

Staffordshire Police

AI Usage Policy

Generative AI, Large Language Model

Name		Function
Document Author		DDaT
Authorised By		DDaT
QA Approval		DDaT

CHANGE HISTORY

Issue Number	Description of Change	Issue Date
0.1	Baseline – Initial Draft for circulation	TBC
1.0	Release of AI policy	14/11/25

This document will be reviewed every 6 months from its published date.

Next review will be: TBC

TABLE OF CONTENTS

1.	INTRODUCTION.....	3
1.1	Purpose.....	3
1.2	Supersedes.....	3
2.	SCOPE	3
3.	OBJECTIVES.....	3
4.	DEFINITIONS & ACRONYMS.....	4
5.	POLICY STATEMENTS	4
5.1	Which Generative AI tools are permitted for use in Staffordshire Police?	4
5.2	Prohibited Information Types.....	4
5.3	What should I consider when using generative AI?	5
5.4	Intended uses of Generative AI tools in Staffordshire Police	6
5.5	Key Risks of Using Generative AI eg: Microsoft Copilot	7
6.	ROLES AND RESPONSIBILITIES	7
7.	RELEVANT LEGISLATION AND POLICIES	8
8.	EQUALITY IMPACT ASSESSMENT	9

1. INTRODUCTION

1.1 Purpose

This policy sets out the authorised use of and associated considerations relating to generative AI in Staffordshire Police.

Generative AI tools, such as Large Language Models (LLMs), present significant opportunities to make policing more effective and efficient but also present substantial issues with how they are safely used. While they can improve efficiency, support professional development, and aid administrative tasks, their improper use can result in ethical breaches, data protection issues, and damage to public trust and confidence.

1.2 Supersedes

N/A

2. SCOPE

The force SIRO (Deputy Chief Constable) has overall responsibility for data and assurance within Staffordshire Police and is ultimately accountable for all policies and supporting documents of the organisation and its actions. Adherence to this force policy will be expected from:

- All employees (direct or in-direct) and representatives of Staffordshire Police.
- All Officers of Staffordshire Police
- All police staff including police staff employed by the PfCC.

3. OBJECTIVES

This policy will

- Specify which Generative AI tools are permitted for use in Staffordshire Police.
- Provide the list of prohibited information types
- Set out the considerations for their use
- Highlight the intended uses and risks associated with using Generative AI tools
- Set out the expectations for the use of product delivered by Generative AI LLM's.

4. DEFINITIONS & ACRONYMS

Acronym	Definition
SP	Staffordshire Police
AI (Artificial Intelligence)	Technology that allows machines to perform tasks that usually require human intelligence, such as understanding language or making decisions.
Generative AI	A type of AI that can create new content, like text, images, or audio, based on the data it has learned from.
LLM (Large Language Model)	A kind of generative AI trained on large amounts of text to understand and produce human-like language.
Copilot	Microsoft's AI tool approved for use in Staffordshire Police, integrated into Microsoft 365 applications.
Special Category Personal Data	Sensitive personal information such as race, religion, health, or sexual orientation, which requires extra protection.
CHIS (Covert Human Intelligence Source)	A person who provides information to the police in secret, often about criminal activity.
DPO (Data Protection Officer)	The person responsible for ensuring Staffordshire Police follows data protection laws and handles personal data properly.
MOPI (Management of Police Information)	National guidance on how police information should be handled, stored, and shared.
SIRO (Senior Information Risk Owner)	The senior individual responsible for understanding and managing information risks that could impact the organisation's strategic goals.

5. POLICY STATEMENTS

5.1 Which Generative AI tools are permitted for use in Staffordshire Police?

Only Microsoft Copilot tools accessed via Staffordshire Police-issued devices and authenticated through the official Staffordshire Police Microsoft 365 environment are permitted.

The use of ChatGPT, Deepseek, Gemini, Perplexity or any other publicly available LLM or generative AI tool are prohibited and **must not be used** in any way for Staffordshire Police purposes or accessed on Staffordshire Police-issued devices.

If new solutions are procured or upgraded that have generative AI capabilities, separate approval of the use will be required along with assurances from the supplier and the associated models.

