WEST LOTHIAN COUNCIL ARTIFICIAL INTELLIGENCE POLICY

Data Label: Public

West Lothian Council

ARTIFICIAL INTELLIGENCE POLICY CONTENTS

Contents

West Lothian Council

1. BACKGROUND

AI technologies are rapidly advancing and have the potential to support the Council by enhancing efficiency, improving operations and assisting with decision-making for some of its key services. Although the adoption of AI presents significant opportunities to enhance efficiencies in the Council, there are risks that must be carefully considered prior to adopting AI within Council operations, which will be outlined in this policy.

2. PURPOSE

The purpose of this policy document is to establish guiding principles for West Lothian Council that must be considered when using AI technologies, including, but not limited to machine learning models, natural language processing systems and Generative Artificial Intelligence Large Language Models (GenAI) such as ChatGPT, Google Gemini and Microsoft Copilot.

GenAI is one of the most prevalent AI technologies utilised across industries and applications, allowing users to input prompts to produce various types of content such as text, images, audio, video, software code and other media. The GenAI models can learn and evolve as it trains on data structure and patterns to produce new data, which is based on the input from the user.

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 Governance and Information Security policies including the Council's Acceptable Use Policy (AUP). This policy is supplementary to existing policies and should be read in conjunction with them.

AI is a group of complementary technologies, which are evolving constantly. For that reasons this policy does not focus on any individual trends or innovations. The pace of development and application of AI is such that this policy will be reviewed on a regular basis to ensure continued relevance.

3. SCOPE

This policy applies to all users of the Council's data, systems and resources with access to AI, including elected members in relation to information controlled or processed by the council, as well as any other policies and procedures in support of this policy.

AI used must be trustworthy, ethical and inclusive and present people with the skills and opportunities to play their part as part of a diverse workforce, and benefit from the transformations that AI will bring to our ways of working. The use of AI must be in a manner that provides assurance that the products, services and decisions enabled by AI are safe and secure, and will protect their rights. The AI must promote fairness and avoid bias to prevent discrimination and promote equal treatment and be used in such a way as to contribute positively to the Council's goals and values, aligning with the Council's equality and diversity policies.

Users may use AI for work-related purposes subject to adherence to this policy and relevant guidance, and procedures. This includes tasks such as generating text or content for reports, emails, presentations, the delivery of training, images and customer service communications.

The policy encourages initiatives to enhance AI literacy and skills among all stakeholders, particularly those involved in developing AI solutions, as well as those using AI technologies in their work.

Particular attention should be given to Governance, Vendor practices, Copyright, Accuracy, Confidentiality, Disclosure and Integration with other tools, as described in the following sections.

4. GOVERNANCE

If there is a business requirement to input personal or confidential information to Generative AI technology, users must complete a Data Protection Impact Assessment (DPIA) and facilitate the completion of an IT Security Assessment for the Councils IT Security team to assess.

Personal information may not have been requested but may have been provided by individuals. All such information must be reviewed and personal information removed prior to using AI technology.

Approved AI solutions must be recorded and managed in the council's information asset register, ensuring their use remains transparent across the organisation.

Deployment of AI technologies across the Council must adhere to the council's Information Security Guidance.

4.1. Vendors

Any use of AI technology in pursuit of Council activities should be done with full acknowledgement of the policies, practices, terms and conditions of developers/vendors. All AI purchases must be managed through the Council's Corporate Procurement Unit.

4.2. Copyright and Licensing

Users must adhere to copyright laws when utilising AI. It is prohibited to use AI to generate content that infringes upon the intellectual property rights of others, including but not limited to copyrighted material.

In addition, users must ensure they comply with licensing terms of any AI system or tools they utilise. This includes verifying whether the generated content can be used commercially, modified, or distributed, depending on the licensing restrictions of the AI service provider.

If a user is unsure whether a particular use of AI constitutes copyright or licensing infringement, they should contact the council's Corporate Communications Team via email – media@westlothian.gov.uk.

4.3. Accuracy

All information generated by AI must be reviewed, checked and edited to ensure 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.

Users remain professionally responsible and accountable for the quality and content of any output generated by AI, however generated or used.

4.4. Confidentiality

AI systems must comply with data protection regulations, including GDPR and other applicable laws and statutory guidance

Confidential and personal information must not be entered into public GenAI tools, applications or web sites (like ChatGPT), as information will become available to the public domain. Users must follow all applicable data privacy laws and organisational policies when using AI.

If a user has any doubt about the confidentiality of information, they must not use that AI tool.

4.5. Ethical Use

AI must be used ethically and in compliance with all applicable legislation, regulations, statutory guidance, and Council policies.

Users are responsible for ensuring that any AI generated content is not discriminatory, offensive, or inappropriate. Users should be aware of discrimination that biased data or inadequate design or use of AI might create. If there are any doubts about the appropriateness of using AI in a particular situation, users should consult with their manager or seek advice from a relevant contact.

Human oversight is essential for the ethical use of AI ensuring that AI systems operate in alignment with societal values and ethical standards. Human review must be conducted on AI outputs for biases, discrimination and accuracy.

