



Artificial Intelligence (AI) Policy

Document Reference Number:	AI001	Document Title:	Artificial Intelligence (AI) Policy
Document Type:	Policy	Status:	Approved
Current Version:	1.0	Document Author:	Ben Allen – M365 Solutions Architect Mark Cole – Infrastructure and Operations Manager Sandra Lewis – Head of Digital, Programme Management & Customer Services In consultation with the Digital team and Information Governance team
Published Date of Current Version:	January 2026	Approved By:	CLT

1. Purpose

Artificial Intelligence (AI), including Generative AI technologies such as ChatGPT, Microsoft Copilot, Google Gemini, or other similar tools, is rapidly transforming how organisations operate.

This policy sets out the council's responsibilities for ensuring the secure, ethical and responsible use of AI in council activities. This policy also aims to fully utilise the new opportunities to enhance efficiency and service delivery provided by AI while minimising any risks.

2. Scope

This policy applies to all employees, elected Members, contractors, agents, volunteers, representatives, and temporary staff, working for or on behalf of the Council, and our Trading Company East Suffolk Services Ltd, using digital platforms, who will be referred to as 'users' for the purposes of this policy.

This policy applies to all users with access to GenAI and other AI modules, whether through Council-owned devices or undertaking council activity on own devices (BYOD).

3. Responsibilities

Whilst the appropriate use of AI is everyone's responsibility there are some specific roles and responsibilities assigned:

Head of Digital, Programme Management and Customer Services - Responsible for leading development of AI technology as appropriate and ensuring compliance with the AI Policy.

Senior Information Risk Owner (SIRO) - This role is undertaken by the Head of Internal Audit Services who has the responsibility for ensuring the council meets data protection obligations in relation to the use of AI.

All Managers - Ensure that the implications and responsibilities for AI use are understood within all staff recruitment, training, development and in relation to service delivery.

Digital Service Area (the ICT Team) - Responsible for providing overview, training, guidance, development and technical support for AI tools.

4. Policy Statement

While several free AI tools are available, such as ChatGPT, Gemini and others, users must only use AI tools that are authorised. The main provider of general AI tools within East Suffolk Council will be formed from Microsoft Copilot applications. This is because Microsoft Copilot includes enterprise-grade data protection as part of our existing M365 Tenant and licensing arrangements, ensuring council data remains secure, private, and is not used to train foundation models. If Copilot isn't appropriate for certain tasks, users should seek guidance from the Digital team.

A register of authorised AI tools can be found internally on the ICT SharePoint page (for both ESC and ESSL).

Employees shall agree, prior to being authorised to use AI for work purposes, that they will not:

- Violate the law.
- Attempt to use personal data as an input to the AI – to process personal data using AI a Data Privacy Impact Assessment (DPIA) must be completed, Record of Processing Activities (RoPA), legal basis applied, and Privacy Notices updated to reflect the processing. Consent from data subjects may be required, depending on the nature of the processing.
- Attempt to disrupt the information security of any network or device.
- Attempt to create or distribute malicious campaigns or programs.
- Attempt to create Deep Fakes.
- Attempt to disrupt national security.
- Attempt to cause harm or loss to any individual or organisation.
- Attempt to conduct hacking activities.

5. Principles

This AI Policy uses and follows the main principles developed by Central Government for public sector use of AI, set out in the [Artificial Intelligence Playbook for the UK Government \(HTML\) - GOV.UK](#) (First published 10 February 2025) and applicable to all users:

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

To address these principles for East Suffolk Council and translate for the purposes of this policy, the good practice acronym of ‘FAST’ is used, to serve as the foundation for the ethical use of AI in this Policy. This establishes clear expectations for responsible AI practices and reinforces the importance of good governance, expanded upon in the body of this policy document:

F	A	S	T
Fairness	Accountability	Sustainability	Transparency

6. General Use of AI Tools

- 6.1 All users must follow all council policies when using AI tools.
- 6.2 Users may use GenAI and other AI modules for work-related purposes subject to the adherence to this policy. This includes tasks such as generating text or content for reports, emails, presentations, images, or other service-related purposes.
- 6.3 Before using AI for council business purposes, users must have undertaken the mandatory corporate digital skills training provided on AI, which outlines the basis of this policy, how to get the best out of AI and risks to be aware of.
- 6.4 AI tools should be used ethically and with caution and an understanding of their limitations.
- 6.5 Users must not use or procure AI tools without the appropriate consultation and consent. All digital solutions, including AI tools, must be procured through the Digital team in the first instance, in accordance with the ICT Security Policy.
- 6.6 The procurement of any external services should take into account the use of AI by suppliers to the council, even if the goods or services being procured are not of a digital nature, to ensure council related data and services adhere to this policy. The Procurement team should be consulted at the earliest stage of any procurement process as per our Procurement Strategy.
- 6.7 For any new implementation of AI, the Information Governance team must have prior involvement to review compliance with Data Protection legislation, including the completion of a Data Protection Impact Assessment as per Data Protection Policy.
- 6.8 All users must use AI responsibly and ethically, in compliance with council policies and applicable laws and regulations that apply to all council business, including but not limited to:

