



Lostwithiel Town Council

Artificial Intelligence (AI) Policy

Approved	14/04/2026
Minute ref:	381/25
Review:	Annually
Last Reviewed:	Apr-26
Next Review:	Apr-27

1. Introduction

Lostwithiel Town Council recognises that Artificial Intelligence (AI) technologies can support efficient, accessible, and high-quality public services. AI may assist with tasks such as drafting documents, summarising information, analysing feedback, and improving accessibility. However, AI must be used safely, transparently, and in a way that protects residents, upholds democratic accountability, and complies with all legal and regulatory obligations. AI can help, but people stay in charge. Staff must always check and approve anything AI produces.

This policy forms part of the Council's internal control environment and supports compliance with NALC's Annual Governance and Accountability Return (AGAR) – Assertion 10 on risk management, cybersecurity, and data protection.

1. Purpose

This policy establishes a clear framework for the responsible, lawful, and transparent use of AI by:

- Councillors
- Employees
- Contractors
- Temporary staff
- Consultants

It ensures AI use aligns with NALC model policies, the Council's Standing Orders, Financial Regulations, Information & Data Protection Policy, and the Local Government Transparency Code.

2. Scope

This policy applies to:

- AI tools directly used by staff
- AI features embedded within software platforms
- Any system that uses machine learning, natural language processing, or automated analysis

It covers all council services, administrative functions, communications, and public-facing outputs.

3. Guiding Principles

The Council's use of AI must be:

a) Transparent

Where AI has materially contributed to public-facing content, this must be clearly acknowledged.

b) Ethical and Inclusive

AI must not be used in ways that discriminate, mislead, or reinforce bias. Outputs must be fair, proportionate and accessible.

c) Human-Centred

AI may assist with tasks, but it will not replace human judgement. Officers and Councillors remain responsible for reviewing and approving AI-generated content.

d) Compliant within Legal Framework

AI use must comply with all relevant legislation, including UK GDPR, the Data Protection Act 2018, the Human Rights Act 1998, the Equality Act 2010, the Freedom of Information Act 2000, Public Sector Bodies (websites and Mobile Applications) Accessibility Regulations 2018 and intellectual property regulations.

e) Environmentally Responsible

The Council will consider the environmental impact of AI systems, including energy use and sustainability.

f) Consistent with NALC Governance Standards

AI use must support, not undermine, the Council's statutory duties, democratic processes, and internal controls.

5. Definition of AI

AI refers to computer systems capable of performing tasks that typically require human intelligence, including:

- Machine learning tools
- Generative AI
- Natural language processing systems
- Automated decision-making tools

6. Opportunities and Benefits

When used safely and appropriately, AI tools may offer benefits including:

a) Service Enhancement

- More efficient service delivery
- Better use of council resources
- Improved accessibility

b) Operational Efficiency

- Automate routine administrative tasks
- Analysis of unstructured data
- Support for decision-making
- Cost reduction

c) Staff Support

- Assistance with research and information gathering
- Creative problem-solving
- Professional development

7. Risks

All systems present risks including:

- Bias
- Inaccuracy
- Copyright /IP Risk
- Lack of auditability
- Public trust concerns
- Cybersecurity vulnerabilities
- Legal and compliance risks
- Reputational and financial consequences

8. Risk Assessment and Categorisation

Unacceptable Risk (Prohibited)

Completely prohibited (e.g., social scoring, subliminal manipulation, automated decision-making affecting individuals).

High Risk (Prohibited unless approved)

Generative AI tools fall into this category by default, any tool processing personal data, tools influencing decisions.

Limited Risk (permitted with oversight)

Examples: chatbots, transcription tools, productivity assistants.

Minimal Risk

Low-impact tools such as grammar checkers, autocomplete, spam filters.

Generative AI Clarification

Generative AI may be used only when:

- The tool is explicitly approved and listed in Appendix B
- The use case is low-risk (drafting, summarising, idea generation)
- No personal or sensitive data is entered
- A human reviews all outputs

9. Responsibilities

The Council

- Ensures the policy is fit for purpose and regularly reviewed
- Approves significant AI implementations
- Ensures compliance with NALC governance standards

The Town Clerk

- Ensures compliance with this policy
- Provides training and awareness
- Oversees performance reporting
- Determines whether a DPIA is required
- Maintains the AI Register (Appendix B)

All Staff, Councillors, and Users

- Must adhere to this policy
- Must follow Appendix A (Guidance Note)
- Must report incidents immediately

10. Confidentiality and Permitted Use

a) Prohibited Actions

AI must not be used for:

- Making, automating, or influencing decisions affecting individuals
- Surveillance, biometric analysis, or facial recognition
- Generating or disseminating misinformation
- Entering confidential, sensitive, or personal data into public AI tools
- Drafting responses to FOI requests
- Any use that undermines democratic decision making
- Any use without human review

b) Permitted Use

- Council-approved AI tools
- Research and general information gathering
- Transcription and meeting recording
- Drafting content (with human review)

c) AI Tool Approval Process

1. Staff member submits proposal
2. Risk assessment completed
3. DPIA considered
4. Council approval for significant tools
5. Tool added to Appendix B

11. Public & Internal Transparency

Public & internal documents containing AI generated content must include:
“This document includes content generated with the assistance of Artificial Intelligence and reviewed by Council Officers.”

12. Copyright and Intellectual Property

AI tools must not be used to reproduce or generate copyrighted material without permission. Seek advice from the Town Clerk where unclear.

