



WESTON-SUPER-MARE TOWN COUNCIL

Artificial Intelligence (AI) Policy

History of Policy Changes

Date	Version	Author	Origin of Change e.g. change in legislation	Changed by
July 2026	V1	H Morton (DoFR)	New policy and legislation	
August 2026	V2	H Morton (DoFR)	Consultation feedback and governance review	

This policy applies to Weston-super-Mare Town Council

Date policy adopted	August 2026
Review cycle	Annually, and following material trigger events
Review date	12 months from V2 adoption

Contents

1. Introduction.....	4
2. Use of AI	4
3. Governance Requirements for Using AI	5
4. Supplier/Vendor	6
5. Copyright Considerations	6
6. Accuracy of AI Output	7
7. Confidentiality	7
8. Disclosure and Transparency.....	7
9. Integration with Other Tools	7
10. AI Risks	8
11. Compliance with Legal and Regulatory Requirements	8
12. Business Impact Analysis and Discrimination	8
13. Security.....	8
14. Data Sovereignty and Protection	9
15. Training and Awareness	9
16. Compliance.....	9
17. Review	10

1. Introduction

This policy establishes the governance framework for the responsible, lawful, secure, fair and transparent use of Artificial Intelligence (AI) by Weston-super-Mare Town Council (the Council).

- 1.1 The Council recognises that AI can help staff and Councillors work more efficiently, improve accessibility and support better services. AI must be used responsibly to protect people, Council information, public trust and democratic accountability.
- 1.2 The Town Council is committed to taking a risk-based approach to the implementation and use of AI. This means:
 - Assessing the risks to the rights and freedoms of individuals that may arise when using AI
 - Implementing appropriate and proportionate organisational and technical measures to mitigate these risks.
 - Ensuring that a named member of staff or authorised decision-maker remains responsible for the work, decision, communication or service supported by AI.
- 1.3 AI is an assistive tool. It does not replace human judgement, responsibility or accountability. Staff and Councillors remain responsible for decisions, actions and communications undertaken with the assistance of AI.
- 1.4 This policy applies to employees (including temporary and agency staff), Councillors, contractors, agents, volunteers, suppliers and any other person using AI for, or on behalf of, the Council.
- 1.5 This policy applies to AI tools and AI features used for Council business, including assistants, chatbots, content generation, transcription, summarisation and systems that support recommendations or decisions.
- 1.6 This policy should be read alongside the Council's data protection, information security, records management, information sharing, retention, procurement, HR, equality, complaints and communications requirements. Where another Council policy sets a higher standard, the higher standard applies.
- 1.7 This policy sets out the Council's rules, responsibilities and minimum requirements for using AI. Detailed technical instructions will be kept in supporting Council guidance and procedures.

2. Use of AI

- 2.1 The use of AI solutions/technologies should always support the Town Councils vision, priorities and values.
- 2.2 Council use of AI must be lawful, fair, transparent, proportionate, secure and subject to meaningful human oversight. AI must support, not replace, the judgement of staff or Councillors.
- 2.3 Public-facing or significant AI uses must consider transparency, public confidence and whether resident, stakeholder or Member engagement is appropriate before implementation.
- 2.4 Before a new AI use is introduced, the responsible manager or Business Owner must consider the main risks and requirements, including data protection, security, procurement, copyright, confidentiality, accuracy, equality, records, oversight and links to other systems.

- 2.5 AI services should have logging and auditing capabilities appropriate to the risk and intended use.
- 2.6 AI must not make a final Council decision that has a significant effect on a person's employment, rights, access to services, complaint or grant outcome, safeguarding position or other significant interests, unless the law allows it and the Council has specifically approved the use with appropriate safeguards.
- 2.7 Without specific prior approval, AI must not determine, score or rank people for recruitment, appointment, dismissal, disciplinary action, performance management, redundancy, grant awards, complaint outcomes, safeguarding decisions or similarly significant Council decisions.
- 2.8 AI may assist with administrative or preparatory work in restricted areas only where the approved tool/use case permits it and a responsible human independently reviews the work and makes the decision.
- 2.9 AI must not be used to impersonate another person, fabricate evidence, create misleading Council records, make deceptive public communications, or bypass professional advice, statutory decision-making requirements, Council delegations or committee responsibilities.

