Artificial Intelligence (AI) Policy

2025

We see the potential for AI to **create efficiencies, improve our services and connect with our communities in new ways.**

Tewkesbury
Borough Council

Contents

Tewkesbury
Borough Council

1.0 Introduction

As technology continues to evolve, the adoption of Artificial Intelligence (AI) is increasing rapidly. At Tewkesbury Borough Council, we see the potential for AI to create efficiencies, improve our services and connect with our communities in new ways. Enhancing our ability to fulfil our Council Plan vision of 'supporting people, strengthening communities', while paving the way for a more resilient future.

This policy outlines our approach to using AI responsibly and ethically. It has been developed to complement and reinforce the aims of our Digital Strategy, ensuring consistency in how AI technology is adopted and governed. Our Digital Strategy already focuses on using technology to make our services more efficient and accessible; and through the responsible use of AI, there are opportunities to provide faster responses, better insights and improved services to our communities.

2.0 Purpose

The purpose of this policy is to provide a framework for the ethical adoption, deployment, and management of approved AI systems and tools used across the council. Ensuring alignment with the council's values, legal obligations, and strategic goals.

3.0 Scope

This policy applies to all Tewkesbury Borough Council employees (including temporary staff), councillors, contractors, consultants and all other third parties or partner organisations using or sharing the council's information. They will be referred to throughout the policy as 'users.'

All AI systems and tools fall within the scope of this policy. These include, but are not limited to:

- Large Language Models (LLMs)
- Machine learning algorithms
- Generative AI, for example Copilot
- Natural Language Processing (NLP)
- Robotic Process Automation (RPA)
- Predictive analytics tools.
- Other similar tools.

Adherence with this policy is mandatory and the approval mechanisms, outlined at page 6, must be followed prior to the use of any AI tools.

4.0 What is AI?

AI refers to computer systems and software that perform tasks that usually require human thinking. This includes things like understanding language, recognising images, reasoning, prediction and making decisions. AI can help humans solve problems and perform tasks. Common AI functionalities include:

- **Large Language Models (LLM):** an AI model trained on vast amounts of text data such as books, articles and websites to understand, generate and manipulate human language.
- **Machine Learning (ML):** systems that learn and improve autonomously from data.
- **Generative AI:** tools that create text, images, code, or media content based on input.
- **Natural Language Processing (NLP):** systems that analyse, generate, or interact using human language.
- **Robotics and automation:** technologies that perform repetitive tasks without human intervention.
- **Predictive Analytics:** AI-driven insights that forecast outcomes or trends using historical data.

These AI tools can work by themselves or can be added to other software platforms. They can help improve operations, automate tasks, and provide helpful insights.

5.0 Policy principles

In 2018 the council signed the Ministry of Housing, Communities and Local Government (MHCLG) Local Digital Declaration - a shared ambition with other local authorities and organisations, aimed at transforming local public services through digital technology.   Together with our own commitment to the ethical, secure, and transparent deployment of AI, we have eight core principles which will guide the declaration's use:

These principles underpin all AI-related activities:

1. **Accountability:** human oversight must accompany AI deployment. There must be clear processes and a review of outputs to ensure any impact on users is taken into consideration and reviewed.
2. **Accuracy and reliability:** AI outputs must be evaluated, fact-checked, and validated to avoid errors, inaccuracies, or misinformation.
3. **Continuous improvement:** AI systems should undergo regular evaluation, updating, and monitoring to align with technological advancements and the council's digital priorities.
4. **Data privacy and security:** personal, sensitive, or confidential data must be protected through compliance with UK GDPR, the Data Protection Act 2018 as well as the council's Data Protection Policy and ICT acceptable use policy.
5. **Environmental sustainability:** AI deployment must consider energy consumption, resource efficiency and overall environmental impact to support our continued commitment to reduce the council's carbon footprint.
6. **Ethical use:** AI should be developed and used in ways that promote the public good, operate within ethical frameworks, and respect human dignity and rights.
7. **Fairness and inclusivity:** one of our key values within the Council Plan is 'inclusive'. AI systems must therefore avoid biases, discrimination or exclusion against any group or individual. Measures must be taken to identify and mitigate algorithmic bias.
8. **Transparency:** another core value of the council is being 'open and honest'. AI systems must therefore be transparent, with processes and decision-making clearly documented. Users should be able to understand how decisions are made and the rationale behind outcomes.

