Mid-Kent
Artificial Intelligence Policy

Maidstone Borough Council

Swale Borough Council

Tunbridge Wells Borough

Contents

1. Introduction

1.1 The Council is committed to delivering the best possible services to its residents and embracing innovation. It recognises the transformative potential of Artificial Intelligence (AI) to enhance efficiency, creativity and decision-making across all its operations. This policy has been written to provide a clear and responsible framework for the use of AI, ensuring that it complements the Council's existing information governance and security policies while upholding its legal and ethical obligations.

1.2 The Council encourages the responsible use of AI technologies by its employees, contractors, and consultants to improve service delivery and internal operations. AI refers to computer systems capable of performing tasks that would normally require human intelligence. This includes both decision-making AI and Generative AI (GenAI), a specific type of AI that can create new content such as text and images. Common examples include algorithms, predictive analysis, virtual assistants, chatbots, and transcription tools.

1.3 The purpose of this policy is to provide a clear framework for safe, effective and ethical use of these tools and systems within the Council. It sets out the guidelines to enable staff to responsibly harness AI's benefits while mitigating associated risks. By following this policy, all staff will understand the principles for using AI lawfully and ethically, protecting data, and remaining accountable for outcomes. In addition, staff will be expected to follow appropriate procedures, such as testing and review processes, to identify and mitigate potential bias or discrimination in AI use.

1.4 The Council's approach to AI balances innovation with safeguards, ensuring it enhances, not replaces, human judgement. The Council is looking to explore the use of AI technologies to enhance efficiency and service delivery. The goal is to improve productivity and achieve better outcomes for residents as part of our commitment to continuous improvement.. This policy ensures AI complements staff expertise, allowing more time for complex,

people-focused work. Given the rapid development of AI technologies, this policy will be subject to regular review.

2. Scope

2.1 This policy applies to all information processed by the Council or its representatives. This includes all Council employees, elected members, contractors, volunteers, and third parties working for or on behalf of the Council.

2.2 It covers the use of any AI system, application, or tool when conducting Council business or handling Council information. This includes AI used on Council-owned devices and AI used on personal devices for work purposes (in line with the Acceptable Use Policy).

2.3 It is not limited to stand-alone AI applications; it also covers AI functionality embedded in other software (e.g. AI features in email, document editing, customer service platforms, video conferencing for transcription, etc.). This policy applies to any use of AI within the workplace, regardless of the capacity in which it is used.

3. Principles

3.1 This AI Policy is governed by 10 key principles taken from the UK Government's 'AI Playbook'. The principles clarify our expectations around responsible AI use and describe good governance at all stages of its use:

Principle	Definition
You know what AI is and what its limitations are	Understand how AI can help and the risks it poses; Use techniques to increase the accuracy of outputs; Put processes in place to test tools thoroughly.
You use AI lawfully, ethically and responsibly	Engage with compliance, data protection and legal experts early on; Manage and protect personal data; Test tools to minimise bias in their data at all stages.
You know how to keep AI tools secure	Make sure tools can only access the data they need for the task; Don't train tools using confidential or sensitive data

	sources; Put technical controls in place to detect malicious activity and data leaks.
You have meaningful human control at the right stage	Make sure a trained and qualified person reviews outputs; Test tools fully before they go live and check them regularly; Incorporate feedback from end users.
You understand how to manage the AI life cycle	Know how to set up, update and close down tools securely; Have the right resource to support day-to-day maintenance of tools; Put robust and proportionate testing processes in place to monitor drift, bias and, in the case of generative AI, hallucinations.
You use the right tool for the job	Select the most appropriate technology or model for your needs; Be open to AI solutions and approaches; Use tools to support time-consuming or administrative tasks.
You are open and collaborative	Engage with stakeholder organisations from the start; Join cross-government communities to learn from others and share insights; Be open with the public and identify where and how tools are used.
You work with commercial colleagues from the start	Get advice on the commercial implications of tools; Know how to use AI in line with commercial requirements; Ensure ethical expectations are the same between in-house and third-party tools.
You have the skills and experience needed to implement and use AI	Understand the technical requirements for using tools; Make sure your team has the necessary skillset; Take part in learning courses and keep track of AI developments.
You use these principles alongside your organisation's policies and have the right assurance in place	Understand, monitor and mitigate the risks of using AI tools; Connect with the right assurance and design teams early on; Put documented review and escalation processes in place.

4. Governance

4.1 Good governance is essential to ensure AI is used responsibly and effectively. The Council and its representatives are responsible for the protection and security of the sensitive information it processes. This can be personal or commercially sensitive information therefore the Council must ensure that any data is used in a transparent, fair and lawful manner. The use of AI must be carefully managed to ensure it does not compromise the security or privacy of information.

