South Ayrshire Council
Comhairle Siorrachd Àir a Deas
Making a Difference Every Day

Policy
Artificial Intelligence (AI)

A policy governing the use and application of AI

April 2026

Document information

Name:	Policy – Framework for the use Artificial Intelligence at South Ayrshire Council		
Prepared By:	Stewart McCall	Document Version No:	2.0
Type:	Policy	Document Version Date:	23-04-26
Reviewed By:	Various – see distribution list	Review Date:	May 27

Distribution list

From	Date	Phone/Email
Stewart McCall	30-03-26	stewart.mccall@south-ayrshire.gov.uk

To	Action*	Phone/Email
Kev Mullen	Approve/Review	Kevin.mullen@south-ayrshire.gov.uk
James Andrew	Review	James.andrew@south-ayrshire.gov.uk
Chris Richards	Review	Chris.richards@south-ayrshire.gov.uk
Anne Yeo	Review	Anne.yeo@south-ayrshire.gov.uk
Paul Gibson	Review	Paul.gibson@south-ayrshire.gov.uk
Rachel Peterson	Review	Rachel.peterson@south-ayrshire.gov.uk
Deborah McVey	Review	Deborah.mcvey@south-ayrshire.gov.uk
Lynn Robertson	Review	Lynn.robertson@south-ayrshire.gov.uk
Thomas Griffin	Review	Thomas.griffin2@aapct.scot.nhs.uk

* Action Types: Approve, Review, Inform, File, Action Required, Attend Meeting, Other (please specify)

Document version history

Version Number	Version Date	Revised By	Description
1.0	28-05-25	S McCall	Approval by SAC Cabinet 28 May 2025
1.1	30-03-26	S McCall	Revised and updated to expand scope to include all AI and improve clarity on roles and responsibilities. Section on hidden AI added. Governance in Education made clearer.
1.2	15-04-26	S McCall	Updated to reflect reviewers' comments.
2.0	23-04-26	S McCall	Approval by SAC Cabinet 26 May 2026

Table of Contents

1. Background

Artificial Intelligence (AI) refers to technologies that enable systems or machines to perform tasks normally requiring human intelligence, such as understanding language, analysing data, identifying patterns, making predictions, supporting decisions or recognising images, audio and other inputs. AI includes rule-based systems, machine learning, deep learning, natural language processing, computer vision, robotics, predictive analytics and embedded AI features within software platforms.

AI capabilities are increasingly built into everyday tools used across public services, such as productivity suites, communication platforms and case-management systems, often operating in the background. All AI, whether explicitly deployed or embedded, must therefore be used responsibly, ethically and in line with legislation, policy requirements and governance processes.

Generative AI (GenAI) is one category of AI that creates new content such as text, images, audio, video or software code. Large Language Models (LLMs) use deep learning and large datasets to generate human-like text. While GenAI has attracted significant public interest due to its creative and flexible capabilities, it represents only one part of the wider AI landscape relevant to the Council. Emerging forms of agentic AI go further by not only generating content but also taking actions, making decisions and autonomously executing tasks to achieve goals. These agent-based systems can plan, chain actions together, call external tools or systems, and operate with a greater degree of autonomy than traditional GenAI models. Understanding the distinction between generative and agentic AI is important, as the latter introduces additional considerations around safety, oversight, decision boundaries and accountability in public-sector use.

All AI technologies, generative, agentive, predictive, analytical or embedded, present opportunities to improve efficiency, enhance services and support informed decision-making. They also introduce responsibilities around data privacy, fairness, transparency, non-discrimination, security and accountability. Ethical use and effective risk assessment are essential.

AI systems are not always accurate. Outputs may contain errors, biases or misleading information. Human oversight is therefore required, and users remain accountable for checking and validating AI-generated or AI-supported outputs before relying on them. AI should assist professional judgment, not replace it.

Safe and responsible AI use requires appropriate controls, including data protection and security assessments, ethical and equality considerations, transparency, monitoring and ongoing validation. All AI used by the Council must comply with UK GDPR, the Data Protection Act 2018 and internal governance procedures, and must align with the Council's values of fairness, transparency, accountability and respect.

