruitment and should include IT, Data Protection, Procurement and other teams using AI
- Be a critical and curious space to exchange ideas, with invited external speakers from peer organisations to inspire and engage members
- Support the adoption of the AI Policy by communicating the work of the group back to teams
- Meet every quarter to ensure the AI register is up to date, help identify and scrutinise new projects and consider different options to explore the use of AI. The group will assist in the annual review of the policy.

4.6 Accuracy

All information generated by AI must be reviewed and checked for accuracy before use. AI may provide highly plausible results but could contain errors, known as hallucination.

Staff are responsible and accountable for ensuring the accuracy of AI generated content before use or release. If a member of staff has any doubt about the accuracy of information generated by AI, they should not use that AI tool without thoroughly checking the source data.

4.7 Confidentiality

Staff must consider the risks associated with the use of confidential and commercially sensitive data. Confidential and personal information must not be entered into any public AI tool. The information may purposefully or inadvertently be released into the public domain, including if the system is breached or hacked. This could lead to the Council facing legal proceedings for breach of confidence or copyright. Some examples of the use of confidential information are below:

- Staff must not use an AI tool to write a letter to a resident with any personal details in, for example the use of name or address as that data will be kept by AI for re-use. It would be acceptable for AI to write parts of the correspondence which doesn't include personal information
- Staff must not use AI apps on personal phones to record and summarise work meetings, or to use translation services
- Staff should check if they are able to use AI generated images and content if publishing to an external audience
- Staff must not upload personal data for AI analysis into Copilot. Confidential or personal information should only be entered into an AI tool that has been built or procured specifically for the Council where the data entered is restricted for our sole use and won't be externally published without being anonymised and significant officer scrutiny.

4.8 Bias

Data and information generated by AI will reflect any inherent biases in the data set accessed to produce it. This could include content which may be discriminatory based on factors such as race, gender, or socioeconomic background. Staff must ensure they follow the requirements of the [Equality Act 2010](#) as set out in the Council [Integrated Impact Assessment process](#). Particular care must be taken where AI could be used for profiling purposes (for example, identifying the most suitable candidate characteristics for a particular job role).

4.9 Staff oversight

A lack of staff intervention may result in AI outputs going unchecked. Staff should be aware that AI lacks flexibility, human understanding and compassion. Some AI models only collate data prior to a certain date so content generated may not reflect the most recent information.

4.10 Environmental sustainability

Staff should be mindful of the environmental impact of AI. Every query or prompt to an AI platform uses energy, produces carbon dioxide and demands significant water use. This demand will grow as more AI models are developed, and usage grows. The Council should seek AI partners who are transparent about their carbon and water footprint, can demonstrate energy and resource efficiency and have a development roadmap to shift to lower carbon technologies.

All staff who use AI or are responsible for procuring AI should be mindful of their role in helping to achieve the Council's target of becoming carbon neutral by 2035.

4.11 Disclosure

Any content produced by AI including text and images should be reviewed and, if necessary, identified as containing AI generated information. An example of the suggested text that should be used.

Note: This image/document contains content generated by Artificial Intelligence. All AI generated content has been reviewed by the Council for accuracy and edited/revised where necessary.

4.12 Related policies

This policy forms a key part of the Council's overall policy framework and should be read in conjunction with:

- IT Security Policy
- Security Updates and Update Management Policy
- Data Protection Policy

5. Procurement

When staff are satisfied that [AI is the right technology for the specific business challenge](#) and ready to go to market, they should follow the Council's [contract procurement rules](#). As a burgeoning field, the AI marketplace is not fully developed, meaning that in some areas, available technology may still be in pilot stage and the risks or limitations not fully understood. The commissioning Officer will need to work with the supplier to fully understand the risks and considerations that have been made in the AI's development, as ultimately responsibility for the accuracy of information will sit with the Council. [The LGA provide guidance on responsibly buying AI.](#)

Staff should be satisfied of the suppliers' response in the procurement process to a range of specific questions including:

- their openness to providing transparent and clear explanations for the AI decisions where appropriate
- how they would address potential biases in AI data and algorithms it uses
- their commitment to protecting sensitive data
- how they ensure the security of their AI product
- how they adhere to legal and ethical principles
- their commitment to reducing the environmental impact of AI deployment – see [Environmental sustainability](#)
- the ownership and security of the data that the AI is trained on
- how they manage changes to their AI product
- integration into existing council platforms and processes.

Staff will need to consider the level of scrutiny each element requires depending on the scale and complexity of the project, and whether the entire procurement exercise is for an AI platform or if it is a small part of a wider contract.

[Appendix 4](#) provides a list of suggested questions as part of the procurement process

6. Risks

The use of AI can carry inherent risks. A comprehensive Integrated Impact Assessment should be conducted for any project or process where use of AI is proposed. The risk assessment should identify the risks with consider potential impacts including:

- legal compliance
- bias and discrimination
- security including technical protections and security certifications
- data protection.

For further reading around risk in AI, NIST has produced a [risk management framework to develop understanding of the risks associated with AI](#) and suitable actions to mitigate them.

7. Training

The Council will need to identify suitable, accredited courses to establish a core number of staff specifically trained in the use of AI. AI readiness will align with the Council's transformation programme, focusing on upskilling staff and fostering a culture of innovation.

Core aspects of the training programme will include:

- AI literacy - building an understanding of AI applications, data management and ethics among all staff
- role-based skills - tailored training for specific roles that interact directly with AI tools, ensuring practical proficiency in AI-assisted processes
- continuous learning - ongoing sessions and workshops to address emerging AI trends, operational skills, and responsible AI usage

In addition, and to support this policy, additional guidance for staff will be developed, supported by updates to the e-learning package on SEEDL.

8. Review

This policy will be reviewed annually and updated when necessary to ensure the Council remains up to date and compliant with all applicable legislation, regulations and organisational policies.

Version

0.1	Draft version	Steve Bennett	8 August 2025
0.2	Edited to reflect comments from SLT	Steve Bennett	9 September
0.3	Added LGA definition to 3. Scope	Steve Bennett	29 September
0.4	4.10: edited to include Local Partnerships text on local government	Steve Bennett	6 October
0.5	OMG. Added appendix 1 for definition of terms and edited numbering for other appendices	Steve Bennett	13 October
Final	Policy approved at SLT	Steve Bennett	28 October 2025