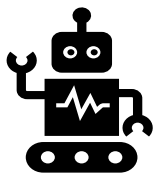




# St Georges and Priorslee Parish Council

## Artificial Intelligence (AI) Policy

### 1. Introduction



*AI* - the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings.

- 1.1 There are clear benefits and risks associated with processing data (including voice data) using AI solutions/technologies.
- 1.2 St Georges & Priorslee Parish Council is committed to taking a risk-based approach to the implementation and use of IA. This means:
  - Assessing the risks to the rights and freedoms of individuals that may arise when using AI
  - Implementing appropriate and proportionate technical and organisational measures to mitigate these risks.
- 1.3 This policy is written to ensure that the use of AI is compliant with all applicable laws, regulations and Council policies. It supports the ethical and moral use of AI under the Council's instruction.
- 1.4 This policy provides a framework for the use of AI solutions/technology by Council employees (whether temporary or permanent), Members, contractors, agents, vendors and anyone else processing information in pursuit of the Council's activities.
- 1.5 Given the pace of IA development, this policy will be continually developed to ensure it mirrors legislative/regulatory requirements and best practice.

### 2. Use of AI

- 2.1 The use of AI solutions/technologies should always support the Councils vision, priorities and values.

- 2.2 Councils that are considering the use of AI should engage with internal stakeholders as part of their due diligence. As a minimum, the Council's ICT and data protection support should be consulted on all AI projects.
- 2.3 If a Council is looking to use IA to develop public facing publications, they should also consider the public relations element of this.
- 2.4 In the feasibility stage of plans to use AI, the Council must consider the relevant governance requirements, any provider practices if 'off the shelf' applications and/or technologies are procured, copyright, confidentiality, disclosure, accuracy and potential integration with other tools.
- 2.5 The AI solution should have appropriate logging and auditing mechanisms in place to capture activities related to AI usage.

### **3. Governance Requirements for Using AI**

- 3.1 Any stakeholder looking to use/implement an AI solution/technology must be fully aware of the Council policies and procedures relating to data. As a minimum the stakeholder must have a good understanding of the requirements detailed in the following documents:

- Data Protection Policy
- Corporate Information Security Policy
- Records Management Policy
- Information Sharing Policy
- Corporate Information Retention Schedule

- 3.2 The risks associated with the introduction and use of an AI solution/technology need to be assessed and managed. To assist in the identification, mitigation and management of AI associated risks, the Council intending to use AI must complete:

- AI Risk Assessment
- AI Data Protection Impact Assessment

Templates for these assessments can be obtained from your data protection support.

Both assessments require approval before the Council implements the AI solution/technology.

### **4. Supplier/Vendor**

- 4.1 Where a Council looks to procure AI solutions/technology, engagement should be established with the relevant Information Asset Owner, senior management and developers/vendors.

### **5. Copyright Considerations**

- 5.1 Copyright law must be complied with when using AI.
- 5.2 AI must not be used for generating content that infringes upon the intellectual property rights of others, including but not limited to copyrighted materials. If the Council is unsure as to whether the intended use of IA may infringe copyright they should contact their legal support.

## 6. Accuracy of AI Output

- 6.1 Information produced by using AI solution/technology must be reviewed by the Council employee for accuracy prior to sharing/using the information.
- 6.2 If the Council has any doubt about the accuracy of IA output then IA solutions/technology should not be used.

## 7. Confidentiality

- 7.1 Personal and confidential information must not be processed using public AI solutions such as ChatGPT, as this may enter the public domain.
- 7.2 If a Council is planning to use a non-public AI solution, and this will include processing personal data, then as a minimum an AI Data Protection Impact Assessment must be completed.
- 7.3 Any processing of personal data using an AI solution must comply with the principles of the UK Data Protection Act 2018.