2. Purpose

The purpose of this Policy is to ensure that everyone who uses AI on behalf of the Council, whether employees, contractors, developers, vendors, consultants, temporary staff or other third parties, are fully aware of their responsibilities and the risks involved.

Safe and responsible use of Artificial Intelligence (AI) requires strong controls, including data protection and security assessments, ethical and equality considerations, transparency and

monitoring. This Policy looks to provide the framework for these controls, ensuring that all AI activity is ethical, responsible, transparent and compliant with relevant legislation and regulatory requirements.

Given the rapid pace of change in AI technologies, this Policy will be kept under continual review and updated regularly to ensure it remains current, effective and fit for purpose.

3. Scope

The Policy provides a framework for the use of all types of AI.

It applies to all users with access to AI, whether through Council-owned devices or BYOD (Bring Your Own Device) in pursuit of Council activities. This includes all Councillors, employees, contractors, developers, vendors, temporary staff, consultants or other third parties (referred to as 'users'). It also applies to third parties carrying out work on the Council's behalf or accessing its information systems.

This Policy should be read alongside the Council's ICT Acceptable Use Policy.

4. Roles and Responsibilities

All Directors, Assistant Directors, Service Leads and Coordinators/Team Leaders will be responsible for ensuring that the Policy is applied consistently and that existing employees who will/may use AI are fully aware of the Policy and their responsibilities with regards to the use of it.

Service Leads and Coordinators/Team Leaders are responsible for discussing the Policy with their staff to ensure the content is understood.

The Transformation Delivery Group (TDG), which includes but is not limited to Transformation, Information Governance, ICT Operations and Organisational Development, are responsible for approving the use of any AI solution being considered by the Council.

Employees who will/may use AI are responsible for reading the Policy and should ensure any concerns or queries are raised with Service Leads/Coordinators/Team Leaders prior using AI systems.

5. AI Usage

Use of AI must be in a manner that promotes fairness and avoids bias to prevent discrimination and promote equal treatment and be in such a way as to contribute positively to the Council's goals and values.

Users may use AI for work-related purposes subject to adherence to this policy. This includes tasks such as generating text or content for reports, emails, presentations, images and customer service communications.

Materials substantially created using AI, and in particularly where it has been used to support a decision, should be annotated as such. The following is an example of standard wording that should be used in this situation.

"Artificial intelligence was used to assist with drafting this content. All outputs were subject to human review and approval by South Ayrshire Council in line with its AI policy."

6. Identifying AI-Enabled Technologies

It is not always apparent when a system or service uses AI. Users must assess technologies against the criteria below to determine whether AI functionality is present. A technology should be considered AI-enabled if it demonstrates one or more of the following characteristics:

- Supports, informs or automates decision-making.
- Delivers, interprets or generates information.
- Detects or identifies patterns within large datasets.
- Utilises machine learning to learn from data, refine outputs or solve problems.
- Predicts outcomes, identifies trends or manages risks.
- Prioritises actions, allocates resources or influences operational workflows.
- Monitors individuals, environments, assets or systems remotely.
- Identifies early indicators of health, wellbeing, behaviour or safety concerns.
- Translates, interprets or generates natural language.
- Analyses data from its environment and takes action in response.
- Recognises images, objects, individuals, speech or other sensory inputs.
- Uses historical data or previous outputs to inform future predictions or actions.
- Adapts behaviour, adjusts outputs or seeks to influence user behaviour over time.

If a system exhibits any of the above characteristics, it may be an AI system and subject to all requirements, controls and approval processes set out within this Policy and associated governance frameworks.

Where uncertainty remains regarding whether a technology incorporates AI functionality, users must seek advice from the Council's ICT Operations Service before the technology is introduced, used, or integrated into any Council process.

7. Governance and process for adopting AI solutions

To ensure the security and protection of Council data, no AI technology or service may be accessed, trialled or commissioned without prior approval. For the majority of Council activity, approval and oversight are provided by the Council's Transformation Delivery Group (TDG), which acts as the primary and mandatory decision-making body for authorising and post-implementation monitoring of all technology and AI-related activity. The TDG coordinates input from Information Governance, Procurement, Information Security, ICT Operations and Transformation as part of its assessment.

