Report to:	**Lead Member for Resources and Climate Change**
Date of meeting:	**22 January 2026**
By:	**Chief Operating Officer**
Title:	**East Sussex County Council Artificial Intelligence Policy**
Purpose:	**To seek approval for the East Sussex County Council Artificial Intelligence (AI) Policy to replace the previous reliance on the overarching Data Protection and Information Security policy**

RECOMMENDATIONS

The Lead Member is recommended to:

1) **Approve the East Sussex County Council Artificial Intelligence (AI) Policy as the Council's dedicated framework for the use of AI;**
2) **Note that this policy supersedes the previous approach of relying solely on the Data Protection and Information Security policy for AI governance; and**
3) **Endorse the annual review of the AI Policy by the Corporate Digital Board to ensure ongoing alignment with technological and regulatory developments.**

1. Background information

1.1. This report presents the proposed East Sussex County Council (ESCC) Artificial Intelligence (AI) Policy (Appendix 1) for approval. The policy establishes a dedicated framework for the responsible, ethical, and lawful use of AI across the Council, reflecting the increasing adoption and complexity of AI technologies in local government operations. It is proposed to replace the previous approach, which relied on the existing overarching Data Protection and Information Security policy and will provide clearer, more comprehensive guidance for colleagues and stakeholders.

1.2. AI technologies offer significant opportunities to improve Council services, drive efficiency, and foster innovation. However, they also introduce new risks and challenges, including ethical considerations, data protection, transparency, and the potential for bias. The Council's previous approach relying on existing data protection and information security policies, does not provide sufficient coverage for the unique issues posed by AI. The new proposed policy addresses this gap, ensuring that AI is used in a way that respects the rights and interests of the public, colleagues and other stakeholders.

2. Supporting information

2.1 Key Provisions of the Proposed Policy:

- **Scope:** Applies to all officers using AI services, including both publicly available and Council-procured AI solutions.
- **Roles & Responsibilities:** Clearly defines responsibilities for Information Governance, Information Security, Records Management, Information Asset Owners, IT & Digital, managers and all staff.
- **Publicly Available AI Services:** Prohibits the use of public AI platforms (e.g., ChatGPT, Bard) for business purposes or with sensitive/personal data.
- **Council-Procured AI Services:** Requires risk assessments, Data Protection Impact Assessments (DPIAs) and compliance with procurement and security standards for any AI deployed in Council operations.

- **Compliance:** Aligns with national guidance (e.g., UK Government AI Playbook, Information Commissioner's Office (ICO), National Cyber Security Centre (NCSC)), mandates transparency, ethical use, accessibility and ongoing monitoring.
- **Governance:** Establishes annual review by the Corporate Digital Board and mechanisms for reporting breaches or incidents.

Governance and Oversight

2.2 The Corporate Digital Board will review the policy annually. Information Governance and IT & Digital will provide ongoing support and assurance. All staff are responsible for compliance, with breaches subject to disciplinary procedures.

2.3 The proposed 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 DPIA.

Financial Impact

2.4 There are no direct financial implications arising from the adoption of this policy. However, implementation will require staff training, awareness and periodic audits to ensure compliance and effectiveness.

2.5 AI-related data breaches carry significant regulatory and financial risks under UK General Data Protection Regulation (GDPR). The ICO mandates prompt reporting within 72 hours and holds organisations accountable for misuse, even when third-party AI systems are involved. Failure to conduct proper DPIAs or ensure lawful, transparent processing can result in enforcement actions, reputational damage, and fines. The ICO has signalled a strong stance on AI misuse, especially where personal data is exploited for commercial gain, making robust governance and risk mitigation essential to avoid costly non-compliance.

3. Conclusion and reasons for recommendations

3.1 The proposed ESCC Artificial Intelligence (AI) Policy provides a robust, future-proof framework for the responsible use of AI. It addresses the limitations of the previous approach and positions the Council to harness the benefits of AI while managing associated risks.

ROS PARKER
Chief Operating Officer

Contact Officer: David Matthewman, Interim Chief Digital Information Officer
Tel No.: 01273 335457
Email: David.Matthewman@eastsussex.gov.uk

Background Documents

None