6.0 Risks associated with using AI

The council recognises that the use of AI presents a range of potential risks. These include:

- **Data privacy:** AI systems can involve the use of datasets, sometimes including personal data, which can increase the risk of data breaches and violations of privacy rights for both personal and organisational data. Access controls and encryption must therefore be implemented to ensure compliance with legislative requirements under UK GDPR.
- **Bias and discrimination:** AI may, unintentionally, produce unfair or exclusionary outcomes impacting decision-making. Regular checks for bias must therefore be undertaken as well as Equality Impact Assessments to help address any equity issues.
- **Accuracy and misinformation:** AI-generated content or predictions which lack reliability or factual accuracy can lead to poor decision-making, financial loss and misleading users. The correct approval process must therefore be followed, as detailed in section 7 of this policy.
- **Legal and copyright issues:** AI systems may use or generate content based on copyrighted material without permission, raising risks around unauthorised use and intellectual property violations. Only tools from reputable providers, who disclose information about how their models were trained, must therefore be used.
- **Environmental impact:** AI systems can have significant energy consumption and contribute to carbon emissions. We will therefore invest in energy-efficient AI models and practices wherever possible.
- **Cybersecurity vulnerabilities:** AI systems may be vulnerable to malicious attacks, data breaches or system compromise. To address this, robust cybersecurity measures must be in place, including up to date software, secure system configurations and staff training on how to recognise and respond to potential threats.
- **Confidentiality:** AI tools may, unintentionally, expose personal or commercially sensitive content. Access to data must therefore be restricted to authorised users with strong anonymisation techniques applied as standard.

To mitigate these risks, all proposed AI use cases must undergo an appropriate risk assessment prior to deployment and be subject to ongoing monitoring throughout their use. This risk assessment must be documented and, where significant risks are identified, appropriate mitigating controls must be implemented.

Tewkesbury
Borough Council

7.0 What do I do if I want to use an AI software or system?

- Never download or use any AI software or system before the correct approval process has been followed.
- Prior approval must be obtained before the user uses AI, especially if the technology will involve the processing of personal data.
- The ultimate decision will be made by our Information Governance and Security Board.
- Appendix A provides a process flow chart detailing the approval process, which is also outlined below.

Employees - including temporary staff

Initial approval must be sought from the appropriate information asset owner, to assess whether using AI could be a consideration.

The project lead must then contact the Audit and Governance team via this email address governanceteam@tewkesbury.gov.uk to outline the proposal and confirm whether a similar software is already in use within the organisation for a comparable purpose. If such software exists and has already been approved, refer to the 'pre-approved process' in section 8 of this policy for further guidance.

If the request relates to a new use of AI, it will require approval from the Information Governance and Security Board (IGSB) once necessary due diligence has been conducted. Officers must be satisfied that its use is compliant with data protection and information security requirements.

The project lead must ensure that the checklist, at appendix B is completed and evidenced.

Councillors

Tewkesbury Borough Council councillors are required to contact the Audit and Governance team via this email address governanceteam@tewkesbury.gov.uk to discuss their proposal to obtain an AI software or system on their council device.

A member of the Audit and Governance team will then go through the necessary process in line with appendix A, whilst also ensuring appendix B is completed in conjunction with the Head of Democratic and Electoral Services, the councillor and a member of the IT and Cyber team.

Tewkesbury Borough Council

Contractors, consultants and all other third parties or partner organisations

The information asset owner will be required to ensure that any requests from contactors, consultants or other third parties or partner organisations are managed between the council and the user. These should be outlined in an appropriate data-sharing agreement and/or contract between the council and the user.

Any new requests for the use of AI must be brought to the council's attention for their records and approval before the implementation of the AI software or system can be purchased/used.

8.0 Pre-approved use

There are some cases where AI systems or software are already in place at the council, such as the use of the council's chat bot service.

A central register of authorised AI software and systems will be maintained by the Audit and Governance team, to keep track of approved AI tools and their use cases within the authority. A link will be available to view the register on the staff intranet.