5.2 Prohibited Information Types

To mitigate data transfer risks and protect sensitive operations, **under no circumstances** should the following types of information be entered, pasted, uploaded, or otherwise submitted into Copilot Chat:

- Information Classified Above OFFICIAL:
 - Any data marked or implicitly classified as SECRET or TOP SECRET.
 - Copilot Chat is approved for information classified as OFFICIAL (including information marked as SENSITIVE) only.
 - Legacy information classified under the Government Protective Marking Scheme (GPMS) should not be used with Copilot Chat.
- Special Category Personal Data:
 - Direct or detailed input of Special Category Personal Data (revealing racial/ethnic origin, political opinions, religious beliefs, trade union membership, genetic/biometric data for identification, health, sex life/orientation) is prohibited.
 - *Note:* Incidental references within a broader context (e.g., "suspect was arrested near the church," "witness described assailant as white male") may be permissible if necessary for the task and the primary focus is not the special category data itself. However, avoid detailed descriptions or analysis centred on these characteristics. Exercise caution and minimise use.
- Covert Human Intelligence Sources (CHIS) Related Information:
 - Any data identifying or potentially identifying CHIS, handlers, or related operations.
- Information Subject to Specific Handling Caveats:
 - This includes, but is not limited to:
 - UK EYES ONLY (UKEO)
 - Information designated under specific international agreements with handling restrictions.
 - Legally privileged information.
- Sensitive Operational Policing Data:
 - Avoid inputting highly sensitive operational details, such as specific tactics in active use, uncorroborated intelligence, or detailed profiles of ongoing covert operations.
 - General discussion or summarisation of concluded, non-sensitive operational reports may be acceptable if other restrictions are met. Focus on business objectives and avoid inclusion of sensitive operational specifics.
- Personal Data of Vulnerable Individuals:
 - Specific details relating to victims, witnesses, or suspects identified as particularly vulnerable, where disclosure could lead to harm.
- System Credentials:
 - Passwords, API keys, private certificates, IP addresses, solutions designs or any other system access credentials. Discussing general system configurations, non-critical vulnerabilities for analysis, or network architecture concepts is permitted if this is necessary for SP digital services work.

Guiding Principle: If you are unsure whether a piece of information is suitable for use in Copilot Chat, do not input it. Consult your line manager or the Data Protection Officer (DPO).

5.3 What should I consider when using generative AI?

The use of generative AI and LLM's in policing is new. It is complex technology that appears to have obvious and immediate benefits across a range of policing activities so it is likely that officers and staff of all ranks and roles will quickly experiment and adopt its use with well founded good intentions.

However, there are number of risks that are real, likely to occur and have the potential to have a high impact on individuals and public confidence in policing as a whole. Users are therefore expected to be cautious and professional. Although the below section will highlight a number of benefits and risk associated with the use of LLM's, there are a few simple steps that users can take to significantly reduce the risks of using generative AI.

1. Only use AI tools that are authorised – at this time this is only CoPilot
2. Think before use – is the use of AI in this case, sensible, appropriate and ethical?
3. Protect our data – keep personal information secure, and out of the AI unless absolutely necessary
4. Check the results – AI is not 100% reliable and you must always read and verify anything produced – be accountable for where outputs are used.
5. Be transparent – Don't claim AI produced work as your own. Although there is no need to declare every use of AI such as for note taking, drafting work you heavily edit or for research, transparency is essential to maintain the public trust so always declare the use of AI in any formal report, creative content or when it is used in decision making. Use a note such as, "*Microsoft Copilot supported the creation of this document*".
6. Report any concerns – raise any concerns, mistakes or breaches as soon as possible with your supervisor or the Data Protection team. The sooner we know about issues the sooner we can mitigate the impact.

5.4 Intended uses of Generative AI tools in Staffordshire Police

CoPilot is intended for use in the following types of activities

1. Productivity and Admin Support
 - Draft emails, reports, and meeting notes
 - Summarise documents or transcripts
 - Improve clarity and tone of writing
 - Create templates, checklists, or standard replies
2. Data and Analysis
 - Explain data trends or summaries
 - Generate charts or visual summaries (with Excel/Power BI)
 - Assist with basic calculations or data interpretation
3. Knowledge and Research
 - Answer questions based on policies or public info
 - Summarise legislation or guidance (non-legal)
 - Provide overviews of complex topics
4. Idea Generation and Planning
 - Brainstorm ideas for campaigns or strategies
 - Draft vision statements or objectives
 - Structure presentations or briefings

Important note:

Users must review all content before making decisions or acting based on Copilot's responses as AI tools can make mistakes