4.2 The Council will integrate AI oversight into its existing governance structures for digital and information management. The Council's Corporate Leadership Team is responsible for setting the strategic direction for AI use. The Senior Information Risk Owner (SIRO) has ultimate accountability for protecting the Council's information assets and thus has oversight of AI from a risk perspective.

4.3 All staff are responsible for adhering to all relevant data policies and procedures, ensuring data security, and completing mandatory training. This includes not implementing AI systems without following the correct process, strictly adhering to the guidelines within this policy, and immediately reporting any data breaches or near-misses. Staff must seek guidance from the Data Protection Officer or the Information Governance Team whenever there is any uncertainty regarding AI or data use.

Role	Responsibilities
Project Leads / Service Managers	Ensure proper risk assessment (DPIA, etc.) is done, follow the policy during implementation, and report/address any issues.
Information Governance (IG) Team and Data Protection Officer (DPO)	Consulted before any personal or confidential data is processed by AI to ensure proper oversight and compliance. This includes providing guidance on legal and ethical requirements, reviewing Data Protection Impact Assessments (DPIAs), and advising on how to mitigate potential privacy or ethical risks.
IT and Digital Services Team	IT and Digital Services are responsible for the technical evaluation of AI tools. This includes ensuring appropriate security measures are in place such as access controls and encryption, conducting necessary testing (including cybersecurity and adversarial testing), and maintaining an inventory of approved AI systems. However, technical testing does not assess whether an AI tool meets the specific functional needs of a service area. It is the responsibility of the service itself to test and

	confirm that the AI tool performs effectively for its intended business use case. Only AI tools that meet security standards should be integrated.
Legal Services	Provide advice on legal implications of AI use (contractual issues with vendors, intellectual property questions, potential liability), and help ensure the Council upholds individuals' rights (like the right to a human review of decisions).
Equalities Lead / Accessibility Champions	Ensure AI deployments undergo equality impact considerations and meet accessibility standards, incorporating fairness and inclusivity in practice.
All Staff (AI Users)	Use AI tools in accordance with the policy and specific approvals/conditions, remain vigilant for problems (like erroneous or biased outputs), correct or escalate issues, and acknowledge responsibilities when using AI for Council work.

5. Use

5.1 This policy applies to all staff using any AI tools for Council activities, whether on Council-owned devices or personal devices. This includes AI functionality embedded in applications such as email clients, productivity tools, and video conferencing.

5.2 Only AI systems that have been approved by the Council for internal use following the appropriate governance process may be used. Access to AI tools and systems for corporate work must be carried out using Council-approved devices.

5.3 Staff may use approved AI for work-related purposes if they comply with this policy. Discussion with managers is encouraged when using generative AI tools in their work. This does not apply to everyday tools that incorporate AI features by default, such as search engines or productivity software. Acceptable uses include generating text or content for reports, emails, presentations, images, and customer service communications.

5.4 However, AI must be used in a manner that promotes fairness and avoids bias to prevent discrimination. AI must not be allowed to solely determine which customers have access to services. Humans must be involved in such decision-making processes, and there must be an appeal process for any automated or AI-informed decisions.

5.5 AI may generate outputs that contain inaccuracies or biases. As such, all AI-generated content must be rigorously reviewed for accuracy, bias, and ethical considerations before it is used. The user is ultimately responsible and accountable for the final output. When presented with the option, staff must prioritise accuracy over creativity. Any concerns regarding the accuracy or ethical implications of AI-generated outputs should be referred to the appropriate service area for review and guidance.

5.6 To ensure transparency with the public, any content generated with the assistance of AI must be identified with a visible disclaimer or note. AI outputs, while intelligent, must be carefully verified and not regarded as foolproof. AI tools are intended to complement, not replace, officers' professional expertise, and should not be relied upon for strategic decisions or critical thinking.

5.7 To promote transparency, the Council may maintain an AI inventory log to catalogue and track all AI systems in use. This log may be shared with staff to support auditing, demonstrate approved systems, and enhance productivity.

6. AI Verification and validation

6.1 No AI solution or feature should be deployed or made available to users until it has successfully completed a documented verification and validation process as part of the Privacy Impact Assessment (outlined in section 7), demonstrating that it meets defined safety and performance standards.

7. Data Privacy and Security

7.1 The use of AI requires additional vigilance to uphold data protection and confidentiality obligations. Before using any AI technology that is new to the Council, new to the service area, or being used for a new purpose, officers must consult the Information Governance (IG) Team to complete a risk assessment. This includes tools that may be familiar to individuals but have not yet been assessed or approved for use within the Council.