The register will capture:

- **Name:** the name of the AI tool.
- **Provider:** the name of the organisation that provides the software/ system.
- **Function:** a brief description of what the tool does.
- **Approval date:** the date the tool was approved by IGSB.
- **Use case:** specific applications or scenarios where the tool can be utilised.
- **Compliance:** information on compliance and ethical considerations e.g. DPIA, EIA.

If the AI system or software you are wishing to use is already approved and on the register, you will need to raise a ticket via the IT and Cyber helpdesk requesting access to use the particular software.

We encourage AI for tasks that enhance productivity, insight, and service delivery, such as:

- Generating draft reports, presentations, and non-confidential correspondence.
- Summarising large datasets, trends, and documents for research or analysis.
- Improving customer support through AI-enabled chatbots and virtual assistants.
- Automating repetitive, manual tasks to improve operational efficiency.
- Supporting decision-making through predictive analytics and performance insights.

9.0 Unauthorised use of AI

Unauthorised use of AI, whether deliberate or inadvertent, should be reported as soon as discovered to the Audit and Governance team.

Users must not engage in unauthorised use of AI technology, this includes any illegal, unethical, or harmful activities such as generating misleading information, promoting violence, or infringing on intellectual property rights.

Deliberate breaches of this policy will be reported to the Chief Officer Group and may result in disciplinary action.

The council will not permit the use of personal data with AI tools or systems which input data to develop or train a public model. A public model is an AI system or algorithm that is made available for everyone to use, access, or build upon.

AI systems must not be used to write emails. All emails must be written by individuals, with AI permitted only to support with grammar correction and improving clarity for the reader.

10 Disclosure and transparency

Where content has been produced using AI, this must be identified as containing AI-generated information with the following disclosure statement:

“Note: This document contains content generated by Artificial Intelligence (AI). AI generated content has been reviewed by the [title of senior officer or team name] for accuracy and edited/revised where necessary. [Title of senior officer or team name] takes responsibility for this content.

Where systems are utilising AI to process personal data, this must be communicated via a service specific Privacy Notice, displayed on our website and linked where appropriate throughout the process.

11 Roles and responsibilities

We have established clear accountability for AI oversight within the council to ensure everyone understands their part in ensuring ethical, responsible, and compliant AI practices are delivered.

- **Chief Officer Group:** ensures AI is used in ways that align with the council's values, goals and legal obligations.
- **Information Governance and Security Board:** approves and/or refuses the use of AI and, where appropriate, challenges its use and monitor compliance.
- **Audit and Governance team:** oversees compliance with the Data Protection regulations whilst providing guidance on ethical use. Supports with the completion of Data Privacy Impact Assessments and monitors and responds to data privacy concerns relating to AI deployment. Maintains the central register of acceptable AI use cases approved by IGSB.
- **ICT and Digital team:** ensures system compliance with security standards and provides technical system support and guidance for AI operations.
- **Procurement team:** vets AI suppliers for ethical practices, data security measures, and legal compliance during acquisition processes.
- **One Legal:** provides advice in relation to intellectual property rights.
- **Information asset owner:** implements AI tools responsibly, ensuring that risks, ethical implications, and performance are managed throughout the lifecycle within their service areas.
- **All officers:** maintain awareness of AI usage policies, adhere to ethical guidelines, and report any issues, misuse, or security concerns promptly.

12 Digital exclusion

In some cases, AI technologies might be intended to be used by customers or service users which could impact on digital exclusion. As part of the council's Digital Strategy, it is important to recognise that we do not intend to 'channel shift' people - effectively forcing them to online channels or to use AI technology. We aim to deliver digital services that are so good, people prefer to use them when they can but can contact us using other methods should they wish.

When considering the use of AI technology, it is important for digital exclusion to be considered as part of the DPIA and Equality Impact Assessment, to ensure that alternatives are in place for those who experience digital exclusion and are therefore unable to access the benefits of the AI technology.

