Artificial Intelligence (AI) Policy

February, 2026

Information and Communication Technology (ICT) and Information and Data Governance teams

Stroud District Council
Ebley Mill
Stroud
GL5 4UB

Email: N/A
Website: https://www.stroud.gov.uk/
Telephone: 01453 766321

Document Responsibility		
Name	**Document title**	**Service**
Head of Technology	AI Policy	ICT

Document Version Control			
Date	**Version**	**Issued by**	**Summary of changes**
1st September, 2025	1.0	Head of Technology	N/A
16th October, 2025	2.0	Head of Technology	Updates following Member and SLT reviews
30th January, 2026	3.0	Head of Technology	Updates following Audit and Standards Committee review

Policy Review			
Updating frequency	**Review date**	**Person responsible**	**Service**
Annually or as required	January, 2027	Head of Technology	ICT

Document Review and Approvals		
Name	**Action**	**Date**
Information and Data Governance Manager	Review	September, 2025
SLT	Review	October, 2025
Audit and Standards Committee	Review	November, 2025

1 INTRODUCTION

1.1 Purpose

This policy sets out the guidelines and regulations that the Council will comply with to influence decisions and actions relating to Artificial Intelligence (AI), ensuring consistency, compliance with laws, and alignment with the Council's values and behaviours and strategic goals.

1.2 Background

Artificial Intelligence (AI) functionality, as defined in Appendix 1, is reshaping industries globally and offers transformative potential for the public sector. Used responsibly the technologies may provide the Council with opportunities that include:

- Streamlining operations
- Elevating service delivery
- Enhancing decision-making through data analysis
- Modernising communication with residents and stakeholders.

As with many emerging technologies, advancements bring ethical, legal, and operational challenges such as increased cyber security threats (Appendix 2), cultural change, cognitive offloading, and process integration that demand rigorous governance, oversight, and responsible use. This policy details how the Council intends to manage these opportunities and challenges in all its activities including delivery of the Council Plan.

Any AI usage at Stroud District Council must comply with national legislation and conform with industry best practice. As of October 2025, there is no specific UK regulatory legislation on the use of AI as the government wishes to encourage innovation (gov.uk 2023). Instead, it has developed 10 principles that should be applied (Appendices 3 and 4). The most relevant legislation is currently the EU AI Act 2024 (Appendix 5) and the new UK Data Use and Access Act 2025 which, among other things, expands the acceptable use of automated decision making and the use of personal data for scientific research purposes including AI.

As AI is a fast moving and complex subject Stroud District Council will continue to learn from other Local Authorities, National Government, and experts in the field to maintain ethical and practical rigor when considering any AI solutions. The speed at which AI is developing poses a significant risk for those wishing to regulate its use and this policy reflects current understanding. It will be reviewed as necessary and no less frequently than once per year.

This policy will be supplemented with practical officer guidance including policy controls hosted on internal systems which can be promptly updated to respond to changes in legislation, best practice, and Council decisions. Delegation to make minor changes to the policy in response to established best practice or legislation is granted to the Head of Technology.

1.3 Scope

This policy applies to the scope of AI technologies as defined in Appendix 1 and:

- All Council staff and employees, councillors, consultants, contractors, vendors, and third-party service providers engaged with Council-related activities
- AI tasks involving Council-owned systems, external platforms, or personally managed devices when used for Council business

- All AI processing of Council controlled data and data held on behalf of the Council by third parties. Data held by the Council and controlled by a third-party will only be subject to AI usage as agreed in any data sharing agreement or alternative agreement mechanism. The term 'data' includes data, documents, images and video
- The procurement of AI technologies, their development, implementation, and business operations including monitoring, evaluation, and decommissioning.

Compliance with this policy is mandatory for all.

2. CORE PRINCIPLES FOR AI ADOPTION

The Council is committed to the ethical, secure, and transparent deployment of AI. The following principles underpin its AI-related activities and must be followed when using AI technology:

- **Accountability**: The Council must ensure human oversight accompanies its AI development and deployment, ensuring that inputs, outputs, decisions, and potential impacts are subject to review
- **Accuracy and Reliability**: The Council must evaluate, fact-check, and validate its AI outputs to avoid errors, inaccuracies and bias, or misinformation. This is particularly important because AI operates on statistical probabilities and lacks true creativity, empathy and common sense. Hence, it can produce 'hallucinations' which appear correct but can be inaccurate. Audits of AI output must therefore be routinely completed where any process uses it to influence outcomes or decision making
- **Continuous Improvement**: The Council's AI systems must undergo regular evaluation, updating, and monitoring to align with technological advancements and Council priorities
- **Data Privacy and Security**: The Council must ensure personal, sensitive, or confidential data is protected through compliance with UK legislation and Council data policy (Information Governance Framework 2024). This includes completion of a bespoke Data Protection Impact Assessment
- **Environmental Sustainability**: The Council must ensure its AI deployments consider and, where possible, mitigate overall environmental impact. Where AI can provide increased efficiencies leading to lower carbon output, this should be recorded as part of the council's carbon accounting actions
- **Ethical and Legal Use**: The Council must ensure its use of AI promotes the public good, operates within ethical and legal frameworks, and respects human dignity and rights. All procurement and usage of AI must be legal and must consider the values of:
    - Respecting the dignity of individuals
    - Connecting with communities sincerely, openly, and inclusively
    - Caring for the wellbeing of all
    - Protecting the priorities of social values, justice, and public interest
- **Fairness and Inclusivity**: The Council must ensure its AI systems avoid perpetuating bias, discrimination, or exclusion. It must also ensure measures are