3. Governance Requirements for Using AI

- 3.1 Any stakeholder looking to use or implement an AI solution/technology must understand the Council policies and procedures relevant to that use. As a minimum this includes:
 - Data Protection Policy
 - Corporate Information Security Policy
 - Records Management Policy
 - Information Sharing Policy
 - Corporate Information Retention Schedule
 - Procurement requirements and Financial Regulations
 - Equality, HR, complaints and communications requirements where relevant
- 3.2 No new AI tool, AI-enabled feature, material integration or materially new AI use case may be used for Council business until it has completed the Council's proportionate approval process.
- 3.3 Approval of an AI product does not amount to approval for every possible use of that product. A materially new or changed use may require further assessment and approval.
- 3.4 Each organisational AI use must have a named Business Owner. The Business Owner is responsible for ensuring that the use remains within its approved purpose, lawful, proportionate and secure, and that appropriate human oversight is maintained.
- 3.5 The risks associated with a proposed AI use must be assessed and managed. A proportionate AI Risk Assessment must be completed and a Data Protection Impact Assessment (DPIA) must be completed where required by data protection law or Council procedure.
- 3.6 As a minimum, the relevant manager or Business Owner must consult ICT and data protection support where appropriate before implementation.

Procurement, HR, legal, equality or other specialist advice must also be obtained where the use requires it.

- 3.7 Final approval for an organisational AI tool or higher-risk use must be given by the Town Clerk or a senior officer formally delegated for that purpose, following completion of the required checks. The Council's Scheme of Delegation and procurement rules continue to apply.
- 3.8 The Town Clerk, or a senior officer acting under delegated authority, may suspend or prohibit an AI tool or use immediately where there are reasonable concerns about legality, data protection, security, accuracy, discrimination, public safety, reputation or other material risk.
- 3.9 The Council will keep a central AI Register of approved organisational AI tools and significant uses. It will record what is approved, why it is used, who is responsible, any restrictions or conditions, the relevant assessments and approval, and when the use is due for review.
- 3.10 Register entries and significant AI uses must be reviewed at least annually and sooner following a significant incident or material change to the system, supplier terms, data use, integration or approved purpose.

4. Supplier/Vendor

- 4.1 Where the Council procures or subscribes to AI solutions/technology, the responsible officer must ensure proportionate supplier and procurement due diligence is completed before approval, with input from the relevant Information Asset Owner, senior management, ICT, data protection and other specialists as appropriate.
- 4.2 Checks must be proportionate to the proposed use. They should cover where Council data is stored and processed, how long it is kept, whether it is used to train or improve AI models, who can access it, any subcontractors or international transfers, security and incident arrangements, intellectual property, significant service changes, and what happens to Council data when the service ends.
- 4.3 Contracts and purchasing decisions must comply with the Council's Financial Regulations, procurement rules and applicable public procurement law. Approval of a supplier does not remove the Council's responsibility to assess the particular AI use case.
- 4.4 Where a supplier materially changes its model, data practices, terms, integrations or security arrangements, the Business Owner must consider whether reassessment or reapproval is required.

5. Copyright Considerations

- 5.1 Council use of AI must comply with the Copyright, Designs and Patents Act 1988 and other applicable intellectual property rights, including database rights, trade marks and confidential information.
- 5.2 AI must not be used deliberately to generate or reproduce material that infringes the intellectual property rights of others. Users must not assume that AI-generated material is free of copyright or licensing restrictions.
- 5.3 Before significant AI-generated material is published or used commercially, the responsible person must consider whether there are ownership, attribution or licensing issues that need specialist advice.

- 5.4 Where there is material uncertainty about ownership, licensing or infringement risk, legal or other appropriate specialist support must be obtained before use.

6. Accuracy of AI Output

- 6.2 If the Town Council has any doubt about the accuracy of AI output then AI solutions/technology should not be used.
- 6.4 The fact that AI produced or recommended an output does not transfer responsibility to the technology. The person who approves, relies upon, communicates or acts on the final output remains accountable for it.
- 6.5 AI-generated legal, financial, HR, employment, procurement, health and safety or other specialist professional advice must not be treated as authoritative or relied upon as the sole basis for Council action. Material advice must be verified by an appropriately qualified or authorised person.
- 6.6 For significant or high-impact AI applications, the Business Owner must ensure appropriate periodic testing and accuracy review, including review after material changes or recurring errors.

7. Confidentiality

- 7.1 Personal, confidential, commercially sensitive or otherwise non-public Council information must not be entered into unapproved public or consumer AI services.
- 7.4 Users must only enter information that is needed for the approved purpose and allowed for that service. Personal information should be kept to a minimum and anonymised or pseudonymised where possible.
- 7.5 Special category personal data, criminal offence data, safeguarding information, confidential HR or legal material, security credentials, payment information and other particularly sensitive information must not be entered into AI unless the specific use is authorised and the necessary data protection and security safeguards are in place.
- 7.6 Any processing of personal data using AI must comply with the UK GDPR and Data Protection Act 2018, as amended, and with the Council's Data Protection Policy.