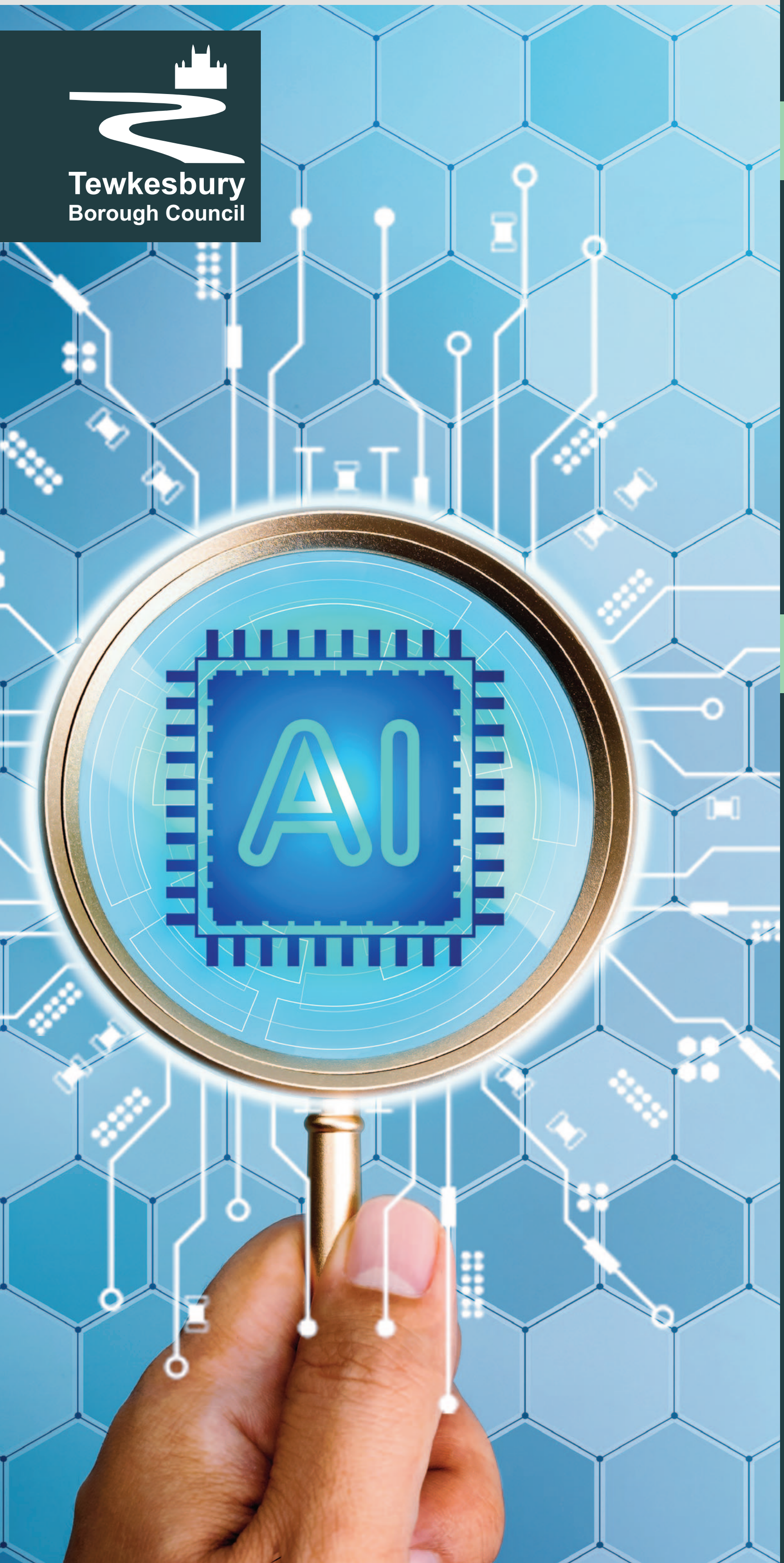
13 Procurement

When acquiring an AI system or product, it is essential to adhere to the approval steps outlined in Section 7 of this policy, as well as following the council's contract procedure rules, a statutory requirement under S135 Local Government Act 1972. This approach ensures transparency, compliance and the achievement of optimal value for money.

To discuss contract procedure rules and procurement requirements, please contact the Asset Management team- procurement@tewkesbury.gov.uk for advice.

14 Training and awareness

All staff and councillors are required to complete mandatory data protection and cyber security training and must ensure their knowledge remains up to date. This is essential for the safe, lawful and responsible use of AI and other digital technologies. Regular completion of training helps safeguard personal data, reduce risks and support compliance with legal and organisational requirements.