## 8. Disclosure and Transparency

- 8.1 If IA is used to create content, the content should be disclosed as containing AI generated information. Any documents and/or publications that include AI generated content should include a statement to make this clear to the reader, an example statement is detailed below:

**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.*

## 9. Integration with Other Tools

- 9.1 API and plugin tools enable access to AI and extended functionality. Council's planning to integrate AI should follow Open AI's [Safety Best Practices](#):
  - **Adversarial testing** – testing AI should include typical scenarios as well as tests to 'break' the system
  - **Human in the loop (HITL)** – a person should review AI output before it is used more widely
  - **Prompt engineering** – reduces the chance of producing undesired content

- **Know your customer (NYC)** – AI users should have to register to use the AI solution and have a unique use rid
- **Constrain user input and limit output tokens** – limiting the amount and type of input/output can reduce the likelihood of misuse/error
- **Allow users to report issues** – a mechanism should be available to allow AI users to log concerns they have while using the AI solution
- **Understand and communicate limitations** – consider whether the AI solution has limitations that could create offensive and/or discriminatory content
- **End-user IDs** – the use of unique user IDs can help detect improper use of AI

9.2 Any relevant API and plugin tools must be rigorously tested for:

- **Moderation** – AI handles inappropriate input that can be categorised as hate, discriminatory, threatening, etc
- **Factual responses** – establish a ground of truth for the API and review responses against this

## 10. AI Risks

- 10.1 The use of AI carries inherent risks. Before AI solution/technology is implemented, a thorough risk assessment should be completed. See 3.2 for what assessments are required.
- 10.2 Each new IA project will have its own context, data flows, output requirements and therefore needs to be assessed individually against the core requirements of this policy. The completion of the risks assessment and AI Data Protection Impact Assessment will assist the Council manage each AI project.

## 11. Compliance with Legal and Regulatory Requirements

- 11.1 Data processed by public facing AI solutions may enter the public domain resulting in potential personal data breaches, breaches of confidentiality and/or compromising intellectual property.
- 11.2 Council's using AI solutions/technology must ensure that this use complies with all applicable laws, regulations and Council policies at all times.
- 11.3 Unauthorised use of copyrighted material or the creation of content that infringes on the intellectual property of others is strictly prohibited.

## 12. Bias and Discrimination

- 12.1 Some AI solutions may use and/or generate biased, discriminatory or offensive content. Therefore, Council's using AI need to understand this and ensure any AI output is comprehensively checked by a human to ensure biased, discriminatory or offensive content can be censored/removed.

## **13. Security**

- 13.1 The Council is committed to protecting the confidentiality, integrity and availability of its data.
- 13.2 AI solutions may store personal, sensitive and/or confidential information which could be at the risk of disclosure due to the AI technology being hacked.
- 13.3 Council's looking to use AI solutions must ensure that the relevant technology in place is secure. Technical controls must be commensurate with the level of risk associated with the information being processed by the AI solution.
- 13.4 Where the AI solution processes personal data, the Council must investigate whether this data can be anonymised.
- 13.5 Any data processed by an AI solution should be encrypted in transit and at rest.
- 13.6 The AI solution should have the appropriate security accreditations such as ISO27001, Cyber Essentials+, etc. If the solution uses cloud computing, then this should comply with the NCSC 14 Principles of Cloud Computing.
- 13.7 Council's should check the level of security of any proposed AI solution with their ICT and data protection support.

## **14. Data Sovereignty and Protection**

- 14.1 Many AI solutions will be hosted internationally. However, under data sovereignty rules any information created or collected in the originating country will remain under the jurisdiction of that country's laws.
- 14.2 Any AI solution used should be checked for its data sovereignty practices prior to use. If the practices cannot be determined, then Council's should contact their data protection support for further advice.

## **15. Training and Awareness**

- 15.1 All users of AI solutions must receive training on the responsible and secure use of AI. This training should cover topics such as ethical considerations, risk management, security and compliance requirements.

## **16. Compliance**

- 16.1 This policy applies to all Council uses of AI solutions/technology.
- 16.2 Any suspected or confirmed security incidents related to AI usage must be reported to the data protection support team.

16.3 Failure to comply with this policy may result in disciplinary action being taken.

## **17. Review**

17.1 This policy will be reviewed periodically and updated where necessary to ensure ongoing compliance with all relevant legislation, regulations, other Council policies and best practice.

Date of policy: December 2024

Approving committee: Full Council

Policy version reference: TWC

Due for Review December 2027