4.6. Disclosure

Transparency in AI is crucial for ensuring accountability, which includes providing information on how the AI-generated decisions are made.

The presence and role of any AI systems will be disclosed in our operations to relevant stakeholders, including employees, customers and partners. This includes information on how AI systems are used, details of the data they process and decision making processes they support.

4.7. Integration with other tools

Application Programme Interface (API) and plugin tools enable access to AI and extended functionality for other services to improve automation and productivity outputs. Users should consult the council's Information Security Guidance for support on the use of such tools and AI.

5. DEVELOPMENT, DEPLOYMENT AND USE OF AI

5.1. Risk Assessment

A comprehensive Data Protection Impact Assessment (DPIA), Integrated Impact Assessment (IIA), Consumer Impact Assessment (CIA) and IT Security Assessment should be conducted

for any project or process where the use of AI is to be developed or deployed. These assessments should consider potential impacts including legal compliance; bias and discrimination; security (including technical protections and security certifications); and data storage location including applicable laws and regulations.

5.2. Legal Compliance

AI systems developed or deployed within the Council must comply with applicable laws and regulations, statutory guidance, and with Council policies.

Data entered within an AI system may enter the public domain. If used inappropriately, this can release non-public information and breach regulatory requirements, customer or vendor contracts, or compromise intellectual property. Any release of private/ personal information without the authorisation of the information owner may result in a breach of relevant data protection laws.

Use of AI to compile content may also infringe on regulations for the protection of intellectual property rights. Users should ensure that their use of any AI complies with all applicable laws and regulations and with Council policies, ensuring responsible use of AI and ethically.

5.3. Bias and Discrimination

AI systems developed or deployed by the Council must be regularly tested for bias, discriminatory or offensive content, where such issues are identified they must be reported to the council's Data Protection Officer who will consider and determine corrective actions as necessary.

5.4. Security

AI systems must be secure by design to protect against data breaches, cyber-attacks and any other misuse. Regular security assessments and updates should be conducted to address potential vulnerabilities to ensure security standards align with frameworks such as Public Sector Network (PSN) and Payment Card Industry Data Security Standards (PCI DSS).

AI may store sensitive data and information, which could be at risk of being breached or hacked. The Council must assess technical protections and security certification of AI before use as part of the DPIA process.

If a user is not clear about the security of information input into a specific AI tool/solution, they should not use that specific AI tool/solution.

5.5. Data Sovereignty and Protection

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.

AI service providers should be assessed for data sovereignty practice by the council service wishing to use their AI solution in conjunction with the information governance policy.

6. COMPLIANCE

Any breaches of this policy should be reported to the Council's Data Protection Officer and relevant Head of Service. Failure to comply with this policy may result in disciplinary action, in accordance with Council's Human Resources policies and procedures.

7. MONITORING AND REPORTING

Governance over this policy is built into normal council processes e.g. line management, service management and project management. Formal governance over this policy is set out in the following table.

Group	Role	Frequency
Corporate Management Team	Scrutinise and review implementation, progress, and compliance	Quarterly
Corporate Governance Board	Reviewing and implementing policies, procedures and standards. Evaluating and monitoring projects in line with this policy.	Quarterly
Information Management Working Group	Developing and implementing policies and procedures relating to the strategy and monitoring/ reporting progress across service areas.	Monthly
Council Executive	To approve the adoption of policy, it's amendment or replacement.	As required
Corporate Policy and Resources Policy Development and Scrutiny Panel	Developing policies with a view to making recommendations for adoption by Council Executive, To review the working of policy and to make recommendations about its working, amendment or replacement to the Council Executive	Annually

8. RESPONSIBILITIES

By using AI, users acknowledge that they have read and understood this policy, associated guidance and procedures.

9. OTHER RELEVANT POLICIES

Information Governance Policy
Special Category Data Policy

10. REVIEW

As AI is an emerging technology, this policy will be reviewed on an annual basis. The Head of Corporate Services may make minor and administrative changes when required, for example, to reflect internal council management structure changes, or new legislation or guidance.

11. GLOSSARY OF TERMS

Algorithm is a rule given to an AI machine to perform a task.

Artificial Intelligence (AI) is an umbrella term for a range of algorithm-based technologies and approaches that often attempt to mimic human thought to solve complex tasks, these may include, visual perception, speech recognition, decision making, and translation between languages.

ChatGPT is owned by OpenAI LP, an artificial intelligence research lab. GPT stands for 'Generative Pre-trained Transformer'. It means that the model has the ability to generate text or other forms of output. ChatGPT is primarily trained using public data from the internet.

Generative AI (Gen AI) is a form of AI, which produces new content, such as images, text or computer code. It works by using large quantities of data, often harvested from the internet, to train a model in the underlying patterns and structures of that data. After many rounds of training the model is capable of generating new content. When a user provides a prompt or input, the AI evaluates the likelihood of various possible responses based on what it has learned from its training data. It then selects and presents the response that has the highest probability of being the right fit for the given prompt. That prompt and response then may be fed back into the model to provide further training.

Large Language Model (LLM) is a huge database of language knowledge that can write articles, answer questions or create realistic dialogue and is pre-trained on large amounts of data.