taken to identify and mitigate algorithmic bias. The completion of integrity and reliability audits will support this principle

- **Transparency**: The Council must ensure its AI systems are clearly documented, with processes and decision-making outcomes made understandable to stakeholders including how the Council complies with this policy. The Council must be transparent with stakeholders if their data, or any decisions made that impact them, have used AI output. This will be achieved by providing information through existing Council privacy notices, or where AI usage may significantly impact an individual, through alternative signposting.

  The Council must include an AI register on its main website to communicate where it is using AI technologies in the services it delivers for customers. This will specify:

  - Product name
  - Brief description
  - Service Lines using the technology
  - Date deployed.

  For general business content generated by AI technology authors must include a simple transparency statement that follows the text:

  > "Content generated/assisted using [AI Tool Name] (URL/Version) with the search prompt input by the author: '[Your Prompt Here]'.

3. PERMITTED and PROHIBITED AI TASKS

3.1 Permitted

The Council must only consider AI for tasks that enhance productivity, insight, and service delivery, including:

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

Each task must be assessed prior to procurement and deployment for security, data protection, ethics, environmental impact and value for money risks and reasonable mitigation measures put in place. Where identified risks cannot be managed, alternative solutions should be sought.

Permitted use must be agreed by the Head of Technology.

3.2 Prohibited

The Council must ensure its AI systems are not deployed for:

- Automated decisions lacking human oversight or accountability

- Generating content that knowingly uses intellectual property of others without licensing, violates ethical guidelines, or promotes misinformation
- Processing sensitive, personal, or commercially confidential data on unapproved platforms
- Tasks that conflict with Council policies and values, and legal obligations
- Any usage identified by the EU Act (Appendix 5) as being an unacceptable risk
- Any usage of personal data which conflicts with the requirements of data protection legislation.

4. AI-ENABLED FRAUD

The Council must protect itself from fraud attempts that are AI-enabled. These include:

- Recruitment Fraud (e.g. creation of fictitious or misleading CVs, covering letters, references, and social media profiles)
- Content fraud (e.g. the creation of fake invoices, receipts, contracts, or other paperwork).

The Council must maintain robust identification and verification processes across services to reduce the risk of AI fraud. It must also ensure officers and councillors are trained to spot materials that may be AI-generated and regular audits must be conducted to confirm appropriate checks are being performed.

Suspected fraud must be reported through the usual channels.

5.VENDORS

Most of the Council's AI solutions will be provided by third parties, and the Council procurement process must therefore ensure vendors specify whether they intend to use AI in their solution/service and that they can comply with the Council's policy and UK Government policy and guidance.

Where AI is part of a contracted service, the contract between the parties must include compliance stipulations including environmental sustainability commitments and should allow the Council to terminate should the vendor not comply at any point during the term of the contract.

6. ROLES AND RESPONSIBILITIES

The Council must establish clear accountability for AI oversight and alignment with this policy:

- **ICT and Information Governance teams**: Must be the gatekeepers to AI adoption in the Council by approving procurements, assuring development activities, conducting risk assessments and data protection reviews, and ensuring system compliance with appropriate standards and policies
- **Executive/Senior Management teams**: Must ensure AI aligns with Council strategy, regulatory requirements, and ethical principles while achieving organisational objectives
- **Councillors**: Audit and Standards Committee must receive periodic updates on AI use and compliance including selection of new and performance of existing products

- **Managers**: Must select and implement AI tools responsibly, ensuring that risks, ethical implications, and performance are managed throughout the lifecycle
- **Procurers:** Must vet AI vendors for Council policy compliance including ethical practices, data security measures, and legal compliance during acquisition processes. Must ensure cost-benefit assessment performed to evidence value exceeds downsides such as environmental impact
- **Sustainability team:** Must support officers to ensure that AI technologies align with the Council's values and practices regarding environmental sustainability
- **All Officers**: Must comply with the Council's AI and Data policies, adhere to ethical guidelines, and promptly report any issues, misuse, or security concerns.