An exception applies to the use of AI in educational settings within schools where review and approval are provided through existing education governance arrangements. See Section AI in Education (Schools).

Users must formally declare their intention to use AI, including the purpose of the proposed use, the nature of the data to be input, the expected outputs and how those outputs will be shared or applied. All proposals must demonstrate how personal data will be protected and how risks, such as bias, discrimination or misuse, will be assessed and mitigated through appropriate testing.

Users proposing the introduction of an AI solution must be able to evidence the benefits it will deliver to the Council. This includes demonstrating how the technology will improve efficiency, enhance service quality, reduce risk, support decision-making or create measurable value.

Benefit claims should be supported by clear analysis, expected outcomes, and, where possible, quantifiable metrics to allow the Council to assess whether the AI solution provides a justified and proportionate advantage.

A Data Protection Impact Assessment (DPIA) and cyber security review must be completed prior to any solution being implemented, as outlined in existing Council policies and procedures. In line with these procedures, approval will be required from the Council's TDG prior to the use of any AI.

An Integrated Impact Assessment (IIA), completed by the Service who wishes to introduce the AI solution, is also required for implementations of solutions which use AI technology.

When procuring or trialling AI technologies, including no-cost pilots, the Council must ensure appropriate legal protections are in place. A Data Processing Agreement alone is insufficient, as it does not address liability, indemnities, or financial recourse, leaving the Council exposed in the event of a data breach or confidentiality issue. Where standard terms and conditions apply, these may not provide adequate protection. A suitable legally binding contract is therefore required to manage risk and meet statutory data protection obligations. Staff must seek advice from the Council's Legal Services before any AI technology is introduced or used.

Details of approved and operational AI solutions will be maintained on an internal register to provide visibility and oversight of use across the Council. This will be managed by the Portfolio Management Office (PMO). Operational solutions will also be published on Scottish AI Register* to comply with the requirements of the Scottish Government.

* *The Scottish AI Register provides information about the AI systems that are currently in use or in development within the Scottish public sector. It aims to promote transparency and trust by allowing the public to learn about these AI systems, understand their purposes, and provide feedback. It's part of Scotland's broader effort to develop ethical and inclusive AI systems*.

7.1. AI in Education (Schools)

AI may also be used within Education settings, but only under strict governance arrangements. Any AI tools, systems or approaches proposed for use in schools must be submitted to the Education Digital Strategy Group for review and approval, ensuring alignment with curriculum objectives, safeguarding obligations and digital safety standards.

AI will only be considered for use in Education where it can be demonstrated that no sensitive personal information is processed, that data protection requirements are fully met and that the use of AI provides clear, positive educational outcomes for learners. Prior to implementation, a Data Protection Impact Assessment (DPIA) and a cyber security review must be completed. These measures ensure that AI is used to enhance learning and teaching in a controlled, ethical and secure way, consistent with the Council's wider commitments to responsible AI use.

7.2. New AI Functionality in an Existing, Approved Solution

When a digital solution provider introduces new AI functionality into an existing product, this constitutes a material change and must trigger a full AI governance review. Any new or updated AI capability, whether enabled by default, embedded within the system, or offered as an optional module, must be treated as a new AI implementation under this Policy.

New AI functionality introduced into an approved digital solution by an existing supplier must be escalated to the Council's TDG for consideration and approval. The TDG will coordinate input from Information Governance, Procurement, Information Security, ICT Operations and

Transformation to determine whether the AI functionality may be enabled, enabled with conditions or must be prohibited. No AI introduced by an external provider may be activated or used until TDG approval has been granted.

8. Data Protection

A Data Protection Impact Assessment (DPIA) is required to identify and minimise the risks of personal data privacy when a service is implementing a new AI solution. The use of AI to process personal data will require the completion of a full DPIA to consider these risks. Information on the Council's DPIA procedures are available at Data Protection Impact Assessment.

