Appendix 1

Artificial Intelligence (AI) Policy

Version control	V0.2
Approved by	TBC
Next review date	October 2027
Job title of responsible officer	Assistant Director, Digital, Data and Technology

Foreword

The world in which the Council operates is changing rapidly. Although types of Artificial Intelligence (AI) have been around for decades, in recent years the rise of generative AI tools that can learn and perform tasks usually completed by humans represents a significant advancement in technology, leading to new opportunities and risks.

It is critical that the Council moves with the times and can derive benefit from Artificial Intelligence, while ensuring that it has adequate controls in place to mitigate potential risks.

The 'What is AI' section of the AI Playbook for the UK Government defines AI as:

"An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment."

Purpose

The purpose of this Artificial (AI) Policy is to set out clear guidelines for the responsible use of AI by employees, elected members, suppliers and contractors. It should be read in conjunction with the Council's Data Protection, Information Security, Equality and relevant HR policies.

Scope

The Policy applies to all Council services, all employees and elected members (while delivering Council work), and to suppliers commissioned to provide products to, or to deliver services, on the Council's behalf.

The policy covers any AI system that is procured, developed by or for, or used by, the Council, or that is used by any partner or supplier in the delivery of Council services.

Policy statement

The Council understands the potential benefit of Artificial Intelligence in the delivery of public services, providing it is used safely, lawfully, responsibly and ethically.

The Council also recognises that the use of AI is not without risk. This policy sets out guiding principles for the responsible procurement, development and usage of AI across the Council and should be read in conjunction with the Council's existing Data Protection, Information Security and HR policies and alongside the Council's Architecture Design Principles that cover the use of all ICT systems.

Principles

The following six key principles must be followed to ensure the safe, lawful, responsible and ethical use of AI at Gedling.

The Council will:

1. Seek to balance risk and benefit in the use of AI

- The Council will welcome ideas across all services in relation to the potential use of AI to support agreed outcomes. All Council staff and elected members are encouraged to consider where AI might be able to add value.

- Where no personally identifiable, sensitive, or organisationally confidential information, is being exposed to AI, and where the relevant AI tooling has been approved for use through the Council's Business Technical Design Authority (BTDA), employees and elected members will be enabled to use approved AI tools provided by the Council in the delivery of their work.

- A single approved technology register shall be maintained by the Council's BTDA and will include approved AI tools.

- In cases where personally identifiable data is being used, or where information that is proposed for exposure to AI is confidential, formal advance approval must be sought from the Corporate Risk Group and a Data Protection Impact Assessment (DPIA) must be completed for each use case.

- Following approval, the Council's Record of Processing activity must be updated to reflect changes to the processing of personally identifiable data. The Record is monitored by the Council's Data Protection Officer and must be kept updated by Data and Process Owners.

- AI tools that are available for personal use and not provided by the Council may be used for general search and research purposes (in the same way that a search engine would) but may not be used to process Council data.

- Results from either AI used outside of the Council or AI tools made available within it must be checked for accuracy before use and must not be replicated in any publication due to the potential for copyright infringement. Any content that has been created using generative AI should include the following footnote as standard:

  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.*

- Data that is held by the Council and not generally available to the public, including all personally identifiable data, must not be exposed to personal, or unapproved, AI tools.

- Unauthorised AI tools will be blocked by the ICT service for use on the Council's network to ensure that no Council data or personally identifiable information is released inadvertently via unauthorised applications.

2. Ensure lawful and ethical use

- AI use will be compliant with all necessary legislation and regulation, including, but not limited to, the Data Protection Act (UK, 2018) and the Copyright, Designs and Patents Act (UK, 1988).

- The processing of personally identifiable information using AI will be limited to that which is strictly necessary and must first be approved by the Council's Corporate Risk Group.

- The lawful basis for processing personally identifiable information will be included in the Council's Record of Processing Activity and a DPIA will be undertaken for each relevant use case.

- AI will not be used to make decisions. It may make recommendations, but all decisions will be reviewed and made by humans.