5.5 Key Risks of Using Generative AI eg: Microsoft Copilot

1. Bias and Stereotyping
 - Copilot may reflect societal biases found in its training data.
 - It could unintentionally reinforce stereotypes (e.g., gender, race, profession).
 - Mitigations are in place, but not all harmful content can be fully prevented.
2. Overrepresentation or Underrepresentation
 - Some groups may be over- or under-represented in responses.
 - Legitimate content (e.g., LGBTQIA+ topics) may be filtered or misrepresented.
 - Microsoft uses classifiers and prompt adjustments to reduce this risk.
3. Inappropriate or Offensive Content
 - Copilot might generate content that is offensive, controversial, or inappropriate.
 - This includes images, text, or audio that may contain harmful symbols or themes.
 - Safeguards are in place, but some content may still slip through.
4. Information Reliability
 - Copilot can produce inaccurate or misleading information.
 - It may "hallucinate" facts or misrepresent sources.
 - Out of date information can be presented in AI results without acknowledging changes or updates.
 - New models are in constant development and learn in different ways which could result in a variation in results.
 - Users should always verify important information and sources before acting on it.
5. Multilingual Performance
 - Copilot performs best in English.
 - Other languages may have reduced accuracy or fluency.
 - Improvements are ongoing to address this.
6. Audio Input Limitations
 - Voice input may be affected by noise, accents, or unclear speech.
 - Copilot Voice does not support web searches, limiting real-time updates.
7. Internet Dependence
 - Copilot requires a stable internet connection.
 - Connectivity issues can affect performance or availability.
8. Data Leakage
 - Users should also submit information to the correct data classification level.
 - Personal Data of victims, witnesses or suspects being leaked.

6. ROLES AND RESPONSIBILITIES

Strategic Lead AI

- Oversees the development, review, and communication of the Generative AI policy.
- Ensures policy compliance across the force and coordinates updates in response to legal, technological, or operational changes.
- Liaises with national bodies and internal stakeholders to align with best practices.

Data Protection Officer (DPO)

- Provides guidance on data protection compliance in relation to AI use.
- Reviews reported incidents or breaches involving AI tools.

- Supports risk assessments and data protection impact assessments (DPIAs) where applicable.

Line Managers / Supervisors

- Ensure their teams understand and comply with the policy.
- Act as the first point of contact for questions or concerns about AI use.
- Escalate any misuse or incidents to the DPO or Strategic Lead.

IT and Digital Services Team

- Manages access to authorised AI tools (e.g., Microsoft Copilot).
- Ensures technical safeguards are in place to prevent unauthorised use.
- Monitors system usage and supports secure integration of AI tools.

All SP Staff and Officers

- Use only authorised AI tools in accordance with this policy.
- Avoid inputting prohibited or sensitive information into AI systems.
- Verify AI-generated content before use and maintain transparency in formal outputs.
- Report any concerns, errors, or breaches promptly to their supervisor or the DPO.

Training and Development Team

- Develops and delivers training on responsible AI use.
- Ensures staff are aware of the risks, benefits, and ethical considerations of generative AI.

7. RELEVANT LEGISLATION AND POLICIES

[Code of Ethics | College of Policing](#)

Data Protection Act

Equality Act

Freedom of Information Act

8. EQUALITY IMPACT ASSESSMENT

This policy has been developed with consideration for the potential risks and benefits of generative AI use across all protected characteristics. It aims to prevent discrimination, promote equality of opportunity, and foster good relations by ensuring responsible and ethical use of AI tools.

	What impact has this policy had on the nine protected characteristics in relation to the three general duties? (If applicable)	How will this updated policy positively impact each of the nine protected characteristics in relation to the three general duties? If not, explain why it will not.
Age (including children and young persons)	No negative impact identified. The policy applies equally to all age groups.	Promotes inclusive use of AI tools and ensures outputs do not discriminate based on age. Encourages review of content to avoid age-related bias.
Disability	No adverse impact identified. AI tools may support accessibility.	Supports productivity for staff with disabilities through features like summarisation and drafting. Encourages review to avoid discriminatory content.
Gender Reassignment	No negative impact identified. Policy prohibits discriminatory or biased outputs.	Reinforces respectful and inclusive language. Promotes awareness of potential bias in AI-generated content.
Pregnancy & Maternity	No direct impact identified. Policy ensures sensitive data is protected.	Prevents misuse of AI in ways that could expose or mishandle personal data related to pregnancy or maternity.
Marriage & Civil Partnership	No direct impact identified.	Ensures AI tools are not used in ways that could lead to discrimination based on marital or partnership status.
Race	Recognises the risk of racial bias in AI outputs.	Promotes vigilance and correction of racially biased content. Supports equality by requiring review and transparency.
Religion or Belief	No negative impact identified.	Encourages sensitivity in AI-generated content and prohibits offensive or inappropriate outputs.

Sex	Acknowledges potential for gender bias in AI tools.	Promotes fair representation and requires users to identify and correct biased outputs.
Sexual Orientation	Recognises risk of underrepresentation or misrepresentation.	Supports inclusion by requiring users to report and address biased or inaccurate content related to LGBTQIA+ topics.