FOREST ROW PARISH COUNCIL
ARTIFICIAL INTELLIGENCE POLICY

Purpose

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

Scope

The Policy applies to all Council services, all employees and Councillors (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, IT and HR policies.

Principles

The following six key principles must be followed to ensure the safe, lawful, responsible and ethical use of AI at this Council. 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 Councillors 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, employees and Councillors will be enabled to use approved AI tools provided by the Council in the delivery of their work.

• 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 Clerk and a Data Protection Impact Assessment (DPIA) must be completed for each use case.

• 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 may be blocked by the Council's IT providers 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 must be identified, and a DPIA will be undertaken for any relevant 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 offered appropriate training and guidance prior to being granted access to AI capabilities.

6. Ensure value for money

• The Council recognises that some AI usage comes at a cost, and will assess each request for the use of such 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.

7. Monitoring

- The use of AI may be subject to monitoring via the Council's IT providers.
- Licences and usage may be periodically reviewed to ensure value for money and licence compliance.4
- Misuse of AI, or unauthorised use of paid-for AI facilities by staff members may constitute a disciplinary offence.
- 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.

New policy introduced March 2026 Due for review May 2027