- It is recognised that AI presents potential risks in relation to unintended bias based on gender, race, age, ethnicity, and other protected characteristics. Where AI is used to process personally identifiable information that has implications for people (e.g. Recruitment process support, analysis of large-scale consultation data), an Equality Impact Assessment will be undertaken and appropriate mitigations put in place.

3. Ensure AI services are secure and resilient

- Safeguards will be considered for all AI tools including ensuring sufficiently robust technical controls are in place. These include security testing and, in the case of generative AI, content filtering to detect malicious activity, as well as validation checks to ensure responses are accurate.

- Requirements relating to AI that are included in any specification document when procuring systems or services using AI will be clear and will required detailed responses from suppliers to enable the Council to ensure security and resilience.

4. Ensure data processing transparency.

- All AI solutions used by the Council will be explainable and open to scrutiny. No solutions or services will be bought, or used, where it is not clear how data is being processed.

- Procurement of new solutions or services that include the use of AI will include reference to this policy and suppliers will be expected to adhere to it.

5. Train employees on the benefits and risks of AI.

- All employees, and relevant partners, suppliers and sub-contractors will be made aware of this Policy.
- All employees will be provided with appropriate training and guidance prior to being granted access to AI capabilities.
- Access to AI will only be granted by the Digital, Data and Technology team and licences will be managed centrally.

6. Ensure value for money

- The Council recognises that AI comes at a cost and will assess each request for the use of AI based on an overall assessment of the value for money that it offers.
- This assessment will follow standard business case principles and consider relative benefit, risk and total costs.
- Requests to use AI must first be logged via the ICT service desk for review.

Monitoring

The use of AI will be monitored by the Digital, Data and Technology team.
Licences and usage will be periodically reviewed to ensure value for money and licence compliance.

Unauthorised use of AI will be referred to the Assistant Director for Digital, Data and Technology and the relevant line manager for investigation.

Suspected data breaches (unauthorised disclosure of personally identifiable or confidential data via unapproved tools) must be reported using the Council's existing data breach process.

Roles and responsibilities

Role	Responsibility
Cabinet	Approval of the Policy and periodic review of the use of AI as part of standard SIRO reporting.
Senior Information Risk Own (SIRO)	Accountable for the Policy and its enforcement.
Assistant Director of Digita Data and Technology	Responsible for policy implementation and review.
Business and Technic Design Authority	Responsible for approving AI for Council use and maintaining a register of all approved solutions (also responsible for assessing supplier solutions where used in the delivery of Council services).
Corporate Risk Group	Responsible for assessing use cases where personally identifiable data is proposed for use and approving usage (in liaison with the Chair of the BTDA and technology approval). Responsible for ensuring completion and assessment of related DPIAs.
ICT team	Responsible for granting access to AI tools following approval from the BTDA (and, where necessary, the Corporate Risk Group). Responsible for reviewing access, usage and licensing on a periodic basis.

Data and Process Owners	Responsible for completing DPIAs, EqIAs and updating the Council’s ROPA as required.
Assistant Director Workforce	Responsible for ensuring appropriate training on AI is captured and fed into the organisation’s Learning and Development plans.
Directors and Assista Directors	Responsible for ensuring all employees are aware of the AI policy and what it means for them.
All employees and electe members	Responsible for adhering to the Policy and related processes.

Review period

This Policy will be approved by Cabinet and reviewed no less frequently than every two years.

Related policies

GDPR

Information Security

Equality and Diversity

Templates and links

Request AI use	Self-Service Portal - SysAid Help Desk Software
BTDA template	Expression of Interest (EOI) Form v1.0 .docx (Note this must be sent to the Service Desk as part of a request for AI use if new technology is to be used).
Data Protection Impact Assessment	https://intranet.gedling.gov.uk/wp-content/uploads/2019/10/Data-Protection-Impact-Assessment-DPIA-Questionnaire.doc (Note this must be sent to the ICT service desk for inclusion on the agenda at the Data Security Group)
Equality Impact Assessment	https://intranet.gedling.gov.uk/wp-content/uploads/2019/01/EIA-form.docx