- 6.8.1 Copyright - Users must adhere to copyright laws when utilising GenAI. It is prohibited to use GenAI to generate content that infringes upon the intellectual property rights of others, including but not limited to copyrighted material. If a user is unsure whether a particular use of GenAI constitutes copyright infringement, they should contact their Manager and the Legal team before using GenAI.
- 6.8.2 Confidentiality - Confidential commercially sensitive information must not be entered into an AI tool, as this information could enter the public domain. If a user has any doubt about the confidentiality of any commercially sensitive information, this should be reported to their Manager and the Legal team, and use of the AI model should be suspended for review.
- 6.8.3 Data Protection - Personal and Special Category data must not be entered into general AI tools, as this information could enter the public domain. All users must follow all applicable data privacy laws and Council policies when using AI and tools. If a user has any doubt about the compliance with the Data Protection legislation, this should be reported to their Manager and the Information Governance team, and use of the AI model should be suspended for review.
- 6.9 If evidence, documentation or information provided by an external party (including a member of the public or customer submitting information to the council) has been created or altered using AI, the party must:
- Disclose AI use when submitting the material, including:
 - The AI tool or system used.
 - The source of the information that the AI system has based its content on.
 - The nature and extent of AI-generated or altered content.
 - The date that you used the AI.
 - Clearly label where AI has been used in the body of the content and in any references to it elsewhere.
 - Declare responsibility for factual accuracy, lawful use, and compliance with ethical, copyright, and data protection standards.
 - For images or video, specify:
 - Whether AI created or altered them
 - What changes were made (e.g., added or removed objects, buildings, or infrastructure)

7 FAST Principles

7.1 Fairness

The council's use of AI should avoid discriminatory harm, especially when processing social or demographic data. To enable this, users should:

- Use only fair and equitable datasets (data fairness).
- Include reasonable features, processes, and analytical structures in the model architecture (design fairness).
- Prevent the system from having any discriminatory impact (outcome fairness).

- Understand bias - AI can display bias, usually because of biased training datasets. In cases where AI tools are being used which may impact on individuals or in the generating of reports for decision making purposes, any bias has the potential to be harmful.
- Implement the system in an unbiased way (implementation fairness) - AI tools must not be used to replace formal decision making and professional judgement. For example, in legal decision-making, for recruitment and hiring, in allocating welfare or supplying insurance.

7.2 Accountability

AI systems must be fully answerable and auditable. To enable this, we must have in place:

- A continuous chain of responsibility for all roles involved in the design and implementation lifecycle of new AI implementations.
- Activity monitoring to allow for oversight and the review of use of AI corporately.
- Accountability for the use of AI that lies with the user.
 - All information generated by AI must be reviewed and edited for accuracy prior to use. Users of GenAI are responsible for reviewing output and are accountable for ensuring the accuracy of the content generated before use/release.
 - If users have any doubts about the reliability of a source, the information must be verified with multiple non-AI sources.
- Awareness - users must not assume that AI-generated sources are reliable without verification. Microsoft states this in their [Transparency Note for Microsoft Copilot](#) about the reliability of Microsoft Copilot (October 2025):

“While Copilot aims to respond with reliable sources where necessary, AI can make mistakes. It could potentially generate nonsensical content or fabricate content that might sound reasonable but is factually inaccurate. Even when drawing responses from high-authority web data, responses might misrepresent that content in a way that might not be completely accurate or reliable. We remind users through the user interface and in documentation like this that Copilot can make mistakes. We also continue to educate users on the limitations of AI, such as encouraging them to double-check facts before making decisions or acting based on Copilot's responses. When users are interacting with Copilot via text, it will attempt to ground itself in high-quality web data to reduce the risk that generations are ungrounded.”