7.2 The risk assessment process helps identify and reduce risks, ensuring AI systems meet quality, performance, and legal standards. It will include a risk-based classification of the AI system, its inputs and outputs based on sensitivity and legal obligations, and ensures appropriate handling and protection. The

process will also document a lifecycle management plan for each AI system.

7.3 When using AI, staff should prioritise the confidentiality and privacy of personal and sensitive information. Any data entered into an AI tool must be handled in accordance with applicable data privacy laws and regulations, including GDPR. Confidential and personal information must not be entered into a public AI tool. This is because the information will then enter the public domain and may be used for further training of the publicly available tool. This would amount to a data breach. Staff must follow all applicable data privacy laws and organisational policies when using AI.

7.4 AI use must comply with all relevant laws and regulations, including those related to data protection and human rights. Under GDPR, individuals have the right to a human review of any automated decision-making, so any AI system involved in such decisions must allow for a human to review and override the outcome.

7.5 If the information involves the processing of personal data, a Data Protection Impact Assessment (DPIA) must be undertaken. A DPIA is a legal requirement for projects that present a high risk to data subjects' rights. For projects involving Council data that is not personal, a separate but similar risk assessment process must be completed with the Information Governance Team. Key documents, including Privacy Notices, will be updated as necessary to ensure transparency.

7.6 To support consistency and reduce duplication in risk assessments, the Council may develop a central library of approved AI use cases. This resource will catalogue common, low-risk applications of AI that have already undergone appropriate governance checks. Staff may refer to this library when proposing similar uses, subject to confirmation by the Information Governance Team.

7.7 AI poses significant governance challenges and risks, including bias, data privacy and security violations, transparency, accountability, and fairness. It should not be solely relied upon for decision-making, as algorithms may produce biased outcomes. When considering AI for projects, it is essential to ensure it does not cause harm or loss to stakeholders.

7.8 Any AI-generated content or outputs used for decision-making are records and must be saved according to the Council's data retention policies. Furthermore, staff must only use AI tools that have been approved and must immediately report any security or

data breach incidents involving AI via the normal reporting procedure.

7.9 Security classification: Where appropriate, an Information Asset Owner should be assigned to each AI tool or system, in line with existing Council policies and the Information Governance Roles and Responsibilities guidance.

8. Vendors

8.1 Any use of AI technology in pursuit of Council activities should be done with full knowledge of the policies, practices, terms and conditions of its vendors. This includes understanding the vendor's approach to data privacy, security, ethics, and environmental and social impacts. The Council should consider the vendor's:

- Ability to provide clear and understandable explanations for the AI model's decisions where appropriate.
- Approach to addressing potential biases in any AI data and algorithms it uses.
- Commitment to protecting sensitive data and ensuring the security of any AI system.
- Adherence to ethical principles and guidelines for AI deployment.
- Commitment to reducing the environmental impact of AI deployment.
- Efforts to address social inequalities and promote inclusive growth through AI, such as ensuring AI systems are not used to perpetuate discrimination or disadvantage marginalised groups.
- Ability to contribute to the regeneration of ecosystems and natural resources through AI-enabled solutions, such as optimising energy consumption or improving resource management.

8.2 By incorporating these considerations into the procurement process, the Council can ensure that vendors contribute to a more equitable, sustainable and inclusive future.

9. Ethical Use

9.1 The Council's use of AI must uphold ethical standards and proactively consider its societal impact. AI must be used ethically and in compliance with all applicable legislation, regulations, and Council policies. Staff must not use AI to generate content that is discriminatory, offensive, or inappropriate. To ensure the safe, fair, and lawful use of AI technologies, the following factors should be considered:

