Artificial Intelligence (AI)

Usage Policy

Version number 1.1

Publication date: January 2026

Author & Owner: IT & Digital

Review: Corporate Digital Board (annually)

Contents

1. Overview 3

2. Roles & Responsibilities 3

3. Publicly available AI services 5

4. Council Procured AI services 5

5. Procurement and Implementation 6

6. Compliance 7

7. Breaches of Policy 8

8. Review 8

1. Overview

This policy sets out individual responsibilities for the use of artificial intelligence (AI) within East Sussex County Council.

AI is an umbrella term for a range of technologies and approaches, such as Microsoft Copilot, used to mimic human intelligence to solve complex tasks. This policy applies to AI in all its forms including bespoke applications and solutions, or where it is embedded in systems and services, pilot AI projects, or those deployed in production.

AI presents enormous opportunities to streamline operations, drive down costs and increase productivity but also poses risks and challenges. The Council is committed to using AI in a responsible, ethical and lawful manner. The purpose of this policy is to ensure that AI is used in a way that respects the rights and interests of the public, colleagues and other stakeholders as well as being prepared for potential future developments in both technology and regulation. When using AI services our Information Assurance and security policies continue to apply.

This policy applies to **all** colleagues using AI services.
For the purpose of this policy, AI services are split into two categories:

- Publicly available AI services.
- Council procured AI services.

2. Roles & Responsibilities

2.1 Information Governance (IG)

- Provides advice and guidance on data protection and information management matters.

2.2 Information Security (IS)

- Provides advice and guidance on information security, completes risk assessments on new systems and undertakes general supplier assurance.

2.3 Records Management (RM)

- Provides advice and guidance on records management matters as defined in the Records Management Policy.

2.4 Information Asset Owners (IAO)

- An IAO is an individual appointed to ensure that specific information assets are handled and managed appropriately. IAO's are key risk decision makers across assets they own.

2.5 Information Technology (IT&D)

- IT&D is responsible for ensuring Council Procured AI systems meet the council's systems and security requirements.

2.6 Managers

- Managers are responsible for implementing this policy, being aware of the use of AI in their area of responsibility and initiating appropriate risk and privacy assessments.

2.7 General Responsibilities

- You must ensure that AI services are used for clearly defined business purposes that align with the Council's vision, corporate plan, and core values and behaviours. AI services should be used to foster innovation, improve services offered to the residents of East Sussex, improve the efficiency of Council operations or make everyday tasks more efficient for colleagues.
- You must check output for accuracy. AI technology can inherit human bias, can respond inaccurately due to leading questions and can respond based on incomplete data.

- You must ensure that data used by, and the results from AI services are accurate, relevant, complete and up to date.
- **You must not** submit prompts that would lead to issues if they were to be made public.
- The Council will add and remove AI services from use as they become useful or represent a security threat.
- As with all Internet traffic, the Council routinely logs the use of publicly available AI services.
- **You must not** download publicly available AI services, packages or machine learning models to the Council's IT network.
- Documentation must be maintained for all AI systems, including decision logic, data sources, risk assessments and system changes, to support accountability and auditability.

3. Publicly available AI services

Publicly available AI services include platforms such as Bard, ChatGPT, DALL-E and Bing AI. These services are insecure for business purposes.

- You must not rely on publicly available AI services for business purposes.
- You must not input business data into publicly available AI services. This includes data that is commercially, politically or financially sensitive.
- You must not input personally identifiable data.

4. Council Procured AI services

Council procured AI services are those provided through commercial agreements with suppliers through which security is validated. As of November 2025, the key AI service that can be used for business purposes is Microsoft Copilot. This AI use policy does not replace or overwrite regulatory requirements. AI projects must

follow relevant laws and data protection policies. Specifically, AI initiatives involving personal data should be subject to a data protection impact assessment (DPIA). If in any doubt, colleagues should consult their line manager, Information Management and/or Legal Service as necessary.

5. Procurement and Implementation

The following apply to colleagues involved in procuring and implementing AI services:

- You must engage with IT&D and Information Governance before procuring any AI services. An IT risk assessment is always needed and a DPIA / Privacy Notice update or creation may be needed.
- You must ensure that normal Council procurement processes are followed when procuring AI services.
- You must consider relevant standards and best practices for development and deployment.
- Consider involving stakeholders in the design, development and deployment.
- You must ensure that as part of the design and development that human intervention is possible in case of errors, failures or adverse effects of AI services.
- You must assess the risks and benefits of the AI service using appropriate methods and tools, such as impact assessments, equality impact assessments, audits or testing. Risk assessments must consider individual use cases and any changes to the use case will require further assessment of risks.
- You must thoroughly understand supplier terms of use and privacy policies before using AI services to process personal data or sensitive information.
- You must seek assurances from the supplier of AI services that the risk of discrimination or bias is understood and mitigated to an appropriate level.

Further assurance can be obtained through appropriate terms and conditions in contracts and through independent certification if needed.

- Where partnerships are set up that use AI services, a Memorandum of Understanding or similar agreement must be implemented to ensure common principles are adopted by all parties.
- You must monitor the quality of outcomes to evaluate accuracy, reliability and efficiency.
- You must ensure colleagues who use or are involved in the procurement of AI systems are given appropriate training and guidance and that it is refreshed regularly to reflect evolving technologies and risks.
- You must ensure there is a testing strategy that incrementally introduces a new AI service.

6. Compliance

6.1 **Alignment with National Guidance:** The Council's use of AI must align with relevant national frameworks and guidance, including the UK Government's AI Playbook, ICO guidance and NCSC advice.

6.2 **Transparency and Explainability:** AI systems used by the Council must provide clear explanations for decisions that affect individuals or services. Where feasible, outputs should be transparent to those impacted.

6.3 **Ethical Principles:** The Council commits to the ethical use of AI, guided by principles of fairness, accountability, transparency and human oversight. These principles must be considered throughout the lifecycle of AI systems.

6.4 **Data Protection Impact Assessments (DPIA):** A DPIA must be completed prior to deploying any AI system that processes personal data, in accordance with ICO guidance.

6.5 **Incident Reporting and Redress:** Colleagues must report suspected misuse, errors, or harm caused by AI systems to Information Governance. Mechanisms for redress must be made available where individuals are adversely affected.

6.6 **Accessibility and Inclusion:** AI systems must be designed and implemented to be accessible to all users, including those with disabilities, and must not exclude or disadvantage any group.

6.7 **Third-Party and Partnership Governance:** The Council must ensure that third-party providers and partners adhere to equivalent standards for AI governance, especially where data is shared or processed externally.

6.8 **Continuous Monitoring and Audit:** AI systems must be subject to ongoing monitoring and periodic audits to ensure effectiveness, fairness, and compliance with Council policies.

7. Breaches of Policy

Any violations of this policy should be reported to the council's Information Security & Governance Team or senior management. Failure to comply with this policy may result in disciplinary action, in accordance with Council's Human Resources policies and procedures. All council staff have a contractual responsibility to be aware of, and conform to, our Code of Conduct, as well as other relevant employment policies. Breaches of policy may lead to staff being subject to disciplinary action.

8. Review

The AI landscape is dynamic, and this policy is not exhaustive, it will be reviewed and updated annually by the Corporate Digital Board as AI technology, its application and regulation evolve.