

ARTIFICIAL INTELLIGENCE (AI) POLICY

We will on request produce this Policy, or particular parts of it, in other languages and formats, in order that everyone can use and comment upon its content.

DOCUMENT MANAGEMENT

Version	Date	Changes
1.1	July 2025	Draft
1.2	Sept 2025	Issue

Accountable owner(s)	Name	Policy approval date
AD, Customer Experience and Digital	Mark Burgess	25 July 2025
Senior Information Risk Owner (SIRO)	Nigel Inniss	24 July 2025
Responsible owner(s)		
IT Product Manager	Kevin Taylor	23 July 2025

Policy reviewer(s)		Policy approval date
Corporate Information Governance Board (CIGB)	Peter Knight	31 July 2025
Data Protection Officer and Compliance Manager	Anna Stephenson	24 July 2025

Publication information		Location
All Staff		IRIS (staff Intranet)
IT Staff		IT Docs (SharePoint)
Public		SCC website

1. Introduction

Artificial Intelligence (AI) is several different technologies working together to enable machines to sense, comprehend, act, and learn with human-like levels of intelligence.

Generative Artificial Intelligence (GenAI), such as ChatGPT, Claude and Gemini augment human capabilities and possibilities. GenAI is a type of AI that, as its name suggests, generates new content.

AI-based technologies can now be used to create pictures, write papers, write application code, draft articles and social media posts, and generate videos and audio recordings simply by writing a few sentences (known as prompts). However, while these capabilities help accelerate the creation of knowledge-based content, there are risks. For example, AI-generated results can be misleading due factors such as training model bias, data quality issues, malicious intent, wider source bias, lack of diversity in AI training models or unethical failure to disclose source content, meaning that users could be misled regarding outputs created.

The applications of artificial intelligence (AI) are very varied insofar as they can be general or bespoke and tailored to specific needs and datasets. AI can improve consistency of outcomes, automate systems and provide cost and time savings. The capabilities of AI include machine vision and sensing, predictive and decision making, natural language processing, image and audio recognition, prescriptive modelling, simulation, and data analytics.

GenAI must be used ethically and in compliance with all applicable legislation, regulations, and organisational policies. Users must not use GenAI to generate content that is discriminatory, offensive, or inappropriate. If there are any doubts about the appropriateness of using GenAI in a particular situation, users should consult with their manager or the Information Governance Team.

2. Purpose and Principles

SCC positively encourages the ethical use of AI tools to improve productivity and effectiveness. This policy sets out the Council's framework for the responsible, lawful, and ethical use of Gen AI tools. This policy also aims to ensure that the deployment and use of AI technologies aligns with its values and the rights of individuals either potentially or unintentionally impacted by its use.

For the purpose of this policy, AI refers to computational systems capable of performing tasks that typically require human intelligence and provide autonomous decision making. These include, but are not limited to:

- Machine learning and data-driven prediction systems
- Natural language processing tools
- Computer vision systems
- Robotic process automation (RPA) with autonomous decision-making

(Note: The Council is currently building an AI support network alongside a library of best practice to assist staff in their use of AI.)

3. Scope

This policy applies to all employees, contractors, developers, vendors, temporary staff, volunteers, Councillors, consultants or other third parties (users) involved in:

- Procuring, designing, developing, deploying, or maintaining AI systems;
- Handling data used in AI applications.
- Making or supporting decisions using AI or automated processes.

This policy should be read in conjunction with the following documents:

- Data Protection Policy
- Acceptable use of Information Systems Policy
- Classification and Labelling of Information Policy
- Information Security Incident Reporting Policy
- Records Management Policy
- Social Media Policy
- Software Policy
- Ethical Data Stewardship Charter

There is useful guidance on the Information Commissioner's Office website ([ICO Guidance on AI and Data Protection](#)), which contains recommendations on good practice for organisational and technical measures to mitigate the risks to individuals that AI may cause or exacerbate.