15 Monitoring and review

In line with the principles of continuous improvement, this policy will be reviewed annually and updated as necessary to ensure continued compliance with all application legislation, regulations and organisational polices.

In addition, the council's retention policies and AI privacy notices will be reviewed as part of the process, to ensure alignment with this policy.

16 Glossary

Artificial Intelligence (AI): a type of technology that allows computers or machines to do tasks that normally require human thinking, like learning, making decisions or understanding language.

UK GDPR: General Data Protection Regulation. A law in the UK that protects your personal information and gives you rights over how it is used, such as the right to access your data or ask for it to be deleted.

Data Protection Act 2018: the UK law that works alongside the UK GDPR to make sure people's personal information is handled properly and kept safe.

Algorithmic bias: when a computer programme or system makes unfair or incorrect decisions because the data it was trained on has built-in mistakes or unfairness.

Encryption: a way of scrambling information so that only someone with the right key or password can read it. It is used to keep data safe from hackers or accidental leaks.

Copyright: a legal rule that protects original creative work, so only the creator can copy, use or share it unless they give permission

Anonymisation techniques: methods to remove or change personal information in data so that individuals cannot be identified.

Information Governance and Security Board: an internal officer board overseeing the council's general information management, including compliance with all UK data protection legislation. It also ensures information and security risks are being properly assessed, controlled and mitigated in line with council policies and procedures. The board also provides governance and technical assurance for ICT related projects (including digital) and any hardware or software procurement.

Information asset owner: service managers and heads of service have been nominated as information asset owners for the information held within their service areas and are responsible for ensuring that their service areas can demonstrate compliance with current data protection legislation.

Intellectual property: refers to creations of the mind that can be legally protected. This can include inventions, creative works, trademarks and confidential business. Having intellectual property rights means that the creator has control over how their creations are used and how it can prevent others from using them within permission.

Data Protection Impact Assessment (DPIA): an assessment carried out before starting a project or introducing a new process involving the use of personal data to ensure due diligence and identify and risks to people's privacy.

Data protection officer: an internal officer at the council who ensures the organisation complies with data protection laws and regulations, such as GDPR. They are the point of contact for data protection authorities and individuals regarding data protection matters.

Privacy notice: a short explanation, often found on a website, that tells you what personal data is collected, why it is needed and how it will be used and protected.

Open AI: a company that builds advanced AI tools and systems, which can understand and respond to human language.

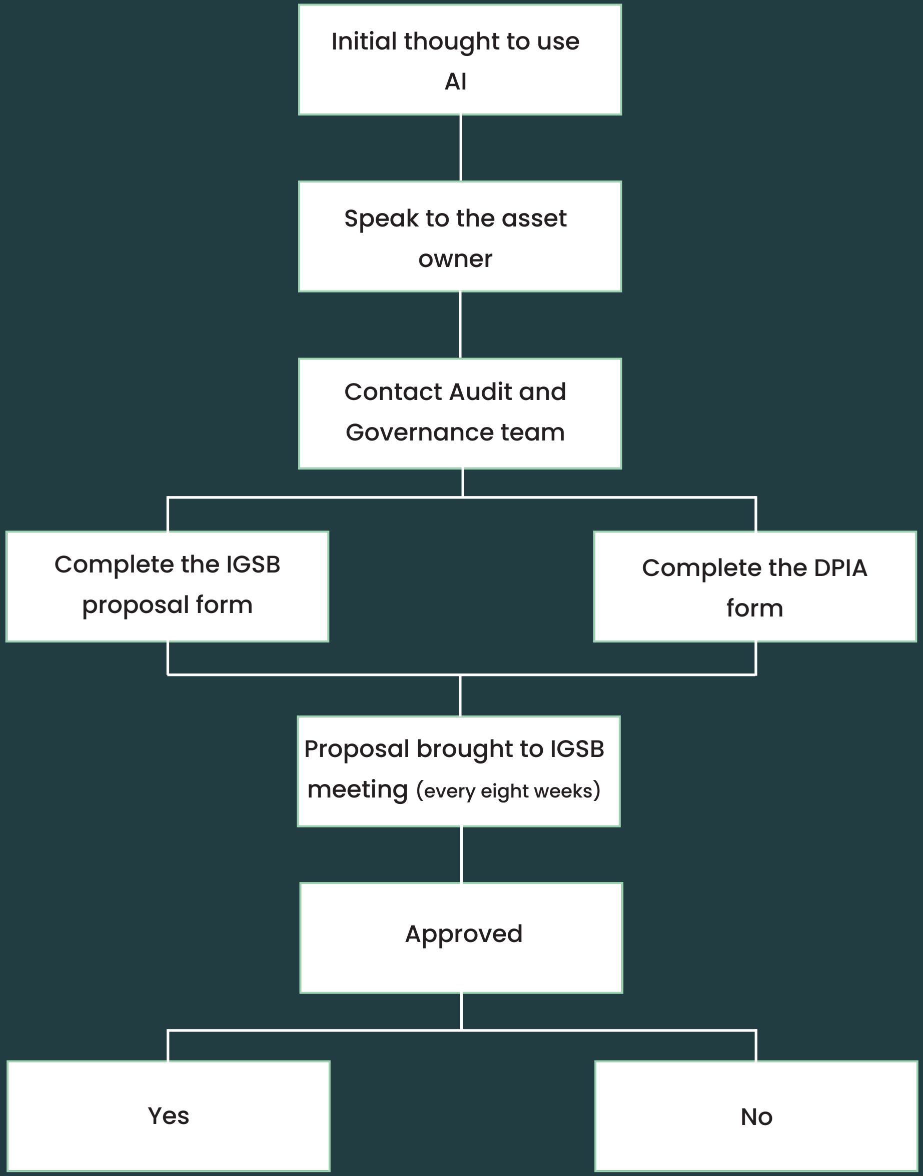
Microsoft Copilot: an AI assistant built into Microsoft tools (like Word and Excel) that helps users write, summarise, analyse data and more.