7.3 Sustainability

The technical sustainability of the system ultimately depends on its safety, including its accuracy, reliability, security, and robustness. For this, users should be aware of and take into consideration:

- The transformative effects AI systems can have on individuals and society.
- The real-world impact that the AI system can have.
- That the correct corporate channels have been used to implement the AI solution.
- Risks that the organisation can be exposed to through improper use of AI.
- Security - AI tools may store sensitive data and information, which could be at risk of being breached or hacked. Different types of AI are susceptible to different security risks. Some threats such as data poisoning, perturbation attacks, prompt

injections and hallucinations are specific to AI. However, AI systems can also amplify generic risks such as phishing and cyber-attacks.

- Security risks associated with the use of AI must be assessed and understood, ensuring that safeguards and technical controls are in place. These include security testing and, in the case of generative AI, content filtering to detect malicious activity, as well as validation checks to ensure responses are accurate and do not leak data. Tools should be resilient to cyber-attacks, as laid out in the [Government Cyber Security Strategy](#). As stated in 6.5, The Digital team should be consulted to review the specification of any technology that requires any additional devices or software to be connected to or run on the network before it is procured or used. If a user has any doubt about the security of information input into an AI tool, they should not use it and raise the concern with the Digital team.
- The loading of AI applications for which a licence is required but not held is prohibited and this is also an offence which could lead to disciplinary action (as stated in the ICT Security Policy).

7.4 Transparency

Users with access to AI must disclose when and how AI has been used. Justify the ethical permissibility, the discriminatory non-harm, and the public trustworthiness of its outcome and of the processes behind its design and use.

- Disclosure - All content produced via an AI tool must include a disclosure statement indicating that it contains AI-generated information. This should be annotated at the foot of the document – for example: ‘This document contains content generated by Artificial Intelligence (AI). AI generated content has been reviewed by the author for accuracy and edited or revised where necessary. The author takes responsibility for this content.’
- Users must ensure that any activities within the organisation where AI is used to assist decision-making or processing are declared (for example via a declaration statement on forms, and privacy notices) prior to any processing taking place. This should include what information is used, why it is relevant, and what the likely impact will be on the individual.
- When using approved AI notetaking applications during meetings, it is important that all participants are informed prior to the meeting's commencement. If any attendee raises an objection to the use of such tools, the meeting organiser must carefully consider the nature of the concern. Should the objection remain unresolved, the organiser should assess whether to proceed without the use of AI notetaking.
- Before engaging in externally hosted meetings where AI tools are used by external parties, where data is captured, recorded, or transcribed and may be stored externally and enter the public domain, all participants must:
 - Stop and consider whether appropriate permissions have been obtained to discuss Council-related information in environments where external AI technologies are active.
 - Challenge the use of AI if there is any discomfort or uncertainty. Users are encouraged to speak up, request the removal of AI tools, or terminate the meeting if necessary.

- If you become aware that a meeting involving Council information has been recorded or transcribed using unauthorised AI tools, report the incident immediately to the ICT Service Desk for review and appropriate action.

8 Policy Compliance Concerns

Any non-compliance with this policy should be reported to the Head of Digital, Programme Management & Customer Services and the Information Governance Team.

9 Review

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

10 Glossary of terms

Term	Definition
AI (Artificial Intelligence)	The capability of a machine to imitate intelligent human behaviour, including learning, reasoning, and problem-solving.
Generative AI (GenAI)	A type of artificial intelligence that can create new content such as text, images, or audio based on patterns learned from existing data.
Microsoft Copilot	A generative AI tool integrated into Microsoft 365 applications that assists users by generating content, summarising information, and automating tasks.
ChatGPT	A conversational artificial intelligence model developed by OpenAI that uses natural language processing to generate human-like responses to text inputs. It is based on the Generative Pre-trained Transformer (GPT) architecture and can be used for tasks such as drafting text, answering questions, and summarising information.
Bring Your Own Device (BYOD)	A policy that allows employees to use their personal devices, such as smartphones, for work purposes.
Users	All employees, elected Members, contractors, agents, volunteers, representatives, and temporary staff, working for or on behalf of the Council, and our Trading Company East Suffolk Services Ltd, using digital platforms to carry out council business.
External Party	Any individual, organisation or other third party that is not directly employed by the Council or our Trading Company East Suffolk Services Ltd.

11 Change Log

Version	Date	Author	Description of Change
0.1	14/10/2025	Ben Allen	Initial draft
0.2	24/10/2025	Sandra Lewis	Revisions and comment
1.0	06/01/2026	Sandra Lewis	Approval and final document following CLT