Where AI is processing personal data; providing automated decision making and/or profiling individuals, the risks around compliance with data protection laws must be fully considered. Information Governance will provide advice and support to services who are undertaking assessments of introducing AI technology or services.

As with all personal data processed by the Council, any personal data processed through AI must comply with UK GDPR , the Data Protection Act 2018 and the Data (Use and Access) Act 2025.

Any release of private/personal information without an appropriate DPIA and a consideration of the legal basis under data protection law to do so, will result in a breach of relevant data protection laws which may result in enforcement actions from the UK Information Commissioner's Office (ICO).

9. Vendors

Any use of AI technology in pursuit of Council activities should be done with full acknowledgement of the policies, practices, terms and conditions of developers/vendors. All AI purchases must be managed through the Council's Procurement service.

10. Copyright

Users are required to comply with copyright and licensing obligations when using AI. Content must not infringe the rights of others and any licensing restrictions on AI tools must be followed. Information Governance should be consulted where clarification is needed.

11. Accuracy

All information generated by AI must be reviewed and edited for accuracy prior to use. Users of AI are personally responsible for reviewing output and are accountable for ensuring the accuracy of AI generated output before use/release.

12. Confidentiality

Until a DPIA has been completed and the AI has been approved as secure by Information Governance and ICT Operations, then confidential and personal information must not be entered into an AI tool as information may enter the public domain.

13. Ethical Use

AI must be used ethically and in compliance with all applicable legislation, regulations and organisational policies. Users must not use AI to generate content that is discriminatory, offensive, or inappropriate.

Ethical AI use depends on meaningful human oversight. Users must examine AI outputs to confirm they are accurate, fair and compliant with equality and ethical standards.

14. Disclosure

Transparency is essential to ensuring accountability in the use of AI. Users must be able to understand how AI systems support or influence decisions. The Council will disclose the presence and purpose of AI systems to relevant stakeholders, including information on how they operate, what data they use and the decision-making processes they support. Any content generated using AI must be clearly identified as such.

15. Integration with other tools

API and plugin tools enable access to AI and extend functionality for other services to improve automation and productivity outputs. Users should follow OpenAI's Safety Best Practices and implement safety measures such as moderation and human oversight. This should include:

- Adversarial testing.
- Human in the loop (HITL).
- Prompt engineering.
- "Know your customer" (KYC).
- Constrain user input and limit output tokens.
- Allowing users to report issues.
- Understand and communicate limitations.

16. Risks

Use of AI carry inherent risks. A DPIA and an Information Security risk assessment should be conducted using their defined processes and templates for any project or process where the use of AI are proposed. The risk assessment should consider potential impacts including: legal compliance; bias and discrimination; security (including technical protections and security certifications); and data sovereignty and protection.

16.1. Legal compliance

Consideration should be given to the possibility that data entered into AI may enter the public domain. Public AI includes, but is not limited to, ChatGPT, Bard, Gemini, n8n, zapier and make, and these can release non-public information and breach regulatory requirements, customer or vendor contracts, or compromise intellectual property.

To mitigate this risk, the presumption in the Council's ICT environment is that all public and/or non-TDG approved AI will be blocked from use.

16.2. Bias and discrimination

AI may make use of and generate biased, discriminatory or offensive content. Users should use AI responsibly and ethically, in compliance with Council policies and applicable laws and regulations.

Where personal data is being processed for the purpose of automated decision making or profiling by AI, appropriate measures must be implemented by a Service to ensure individuals have a right of appeal on decisions. This must be considered as part of the required DPIA process.

16.3. Security

AI may store sensitive data and information, which could be at risk of being breached or hacked. The Council must assess technical protections and security certification of AI before use.

All AI solutions must be assessed technically by the ICT Operations to ensure that information is protected, and security managed before use. The technical assessment will be completed using the information provided in the DPIA.

To mitigate this risk all public and/or non-TDG approved AI will be blocked from use.