Data breach: when personal data is accidentally or unlawfully shared, accessed or stolen.

Public model: an AI system that's made available for anyone to use, often trained on large sets of publicly-available information.

Tewkesbury
Borough Council

Appendix A - approval process flow chart



Initial thought to use AI

Speak to the asset owner

Contact Audit and Governance team

Complete the IGSB proposal form

Complete the DPIA form

Proposal brought to IGSB meeting (every eight weeks)

Approved

Yes

No

Tewkesbury
Borough Council

Appendix B - approval and implementation checklist

Checklist before attending IGSB

- □ Speak to the information asset owner e.g. head of service, associate director or director of the service the software or system will be used for.
- □ Notify the council's Audit and Governance team of the intended use of AI, providing examples of use cases and outlining the benefits of its use.
- □ Complete the Information Governance and Security Board proposal template. This can be obtained from the staff intranet or from the Audit and Governance team.
- □ Complete a Data Protection Impact Assessment (DPIA), approved and signed by the relevant information asset owner for the data impacted by the proposed processing, and the council's Data Protection Officer (DPO). The DPIA shall address the risks involved in processing, together with mitigations which ensure legal and regulatory compliance.
- □ Ensure documentation containing the technical protections and security certification. IGSB shall assess this and if there are any doubts about the security of information input into AI tools or systems, this will not be approved.
- □ Information about a supplier's policies, practices, terms and conditions should be supplied to the Audit and Governance team for consideration by IGSB. Including where the data is being processed.
- □ Circulate completed DPIA and IGSB documents to the IGSB ready for discussions at their next meeting. Contact Audit and Governance team for the date of the next meeting.

Checklist following approval at IGSB

- □ If the AI involves the instruction of a supplier, contact the council's Procurement team. See section 13 of the AI policy.
- □ A detailed technical specification will need to be created, together with IT and Cyber team, Audit and Governance team. To ensure compliance and relevant instructions for the supplier are produced, it is important to ensure that they do not input data to develop and train a public model.
- □ Create and publish a privacy notice, a public document on the council's website (explaining how the council collects, uses, protects and handles personal data).
- □ Users should follow OpenAI's Safety Best Practices
- □ If required, create a project timeline for implementing the software/ system.
- □ Ensure adequate testing has been verified and approved by IT and cyber team.
- □ Provide relevant training for users, using the software/ system.
- □ Ensure the relevant maintenance/ licenses renewals are regularly scheduled.