13. Monitoring and Review

- This policy will be reviewed annually or sooner if legislation changes or new risks emerge.
- AI use forms part of the Council's internal audit and assertion 10 compliance
- Audit trails must record when AI has been used in document creation
- Breaches may result in restrictions on AI use or disciplinary action.

14. Procurement and Vendor Requirements

When procuring AI-enabled systems, the Council must ensure:

- UK GDPR compliance
- Clear information on training data, security, and retention
- Contractual protections
- Auditability and transparency
- Accessibility compliance

14. AI Incident Reporting Procedure

An AI incident includes:

- Personal data entered into an unauthorised AI tool
- Harmful, biased, or misleading AI output
- Unpredictable system behaviour
- Security vulnerabilities
- Breaches of this policy

Reporting Steps

1. Immediate notification to the Town Clerk
2. Stop using the AI tool
3. Contain and secure affected data
4. Assessment by Town Clerk
5. Documentation of incident
6. Follow-up actions including training or policy updates

Guidance Note: Using Artificial Intelligence (AI) in Council Work

Purpose of this guidance:

To help Councillors, staff, and contractors understand how to use AI tools safely, responsibly, and effectively in line with the Council's Artificial Intelligence Policy.

1. What this guidance is for

This note explains:

- When AI tools can be used
- What you must avoid
- How to stay compliant with data protection rules
- How to label or acknowledge AI-generated content
- Who to speak to if you're unsure

It is not a technical manual — it's a practical "how-to" for everyday council work.

2. What counts as AI?

Common forms of AI technology include:

- machine learning tools (e.g. predictive analytics)
- generative AI (e.g. ChatGPT, Copilot, Claude)
- Natural Language Processing systems (e.g. virtual assistants, chatbots)
- automated decision-making tools

If you're unsure whether something is AI-driven, assume it is and follow this guidance.

3. When you can use AI (see Appendix B for current approved list):

AI can be helpful for:

- Drafting reports, letters, minutes, or publicity materials (with human review)
- Summarising long documents
- Generating ideas or alternative wording
- Analysing survey responses or community feedback
- Improving accessibility (e.g., translation, transcription)
- Supporting routine administrative tasks

IMPORTANT:

AI can *assist* your work, but it must ***never replace*** your judgement. You are responsible for checking and approving anything AI produces.

4. When you must not use AI

Do not use AI for:

- Making decisions that affect individuals (e.g., complaints, grants, enforcement)
- Entering personal, confidential, or sensitive information
- Surveillance, monitoring, or facial recognition
- Anything that could mislead, misinform, or cause reputational harm
- Drafting responses to Freedom of Information requests
- Creating content that will be published without human review

If in doubt, ask the Town Clerk before proceeding.

5. Data protection: the golden rules

To comply with UK GDPR and the Data Protection Act:

- **Never** enter names, addresses, emails, phone numbers, or any identifiable information into public AI tools.
- **Never** upload documents containing personal data.
- **Never** use AI to process complaints, HR matters, safeguarding issues, or disciplinary information.
- **Always** check whether an AI tool is secure before using it for internal work.

If you're unsure whether something counts as personal data, treat it as personal data.

6. Labelling AI-generated content

If AI has contributed significantly to a public-facing document (e.g., a press release, website text, consultation summary), include a simple acknowledgement such as:

"This document includes content generated with the assistance of Artificial Intelligence and reviewed by Council officers."

Internal drafts **do not** need labelling.

7. Reviewing AI-generated content

Before using AI-generated text, always:

- Read it carefully
- Check facts and figures
- Ensure the tone is appropriate for a local council
- Remove any assumptions, invented details, or inaccuracies
- Make sure it reflects Council policy and local context

AI can sound confident even when it is wrong — your review is essential.

8. Training and support

- The Town Clerk oversees AI use and can provide guidance.
- Training will be offered when new tools or processes are introduced.
- Councillors and staff should ask for help if they are unsure how to use AI safely.

9. If something goes wrong

If you think AI has been used incorrectly — for example, personal data was entered into a public tool — report it immediately to the Town Clerk.

Early reporting helps minimise risk and ensures compliance with data protection law.

10. Keeping this guidance up to date

This guidance will be reviewed alongside the AI Policy, or sooner if:

- Legislation changes
- New risks emerge
- The Council adopts new AI tools

AI Register

Tool Name	Purpose	Risk (Unacceptable / High / Limited / Minimal)	Conditions of use	Review date
Microsoft Copilot	Drafting, summarising & idea generation	Limited risk	No personal data; human review required	12 months
Otter.ai	Meeting transcription	Limited risk	Audio only; no sensitive meetings	12 months
Grammarly	Grammar and spelling assistance	Limited risk	No personal data	12 months
Google translate	Accessibility support	Limited risk	Not for personal data	12 months
Zoom transcription	Meeting transcription	Limited risk	Not for confidential sessions	12 months

Tools listed must be reviewed annually and approved by the Town Clerk

Appendix C – DPIA Trigger List for AI

A **Data Protection Impact Assessment (DPIA)** is required when an AI tool:

- Processes personal data
- Profiles individuals
- Influences decisions
- Uses large or unstructured datasets
- Monitors behaviour
- Uses biometric or sensitive data
- Is supplied by a vendor with unclear data practices
- Is used for a new purpose
- Presents risk of bias or discrimination
- Is classified as High or Limited Risk