7.TRAINING AND AWARENESS

To foster responsible AI usage, the relevant Council leads (section 6) must:

- Encourage staff and councillors to adopt a proactive, transparent approach to AI integration while maintaining vigilance for unintended consequences
- Promote awareness of AI's benefits, limitations, and associated risks
- Provide ongoing training for staff and councillors on AI ethics, bias detection (e.g. related to the nine protected characteristics (Equality Act 2010)), and legal compliance
- Educate on environmental sustainability considerations and mitigation strategies (e.g. by sharing information that explains how different types of AI requests correlate with consumption of resources such as electricity and water).

8. MONITORING, AUDITING and REVIEW

The Council service lines must ensure the operation of their processes is monitored to ensure compliance with the steps defined in the process maps which must include human oversight of all AI-enabled decisions. Also, the cost-benefit case for each task must be monitored to ensure it continues to be acceptable (e.g. the value versus the environmental impact).

Annual audit plans must include sampling to ensure continued alignment of the Council's AI solutions with legal standards, Council goals, emerging governance frameworks and this policy.

Feedback loops must be established to gather insights from AI users to improve AI usage and productivity (e.g. via satisfaction surveys).

9. RELATED DOCUMENTS

The use of AI must always be operated in consideration of all other applicable UK legislation.

APPENDIX 1 – Artificial Intelligence understanding

This policy applies to the Council's current understanding of these technologies which is described below.

AI refers to computational systems and software that perform tasks normally associated with human-like cognition, including reasoning, prediction, learning, and decision-making.

Common AI functionalities include:

- **Generative AI:** Tools that create text, images, code, or media content based on inputs
- **Machine Learning (ML):** Systems that learn and improve autonomously from data
- **Natural Language Processing (NLP):** Systems that analyse, generate, or interact using human language
- **Predictive Analytics:** AI-driven insights that forecast outcomes or trends using historical data
- **Robotics and Automation:** Technologies that perform repetitive tasks without human intervention.

These AI tools can function independently or integrate with software platforms to enhance operational capabilities, automate tasks, and generate actionable insights.

LGA explainer videos are available via this link: AI Unpacked | Local Government Association

APPENDIX 2 – Cyber Security Threats

Key judgements from Bletchley AI Safety Summit held November 2023:

- Artificial intelligence (AI) will almost certainly increase the volume and heighten the impact of cyber-attacks over the next two years. However, the impact on the cyber threat will be uneven
- The threat to 2025 comes from evolution and enhancement of existing tactics, techniques and procedures
- All types of cyber threat actor – state and non-state, skilled and less skilled – are already using AI, to varying degrees
- AI provides capability uplift in reconnaissance and social engineering, almost certainly making both more effective, efficient, and harder to detect
- More sophisticated uses of AI in cyber operations are highly likely to be restricted to threat actors with access to quality training data, significant expertise (in both AI and cyber), and resources. More advanced uses are unlikely to be realised before 2025
- AI will almost certainly make cyber-attacks against the UK more impactful because threat actors will be able to analyse exfiltrated data faster and more effectively and use it to train AI models
- AI lowers the barrier for novice cyber criminals, hackers-for-hire, and hacktivists to conduct effective access and information gathering operations. This enhanced access will likely contribute to the global ransomware threat over the next two years
- Moving towards 2025 and beyond, commoditisation of AI-enabled capability in criminal and commercial markets will almost certainly make improved capability available to cyber-crime and state actors.

APPENDIX 3 - UK Framework

The ten core principles for AI use in government and public sector organisations are:

- Principle 1: You know what AI is and what its limitations are
- Principle 2: You use AI lawfully, ethically and responsibly
- Principle 3: You know how to use AI securely
- Principle 4: You have meaningful human control at the right stage
- Principle 5: You understand how to manage the AI life cycle
- Principle 6: You use the right tool for the job
- Principle 7: You are open and collaborative
- Principle 8: You work with commercial colleagues from the start
- Principle 9: You have the skills and expertise needed to implement and use AI
- Principle 10: You use these principles alongside your organisation's policies and have the right assurance in place

APPENDIX 4 - Key questions for Parliament

The UK Government AI policy is likely to informed by answers to the following questions:

- What kind of regulatory regime should the UK adopt towards AI. Would it involve more, or less, central oversight?
- Should the government develop a system of verification or certification for AI systems?
- What should the government's role be in any algorithmic audit or algorithmic risk evaluation?
- How should copyright law adapt to generative AI, where the relationship between an author's work and how it is used in training an AI model and generating related outputs is often opaque?
- How should employment law adapt to the use of automated decision making by management in areas such as recruitment or performance management?
- How do data protection laws need to adapt? What ownership and control should people have over data they generate?
- Who should be held legally accountable when AI systems violate these legal principles? What should the balance of liability be between the original developer, the organisation employing or disseminating the tools, and the end user(s)?
- What steps should the government take to reduce the sources, spread and impact of AI generated mis and disinformation? How can potential regulations be balanced with freedom of expression?
- If and how should the UK cooperate with other countries for the development of safe and responsible AI? Should the UK attempt to work with other countries to set global standards, or adopt our own distinct regulatory approach in the UK?