16.4. Data hosting

An AI solution may be hosted either in its entirely or in part outside of the UK and consideration must be given to ensuring this complies with the relevant regulations and laws the Council must comply with. For example, information created or collected in the originating country will remain under jurisdiction of that country's laws. The reverse also applies. If information is sourced from AI hosted overseas, the laws of the source country regarding its use and access may apply.

AI service providers should be assessed for data sovereignty practice by ICT Operations and Information Governance prior to using their AI.

UK Data Protection laws govern the transfers of personal data to processors and organisations located outside the UK. Risks relating to the processing of personal data outside the UK must be considered and managed through the DPIA process.

17. Digital Skills and capacity building

The effective use of AI relies on the Council's workforce having the appropriate knowledge and skills to use it safely, ethically and responsibly. The Council's Corporate Workforce Plan recognises that artificial intelligence will increasingly shape service delivery and workforce roles over the next five years. It therefore places strong emphasis on building digital confidence and foundational AI awareness across the workforce, supporting the safe and effective use of tools such as M365 Copilot Chat to improve productivity, data analysis and workflow management.

AI capability development is embedded within the Council's wider corporate digital skills programme and is supported by this policy. This approach ensures the workforce is well prepared for future technological change.

Employees who use, or may use, AI as part of their role are required to complete the COAST e-learning module on AI to ensure they understand their responsibilities. Additional support and guidance is available through the Council's Digital Skills Coordinator within Organisational Development and the Council's AI documentation resources. As part of the induction process, relevant employees will also be made fully aware of the Council's AI policy.

18. Compliance

Any violations of this policy should be reported to the Council's ICT Service Desk in the first instance or senior management.

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

19. Review

This policy will be reviewed periodically and updated as necessary to ensure continued compliance with all applicable legislation, regulations and organisational policies.

20. Acknowledgment

By using AI, users acknowledge that they have read and understood these guidelines, including the risks associated with the use of AI.

21. Forms and links with other Policies

Related forms and contact us:

- Data Protection Impact Assessment
- Contact Transformation

Internal policies and strategies linked to this Policy include:

- Workforce Planning Action Plan 2026-31
- Digital and ICT Strategy 2023-2028
- ICT Security Policy and ICT Acceptable Use Policy
- Data Protection Policy

External policies and strategies linked to this Policy include:

- Copyright, Designs and Patents Act 1988.
- UK General Data Protection Regulation.
- Data Protection Act 2018.
- Data (Use and Access) Act 2025.
- Equality Act 2010 (Public Sector Equality Duty).

22. Glossary of definitions for the purpose of this Policy

Term	Definition
Adversarial testing	A method used to evaluate machine learning models by intentionally providing them with malicious or harmful inputs to see how they respond. The goal is to identify vulnerabilities and improve the model's robustness and safety.
Application Programming Interface (API)	A set of definitions and protocols that enables data transmission between software solutions.
Bring Your Own Device (BYOD)	Refers to a policy where employees or external partners use their personal devices, such as laptops, smartphones, or tablets, to access Council networks, systems, and data.
Data Protection Impact Assessment (DPIA)	The process carried out on projects/changes involving personal data to help ensure compliance with data protection legislation and embed 'privacy by design'.
Deep learning	A subset of machine learning where systems 'learn' to detect features that are not explicitly labelled in the data.
Human in the loop (HITL)	Refers to a model where human interaction is integrated into the AI system's decision-making process. This approach combines the strengths of both human intelligence and machine learning to create more accurate and reliable outcomes.
Generative Artificial Intelligence (GenAI)	A form of artificial intelligence (AI) that generates text, images, or other media in response to prompts.
Know your customer	Refers to the use of artificial intelligence technologies to enhance the process of verifying the identity of customers and understanding their behaviours, preferences, and needs.
Large Language Models (LLM)	Refers to the number of parameters the model can change autonomously as it 'learns'.
Neural networks	Computational models inspired by the human brain's structure and function
Plugins	A software component that adds a specific feature to an existing solution.
Prompt engineering	Involves designing and refining the inputs (prompts) given to generative AI models to produce desired outputs. This process is crucial for ensuring that AI systems understand and respond accurately to various queries.
Query	A request for data or information from a database table or combination of tables.