- **Fairness:** AI systems must be designed and used in ways that avoid discrimination, exclusion, or harm to individuals or groups. They should respect human dignity and diversity, and promote equitable outcomes. AI processes must be transparent, explainable, and accountable, with clear mechanisms for feedback, review, and correction.
- **Bias and Discrimination:** AI systems can unintentionally reinforce existing societal biases, leading to unfair and discriminatory outcomes. All reasonable steps must be taken to identify, assess, and reduce bias and discrimination during the development, deployment, and use of AI tools.
- **Privacy:** AI systems must protect personal and confidential data ensuring compliance with applicable data protection laws, regulations and Council policies.. Use of AI should respect individuals' privacy rights and preferences, providing them with clear control over their data and informed consent regarding how their information is collected, used, and shared.
- **Safety:** The design, deployment, and use of AI systems should avoid intentional harm to individuals and recognise the evolving nature of potential impacts, including psychological or emotional harm such as job displacement or stress. AI systems must comply with relevant health and safety standards and be designed to be secure, resilient, and capable of managing errors, failures, and uncertainties effectively
- **Human Aspect:** AI use must uphold the autonomy, dignity, and well-being of all individuals, in full compliance with relevant human rights laws and regulations. It should support and empower individuals, whilst respecting their values, choices, and personal preferences. AI must align with human rights principles and reflect the Council's values.
- **Copyright and Intellectual Property:** It is prohibited to use AI to generate content that infringes on the intellectual property rights of others. Staff must verify the originality of any AI-generated content and, if applicable, cite sources used by the AI model. If there is any doubt about potential infringement, staff must consult with Legal Services or the Information Governance Team before proceeding.
- **Workforce Impact:** The Council recognises that the deployment of AI technologies may affect staff roles, responsibilities, and service delivery. Any potential for job displacement or significant changes to working practices must be carefully assessed and managed in consultation with affected teams, HR, and relevant service leads. AI must not be used to replace human judgment in areas where ethical, legal, or professional discretion is required.
- **Responsible Use**:
  Misuse of AI whether intentional or unintentional can undermine public trust, compromise service quality, or cause harm. The Council will monitor AI usage across services and maintain oversight mechanisms to ensure tools are used appropriately, transparently, and in line with organisational values and legal obligations

9.2 The Council is legally required to comply with the Public Sector Equality Duty under the Equality Act 2010. The use of AI can affect different groups of people in varying ways, and officers must understand this potential for unintended bias. To ensure fairness and equality, the Council will:

- **Undertake Equality Impact Assessments (EqIA):** For any AI system affecting the public or staff, an EqIA will be conducted to assess its potential impact on individuals with protected characteristics.
- **Use Representative Data:** The Council will strive to use training data that is representative of the community to avoid perpetuating historic biases.
- **Maintain Human Oversight:** Human review of AI decisions is essential to spot and prevent patterns of unfairness.
- **Serve All Segments of the Public:** We will ensure alternative, non-AI channels remain available for residents who may be less comfortable or able to engage with AI-driven processes.

9.3 The Council recognises the environmental impact of AI tools, primarily from the significant energy and water consumption of AI models and data centres. This consumption contributes to carbon emissions and can strain local resources. Additionally, the production and disposal of electronic waste present environmental challenges. The Council is committed to adopting sustainable practices to mitigate these impacts, ensuring the benefits of AI do not compromise environmental well-being.

9.4 Staff must not use AI in ways that conflicts with the Council's ethical standards or political neutrality. This includes not generating content with political bias, fabricating information, or spreading misinformation. All information from AI must be independently verified by a responsible officer and must not be the sole basis for decisions. If there are any doubts about the appropriateness of using AI in a particular situation, staff should consult with their manager or Information Governance Team.

10. Transparency and Accountability

10.1 Transparency and governance are paramount to maintaining public trust in AI-driven public services. The Council is committed to open communication about its use of AI and to establishing clear mechanisms for accountability.

10.2 The Council will proactively disclose its use of AI to the public in clear and understandable terms. This includes publishing updates on the Council website regarding key AI systems in use,

referencing AI in privacy notices where personal data is processed, and ensuring staff can clearly articulate the role of AI in decision-making processes. The Council will also consider establishing a public-facing Algorithmic Transparency Record for applicable systems.

10.3 The Council recognises the importance of engaging with residents and stakeholders to build trust and ensure that AI technologies reflect community values. Where appropriate, the Council will consult with the public on the use of AI systems that significantly impact service delivery, decision-making, or personal data. Feedback from these engagements will inform the development, deployment, and governance of AI tools.

10.4 AI-generated information is classified as 'held information' by the Council and is therefore subject to Freedom of Information (FOI) and Environmental Information Regulations (EIR) requests. AI-generated documents, data, and logs will be treated as any other Council record and must be stored in a manner that facilitates retrieval for FOI purposes.

10.5 The internal deployment of AI systems must be monitored for compliance, performance, fairness, usage, and cost-effectiveness. Responsibility for monitoring lies with the designated Product Owner, typically the colleague overseeing major systems such as Microsoft products, Workday, or other core platforms.

10.6 Internal Transparency: All Council staff should have access to information about AI-powered products, features, and developments, including pilot projects.

10.7 Staff using AI should be able to suggest new opportunities for AI use through the appropriate channels in a timely manner.