APPENDIX 5 – EU Act (Regulation (EU) 2024/1689)

The EU Act categorises AI use into risk tiers with associated legal obligations and penalties of up to 35M Euros or 7 percent of worldwide turnover, whichever is greater.

Unacceptable risk

AI systems that are deemed to pose a threat to people fall into the category of unacceptable risk. Examples include:

- Social scoring systems
- Systems that aim to manipulate children or other vulnerable groups
- Real-time remote biometric systems

Such systems are banned.

High risk

High-risk AI systems are systems that negatively affect safety or fundamental rights. These are divided into two subcategories:

1. AI systems used in products falling under the EU's product safety legislation, including toys, aviation, cars, medical devices, and lifts.
2. AI systems falling into eight areas that need to be registered in an EU database:
    - Biometric identification and categorization of natural persons
    - Management and operation of critical infrastructure
    - Education and vocational training
    - Employment, worker management, and access to self-employment
    - Access to and enjoyment of essential private services and public services and benefits
    - Law enforcement
    - Migration, asylum, and border control management
    - Assistance in legal interpretation and application of the law.

High-risk systems must be assessed before market introduction and throughout their lifecycle.

Low risk

Low-risk AI systems include chatbots and image-, audio-, and video-generating AI. Such systems must comply with transparency requirements, informing users that they are interacting with an AI system and allowing users to decide whether they wish to continue using it. Generative AI models, such as ChatGPT, must also be designed and trained to prevent generation of illegal content, and their makers must publish summaries of copyrighted data used for training.

APPENDIX 6 – Risks and Mitigations

The Council has identified the following key risks associated with AI deployment and will reduce them through the mitigations below, adherence to this policy and to the EU Act:

Risks	Mitigations
Accuracy and Misinformation: AI-generated content or predictions may lack reliability or factual accuracy.	Council officers must ensure outputs from AI tools are rigorously validated before dissemination or decision-making. Council managers must regularly evaluate AI systems to detect and address algorithmic bias that could impact fairness.
Bias and Discrimination: AI technologies may unintentionally produce unfair or exclusionary outcomes.	Council officers must ensure outputs from AI tools are rigorously validated before dissemination or decision-making. Council managers must regularly evaluate AI systems to detect and address algorithmic bias that could impact fairness.
Cybersecurity Vulnerabilities: AI technologies may increase the risk of exposure to malicious attacks or system compromise.	Council procurers must ensure ICT cybersecurity requirements are met before procurements are signed off. The ICT team must then conduct/ensure on-going monitoring and updates are performed.
Data Breaches: AI technologies may increase the risk of unauthorized access, leakage, or misuse of personal or organizational data.	Council officers must ensure no personal, confidential, or sensitive data is input to public AI tools or platforms. Council procurers must ensure ICT and DPO requirements are met before procurements are signed off. The ICT and Information Governance teams must conduct/ensure on-going monitoring and updates are performed.
Environmental Impact: AI technologies may result in high energy consumption.	The ICT and Sustainability teams must ensure AI technologies operate sustainable practices, such as optimising energy efficiency and reducing unnecessary computational demands.
Fraud: AI-enabled fraud may be attempted	Officers must be trained to identify fraud attempts. Identification and verification

	steps must be improved. Reliance on paperwork-must be avoided.
Legal and Copyright Issues: AI content may be generated that infringes on intellectual property or regulatory standards.	Council procurers and managers must ensure compliance with relevant UK and EU laws, regulations, and standards.
Pre-approval: The Council's AI principles and policy may not be followed.	All officers must obtain approval from the Council ICT and Information Governance teams before adopting or implementing AI systems.
Public engagement: Satisfaction may be reduced if the Council uses AI technologies with no public engagement.	The Council must provide clear and accessible information regarding the Council's use of AI technologies. Consult with Councillors where use of AI technologies will have a direct impact on the public.
Risk Assessments: If these are not performed the mitigations set out in this table may not be actioned.	Officers must conduct risk assessments and Data Protection Impact Assessments (DPIAs) for AI projects especially when involving high-risk personal data or automated decision-making processes.
Unintended consequences: AI systems may produce unintended and harmful outcomes.	Council officers must ensure outputs from AI tools are rigorously validated before dissemination or decision-making. Council managers must regularly evaluate AI systems to detect and address algorithmic bias that could impact fairness.