



GREAT BEDWYN PARISH COUNCIL

ARTIFICIAL INTELLIGENCE (AI) USAGE POLICY (V1)

1. Introduction

This policy sets out the framework for the safe, lawful, and responsible use of Artificial Intelligence (AI) within Great Bedwyn Parish Council.

The Council recognises the potential benefits of AI in improving efficiency and supporting administrative functions. However, its use must be carefully managed to ensure compliance with:

- Data Protection Act 2018
- Guidance issued by the Information Commissioner's Office (ICO)
- UK Government guidance on AI use in the public sector

This policy ensures that AI is used in a manner that protects personal data, maintains public trust, and supports transparent decision-making.

2. Scope

This policy applies to:

- All councillors
- All employees and volunteers
- Contractors and third parties acting on behalf of the Council

It applies to all AI use in connection with Council business, regardless of device or location.

3. Definition of Artificial Intelligence

AI refers to software systems capable of generating outputs such as text, analysis, or recommendations based on user input.

This includes:

- - Generative AI tools
- - Automated data analysis tools
- - Machine learning-based systems

4. Policy Principles

4.1 Lawfulness, Fairness and Transparency – AI must comply with UK GDPR principles.

4.2 Human Oversight and Accountability – AI must not replace human judgement; outputs must be reviewed.

4.3 Purpose Limitation – AI used only for legitimate Council purposes.

4.4 Data Minimisation – Only necessary data used.

4.5 Security and Integrity – Protect confidentiality and data security.

4.6 Equality and Non-Discrimination – Must comply with Equality Act 2010.

5. Acceptable Use of AI

AI may be used for:

- Drafting documents
- Summarising content
- Improving clarity
- Generating templates

All outputs must be reviewed, verified, and approved by council staff or councillors depending on the output and use of the output.

6. Prohibited Use

AI must not be used for:

- Formal decision-making
- Processing personal/sensitive data in unapproved tools
- Entering confidential data into public AI tools
- Producing unverified outputs

7. Data Protection and Information Governance

7.1 Personal Data – Only processed with lawful basis and safeguards.

Special category data must not be entered into AI systems.

7.2 Data Controller – Council remains Data Controller.

7.3 Confidentiality – Sensitive data must not be shared.

8. Accuracy and Reliability

All outputs must be verified by a member of staff before the document is used. A document should not be used without a member of staff first checking the validity of the document. For council policies and other official documents, the council will review and vote on the document before its use at a council meeting.

AI must not be relied upon as sole source.

Legislation must be checked.

9. Procurement and Use of AI Tools

Risk assessment and DPIA required.

Must comply with ICO guidance.

Approval required from Council at a council meeting with a majority vote in favour.

10. Training and Awareness

Users must understand this policy and receive guidance if required. Staff will be given this policy upon joining the council and given time to read and understand it.

11. Monitoring and Compliance

Use may be monitored by council staff and Councillors without notice.

Misuse may lead to disciplinary action. See the relevant council policy for further information on how the council handles disciplinary action.

12. Relationship with Other Policies

- IT Policy
- Data Protection Policy

13. Review

Reviewed every 2 years or after changes/incidents.

14. References

- Information Commissioner's Office (ICO) guidance
- UK GDPR and Data Protection Act 2018
- UK Government AI guidance
- GBPC IT Policy (2025)
- GBPC Data Protection Policy (2026)

Appendix A: AI DPIA (Data Protection Impact Assessment) Template

Project Name:

Purpose:

AI Tool:

Data Used:

Lawful Basis:

Risks:

Mitigation:

Approval:

Appendix B: Councillor and staff AI Dos & Don'ts

DO:

- Check outputs
- Verify facts
- Use for drafting

DON'T:

- Input personal data
- Rely blindly
- Make decisions using AI

Appendix C: ICO Guidance on AI & Data Protection (UK)

1. Risk-Based Approach (Core Principle)

The ICO requires organisations to take a risk-based approach when using AI:

- Identify risks to individuals' rights and freedoms
- Assess likelihood and impact
- Apply measures to reduce those risks

2. Lawfulness, Fairness and Transparency

AI must comply with the core UK GDPR principles:

- Lawfulness → You must have a valid legal basis (e.g. public task)
- Fairness → AI must not produce unjust or discriminatory outcomes
- Transparency → People must understand how AI affects them

3. Purpose Limitation

- AI must only be used for specific, clearly defined purposes
- You cannot reuse data for unrelated AI processing without justification

4. Data Minimisation

- Only use the minimum amount of data necessary
- Avoid excessive data collection "just in case"

5. Accuracy (Including "Statistical Accuracy")

The ICO distinguishes between:

- Data accuracy (correct personal data)
- AI accuracy (correct predictions or outputs)

Organisations must:

- Test AI systems
- Monitor outputs
- Correct errors

AI cannot be relied on blindly

6. Transparency & Explainability

A major ICO requirement:

- You must be able to explain AI decisions to individuals
- Especially important if decisions affect people (e.g. services, complaints)

The ICO provides a full framework on:

- What explanations to give
- When explanations are required
- How to communicate them clearly

7. Accountability & Governance

Organisations must:

- Be able to demonstrate compliance
- Document decisions and processes
- Assign responsibility (e.g. Clerk / Data Officer)

Key expectations:

- Governance structures
- Audit trails
- Clear responsibilities

8. Data Protection Impact Assessments (DPIAs)

Data Protection Impact Assessment (DPIA) is a legally required risk-management document. It must be completed before adopting new technologies like Generative AI for drafting or reviewing council documents that could expose residents' or employees' personal data to privacy risks.

Using AI (such as ChatGPT, Copilot, or specialized AI tools) to handle council papers triggers an immediate requirement for a DPIA because:

- Innovative Technology: Regulators explicitly classify AI as an "innovative technology" that requires strict data safety filtering.
- Data Leakage Risks: Pasting un-redacted documents (like planning objections, staff grievances, or public emails) into public AI tools can accidentally leak sensitive data into the AI's public training dataset.

The ICO strongly emphasises DPIAs for AI:

You must carry out a DPIA when AI:

- Processes personal data
- Involves profiling or automated decision-making
- Presents high risk to individuals

DPIAs should:

- Identify risks
- Assess necessity and proportionality
- Define mitigation measures

9. Security Requirements

AI systems must ensure:

- Data is secure (encryption, access controls)
- Protection against breaches
- Secure storage and processing

10. Individual Rights

AI must respect people's rights under UK GDPR:

- Right to be informed
- Right of access
- Right to object
- Rights related to automated decision-making

People have rights not to be subject to solely automated decisions that significantly affect them.

12. Human Oversight

Although not always stated as a single rule, the ICO consistently expects:

- Meaningful human involvement (human in the loop, review documents)
- No fully automated decision-making in high-impact cases

Approved August 2026. Minute ref 26/98

Renewal date Aug 2028