8. Disclosure and Transparency

- 8.1 The Council will be open about significant uses of AI where this is needed for public trust, understanding, or to meet legal or regulatory requirements.
- 8.2 Disclosure should normally be considered where AI interacts directly with residents; materially contributes to public-facing information; materially influences a Council decision; analyses information about an individual; or is used in a context where knowledge of AI involvement is important to accountability.
- 8.3 Routine assistance such as brainstorming, spelling, formatting or low-risk drafting will not necessarily require a public AI statement where a human has fully reviewed and taken responsibility for the final content.
- 8.4 Where a disclosure statement is appropriate, it should be clear and proportionate. For example: "This content was produced with assistance from an approved AI tool and has been reviewed by the responsible Council

officer/author. Responsibility for the final content remains with the Council decision-maker or author."

9. Integration with Other Tools

- 9.1 AI integrations, plugins, agents, connectors and APIs can extend an AI service's access to Council information and systems and must therefore be specifically approved before use.
- 9.4 Staff and Councillors must not enable unapproved plugins, agents, connectors, integrations or similar functions that could extend an AI service's access to Council information or systems.
- 9.5 Where AI is integrated into a public-facing or decision-support service, the responsible human owner must ensure that users can report concerns and that the limitations of the service are understood and communicated where relevant.

10. AI Risks

- 10.1 The use of AI carries inherent risks. Before an AI solution/technology or materially new use is implemented, a proportionate AI Risk Assessment must be completed and a DPIA undertaken where required.
- 10.2 Each new AI project or significant use must be assessed on its own circumstances, including the information involved, who may be affected and how the output will be used. Approval of the AI product alone is not enough.
- 10.5 The Council must ensure risks are reviewed throughout the life of the use and must seek reassessment or reapproval where circumstances materially change.

11. Compliance with Legal and Regulatory Requirements

- 11.1 **Council use of AI must comply with all applicable law and Council policy. Depending on the use case, relevant legislation includes:**
 - **UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended, including relevant changes made by the Data (Use and Access) Act 2025.**
 - **Equality Act 2010, including the Public Sector Equality Duty.**
 - **Human Rights Act 1998.**
 - **Freedom of Information Act 2000 and, where applicable, the Environmental Information Regulations 2004.**
 - **Copyright, Designs and Patents Act 1988 and other applicable intellectual property law.**
 - **Procurement Act 2023 and associated regulations where applicable to AI-enabled goods and services.**
- 11.2 Where AI processes personal data, the Council must have a lawful basis, be clear about how the data is used, protect people's data rights, build data protection into the use from the start, and complete a DPIA where required.
- 11.3 Where an AI system is used in relation to a significant decision about a person, the Council must ensure that any involvement required by law is genuine. The decision-maker must be able to understand, question, influence, amend or reject the AI-supported outcome rather than simply approve it automatically.

12. Business Impact Analysis and Discrimination

- 12.1 The Council must take reasonable steps to identify and mitigate risks of unfairness, bias and discrimination before, during and after deployment of AI. Reviewers must not assume that an AI output is neutral or objective.
- 12.5 The responsible reviewer must actively consider whether an output reflects inappropriate assumptions, stereotypes, omissions or unequal treatment and must challenge, amend or reject it where necessary.

13. Security

- 13.1 The Town Council is committed to protecting the confidentiality, integrity and availability of its data.
- 13.2 AI services must be checked for security before they are approved. The responsible officer must seek appropriate ICT and data protection advice and make sure the safeguards match the type of information involved and the level of risk.
- 13.4 Where personal or confidential information is processed, the responsible officer must consider data minimisation, anonymisation or pseudonymisation and ensure appropriate access controls, encryption and other safeguards are applied in accordance with Council security requirements.
- 13.5 The Council must understand how the service protects Council information, deals with incidents and supports business continuity. Independent security assurance or certification should be considered where the level of risk justifies it.
- 13.6 Suspected weaknesses or security concerns must be reported promptly and may result in immediate suspension of the relevant AI service or integration pending investigation.

14. Data Sovereignty and Protection

- 14.1 Before approving an externally hosted AI service, the Council must know where Council information is processed and stored, how any international transfers are protected, and how long the supplier keeps the data and how it is deleted.
- 14.2 Where personal data may be transferred outside the United Kingdom, the Council must ensure that the transfer complies with applicable UK data protection law and that appropriate safeguards are in place. The Council will always check where a provider's servers are based so that it understands where personal data is being held and processed.
- 14.3 The supplier assessment must also establish, where relevant, whether Council prompts, uploaded files or outputs may be retained, accessed by the supplier or subcontractors, or used to train or improve models, and whether those arrangements are acceptable for the approved use.
- 14.4 If the Council cannot get satisfactory information about where data is held, transferred, kept, deleted or used by the supplier, the service must not be approved until appropriate data protection and ICT advice has been obtained.