4. Roles and responsibilities

- a. The Council's **Digital, Data and Technology (DDaT) Governance Board**: will be established to monitor compliance with this policy and will review and agree changes to the Policy annually or sooner where appropriate. The Board also has the ability to review and assess usage of tools such as Copilot, and can use captured information to assess its effectiveness as needed.
- b. **Managers**: are responsible for ensuring that adequate induction and training is undertaken by staff and that support is provided to them so as to implement this policy. Line managers have additional responsibilities which are outlined throughout this policy. Managers are also responsible for ensuring that staff read and understand any updated guidance and/or communications, see paragraph (d) below.
- c. **The Monitoring Officer**: is responsible for ensuring that adequate induction and training is undertaken by Councillors and that support is provided to them so as to implement this policy.

- d. **Staff:** AI relies on reliable source data, therefore staff using AI are responsible for checking the reliability of data sources and the outputs created using those data sources.

Staff should attend the appropriate training courses where available on the use of AI which will help staff to use AI safely and responsibly. SCC's modular training is available to all users who have access to the council's data and network. All users must engage with this training and complete all mandatory modules as required. Line managers have a responsibility to support this training and must raise with HR if any staff member does not, or cannot, complete mandated training.

All users are responsible for keeping up to date with any guidance and/or communications about GenAI which may be circulated via internal newsletters e.g. InsideSCC, the intranet e.g. the Information Governance pages, or other bulletins.

Security incidents: all staff must report any suspected security incidents via the IT Service Desk as per current policy.

Non-compliance with this policy may be investigated and dealt with under the Council's disciplinary procedure. In certain circumstances, breach of this policy may be considered gross misconduct resulting in dismissal.

Non-compliance with this policy by Councillors may contravene compliance with the Members' Code of Conduct which may lead to a referral to the Council's Monitoring Officer.

5. AI principles

The Council will ensure that its use of AI is in line with five guiding principles:

1. **Fairness:** to ensure outputs are not influenced by gender, race, age or other discriminatory biases.
2. **Accountability for outcomes:** users of AI tools must take responsibility for any outcomes produced by AI tools, including unintended consequences/risks, for you, your Service or the Organisation. This includes being mindful of possible ownership/copyright considerations regarding image creation as well as textual output.
3. **Transparency:** We have a responsibility to disclose our use of AI in decision making and be able to explain where and how AI has been used in making decisions (and being responsible for the accuracy of those decisions).
4. **Ethics by design:** e.g. building in safeguards to avoid promotion of harmful or extremist content, (see [Ethical Data Stewardship Charter](#) for more details).
5. **Empowerment of the individual:** AI should enhance human autonomy and capability and give users control over how AI affects them.

6. Guidance and risk management

Users who are either using or intending to use AI tools should:

Always consult their Directorates' IT Product Manager/Team. The IT Product Manager/Team will be able to provide advice as to whether the AI tools are appropriate for the purpose(s) for which they are required and/or suggest other suitable alternatives.

SCC's information risk management processes, for example, Data Protection Impact Assessments (DPIA), remain key to management of Data Risk through use of GenAI tools, including legal compliance (fairness, accountability and transparency), ethics by design (for example, bias and discrimination), benefits to individuals, security (including technical protections and security certifications) and data sovereignty and protection.

SCC's Ethics Adviser (this role is currently undertaken by the Data Protection Officer), will also be able to provide advice and guidance to staff in relation to AI products and where appropriate can refer matters to SCC's Data Ethics Advisory Panel. For more information on the Council's Ethical Data Stewardship Charter and the Panel's Terms of Reference refer to <https://suffolknet.sharepoint.com/sites/Intranet-InformationGovernance/SitePages/Data-Ethics.aspx>.

All staff should consider the benefits of AI use weighed against the environmental impact in light of SCC's declaration of a climate emergency and commitment to net zero targets, and the environmental consequences of use of AI when compared to use of non AI tools.

Microsoft CoPilot is the Council's preferred generative AI tool – as it has advanced enterprise data protection capabilities, therefore staff should exercise additional caution regarding Information Governance responsibilities when using other uncontrolled generative AI tools and should always discuss potential usage with IT Product Managers.