10.8 The Council retains ultimate accountability for any decisions or outcomes influenced by AI. Responsibility for each AI system will be clearly assigned to a human owner. If an AI error occurs, the Council will accept responsibility and rectify the mistake. Affected individuals will have clear avenues for recourse, and the Council will provide a remedy for any harm caused. Management oversight will include the regular review of AI system performance and related issues.

10.9 Any AI system that is no longer in use must be formally retired and decommissioned to ensure it is fully withdrawn from operational environments.

11. Automated decision making and profiling

11.1 The Council is committed to supporting individuals in exercising their data protection rights. To that end, the Council will:

- Process personal data transparently and in accordance with data protection Legislation.
- Enable individuals to exercise their rights over personal data held by the Council, including the right to request human intervention, express their views, and contest decisions.
- Apply enhanced scrutiny and risk assessment to any use of automated decision-making or profiling, ensuring such processes are justified, alternatives are considered, and individual rights are protected.
- Respect the right of individuals not to be subject to decisions based solely on automated processing—including profiling—that produce legal or similarly significant effects, where applicable.

For more information, please refer to the Council's guide to individual rights under the UK GDPR and the DUAA 2025.

12. Algorithmic Transparency Recording Standard (ATRS)

12.1 The Data Standards Authority recommends that public sector organisations publish details about the algorithmic tools they use and their purposes. Adopting ATRS helps organisations:

- Build public trust by clarifying how and why algorithmic tools are used, including their limitations and role in decision-making
- Ensure senior leaders are accountable for the use and outcomes of these tools
- Share best practices and learn from other organisations
- Reduce administrative burden by proactively addressing queries that may arise through FOI requests or parliamentary questions
- Set clear expectations for third-party suppliers regarding transparency requirements

12.2 An algorithmic tool refers to any product, application, or system that uses complex algorithms to support or solve specific problems. This broad term includes applications of artificial intelligence (AI), statistical modelling, and other advanced computational methods. These tools often combine multiple models within a larger digital solution.

12.3 External Transparency: Any AI product or use that interacts directly with the public or significantly influences decision-making must be logged using the Algorithmic Transparency Recording Standard (ATRS).

13. Training

13.1 The Council is committed to providing comprehensive training and support to all staff to ensure the effective and ethical use of AI tools.

13.2 AI training will be integrated into the Council's digital learning programmes. Baseline training on this AI Policy and general AI awareness will be provided to all existing staff and as part of the induction process for new employees.

13.3 For staff in roles with significant AI use, the Council will provide role-specific training. This will include advanced modules on interpreting AI outputs, best practices for using specific tools, and troubleshooting common issues.

13.4 The IT Helpdesk will be fully prepared to handle all queries and support requests related to AI tools, following standard incident management procedures. Staff can log tickets for errors or performance issues, which the IT team will either resolve or escalate to the vendor as required.

14. Compliance

14.1 This policy is a mandatory Council requirement. Failure to adhere to these guidelines can lead to serious risks and will be addressed. This AI Policy is considered part of the Council's code of conduct for information management. Using AI in a manner contrary to this policy is comparable to the misuse of any Council resource or the violation of data protection rules.

14.2 The Council will monitor the use of AI systems to an appropriate degree. Managers are expected to supervise their teams' adherence to the policy. Any incidents - including data breaches, major errors, or security issues - must be reported immediately to the Information Governance Team or senior management. There will be no penalty for reporting an honest mistake promptly, but attempting to conceal an incident will be considered misconduct.

14.3 Failure to comply with this policy may result in disciplinary action in accordance with the Council's Human Resources policies and procedures.

- **Minor Infractions:** An accidental or non-harmful violation will typically result in corrective action, such as additional advice or training. Repeated minor infractions may, however, lead to further disciplinary measures.

- **Serious Infractions:** A serious breach, such as wilfully or negligently uploading confidential personal data to a prohibited service or bypassing human oversight, may constitute gross misconduct and will be investigated according to the Council's disciplinary procedures.

15. Policy Review

15.1 This policy will be formally reviewed every three years, or sooner if required due to changes in technology, legislation, or best practice. In the meantime, it will be kept under continuous review to ensure any necessary updates are identified and implemented promptly. This policy reflects current best practice and will evolve in line with emerging legislation, including the Digital and Automated Decision-making Accountability Act (DUAA) 2025.The Council treats this as a living document to maintain its relevance and effectiveness.

15.2 Any revisions to the policy will be approved by senior management and communicated to all staff, with highlights of key changes. Additionally, the Council's Retention Policies and Privacy Notices will be reviewed and updated as necessary to ensure alignment with this policy.