15. Training and Awareness

- 15.1 Staff and Councillors must receive appropriate guidance or training before using Council-approved AI where required by the service, role or risk classification.
- 15.3 Completion of mandatory AI training should be recorded.
- 15.4 Managers are responsible for ensuring that users in their area understand the approved purpose and controls and remain competent to exercise meaningful judgement and oversight.

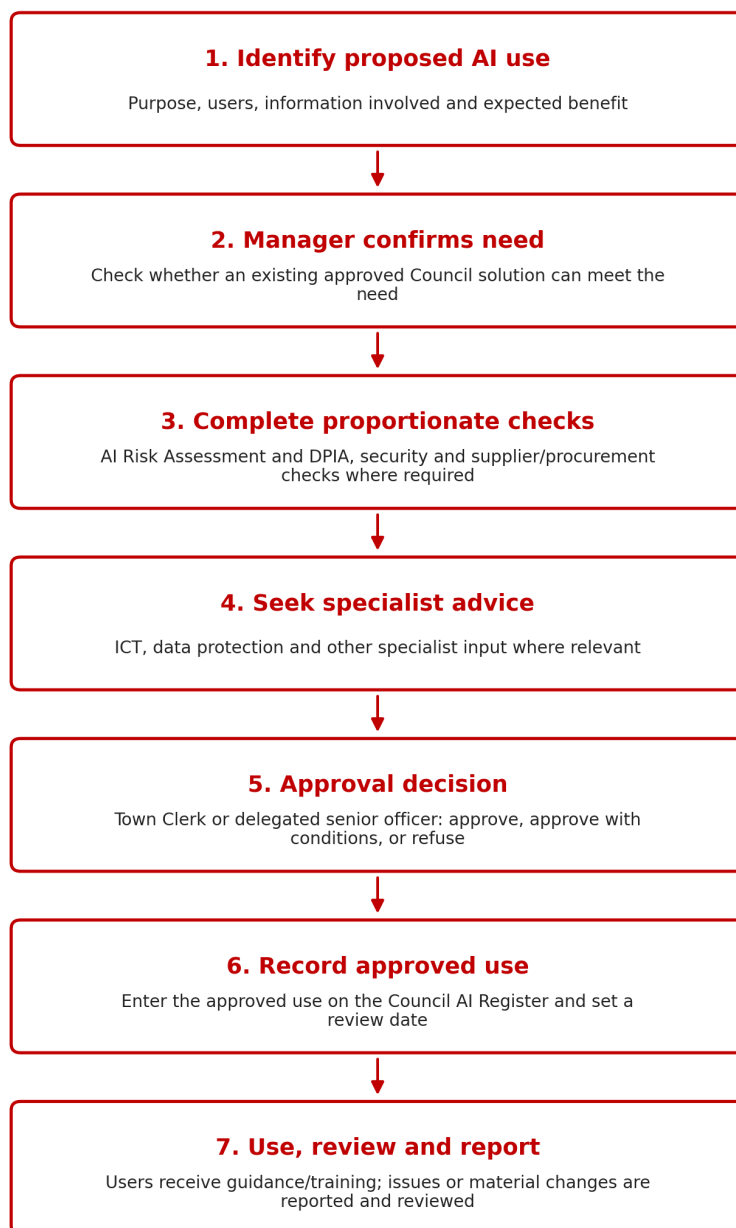
16. Compliance

- 16.1 This policy applies to all Town Council uses of AI solutions/technology.
- 16.2 Staff and Councillors must promptly report suspected AI incidents, significant mistakes or policy breaches through the Council's established reporting route and to the relevant manager. All data protection or security incidents must be reported to the CEO/Town Clerk in the first instance without delay and then referred to the appropriate data protection/ICT support as required.
- 16.3 An AI incident may include a data or security breach, discriminatory treatment, misleading public information, an inappropriate decision, a serious factual error, a copyright or confidentiality breach, unauthorised AI use, or another serious breach of this policy.
- 16.4 Where necessary to protect people or the Council, the Town Clerk or delegated senior officer may require immediate suspension of the relevant AI tool, integration or use case pending investigation.
- 16.5 The Council must respond to incidents in proportion to the risk. This may include stopping the use, keeping relevant evidence, correcting records or communications, making any required reports or notifications, learning from the incident and deciding whether the AI use can restart.
- 16.8 The fact that an AI tool produced, suggested or recommended something does not remove or reduce the responsibility of the person who chooses to use, approve or act upon it.
- 16.9 Failure to comply with this policy may result in access being withdrawn and, where applicable, disciplinary, Member, contractual or other Council procedures being considered.

17. Review

- 17.1 This policy will be reviewed at least annually to reflect changes in AI, legislation, regulation and public-sector guidance.

Appendix A - AI approval workflow



The level of assessment and approval should be proportionate to the intended use and the information involved.