WARWICKSHIRE POLICE	**POLICY**

Security Classification	**Official**
Disclosable under Freedom of Information Act 2000	YES

POLICY TITLE	**Artificial Intelligence**
REFERENCE NUMBER	**WP308**
Version	**1.1**

POLICY OWNERSHIP	
DIRECTORATE	Data, Strategy & Technology
BUSINESS AREA	Information Assurance

DATE FIRST IMPLEMENTED	**24/09/2025**
CURRENT VERSION EFFECTIVE FROM	**02/11/2026**
REVIEW DATE	**02/11/2028**
RISK RATING	**High**
EQUALITY ANALYSIS	**Medium**
TIER	**1**

Warwickshire Police welcome comments and suggestions from the public and staff about the contents and implementation of this policy. Please e-mail policiesandprocedures@warwickshire.police.uk

Contents

1.0 POLICY OUTLINE 3
2.0 PURPOSE OF THE POLICY 3
3.0 IMPLICATIONS OF THE POLICY 4
4.0 ROLES AND RESPONSIBILITIES 4
5.0 PROHIBITED USE OF EXTERNAL AI SYSTEMS 5
5.1 What MUST I consider when using generative AI? 6
6.0 GOVERNANCE 6
6.1 AI Usage Principles 6
6.2 AI Approval Process 7
6.3 Post-Approval Oversight: 8
6.4 External Use and Collaboration. 8
6.5 Ethics 8
6.6 AI Documentation Requirements 8
7.0 DOCUMENT HISTORY 8
8.0 CONSULTATION 9
9.0 REVIEW 9
Appendix 1 - KEY DEFINITIONS 10

1.0 POLICY OUTLINE

Artificial Intelligence (AI) is continually undergoing rapid development and there now exists a growing range of both free and paid AI tools available for people to use in ways that can make their day-to-day life, including their job, easier and more effective to complete.

In recent years we have seen Artificial Intelligence (AI) technologies become embedded in society and our daily lives.
AI technologies have huge potential to support the work of the policing community. AI is already in use across policing, and there is no doubt there are many more opportunities for its use.

At the same time, current AI systems have limitations and risks that require awareness and careful consideration by the policing community to either avoid or sufficiently mitigate the issues that can result from their use in police work.

With the recent developmental leaps in AI capabilities, particularly around generative AI, the public debate around legal and ethical implications of AI systems, as well as the negative effects they could have on society and humanity, has gathered momentum. This Policy does not seek to address the legal or ethical implications as these must be addressed on a use case basis, but staff need to be aware that these must be considered, and that uses of AI must receive appropriate governance sign off before they proceed.

This policy covers all Warwickshire Police Staff and Officers, Contractors, Specials and Volunteers and the OPCC.

2.0 PURPOSE OF THE POLICY

The ways in which Warwickshire Police staff and officers may wish to use AI to support their roles are many and varied, and as such this policy does not aim to define a fixed list of permitted uses of AI but will provide examples of safe usage. Rather, this policy aims to ensure appropriate, responsible staff use of AI by defining some key controls which will apply to all staff use of AI.

However, due consideration needs to be given to the privacy risks associated with AI as many of these tools develop themselves by retaining and processing any data inputted into them. In other words, any law enforcement, confidential or personal data typed into a non-Force endorsed and approved AI tool may be saved by the tool and then shared with other users anywhere in the World.

The newness of AI systems and their potential for driving dramatic change or unearthing crucial business insights suggests that these systems demand an entirely fresh set of control requirements to monitor, police and curate them. This is not necessarily the case. These systems in many ways are similar to existing technologies in use across policing organisations today, making them manageable in the same way as those familiar systems.

Most control requirements relating to the acquisition and use of AI and AI-based solutions can be found in the existing standards which have been written, or are being written to support the National Policing Community Security Policy and Principles, and will apply to AI tools and AI integrated tools, just as they do to any other digital solution, however AI tools and AI integrated solutions can present a unique set of vulnerabilities, and so the requirements below are to address these.

3.0 IMPLICATIONS OF THE POLICY

3.1 This policy has implications for adherence with the following and due regard should be had to those documents and legislation and the obligations placed upon the Force.

This policy and associated procedures support compliance with legal, national and best practice standards including:

- Freedom of Information Act 2000
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Equalities Act 2010
- Human Rights Act 1998
- Crime and Disorder Act 1998
- Computer Misuse Act 1990
- Official Secrets Act 1989
- Government Security Classifications June 23
- Artificial Intelligence Toolkit (Interpol) June 2023
- ChatGPT – Impacts on Law Enforcement – August 2023
- Principles for Responsible AI Innovation (Interpol) June 2023
- A guide to using artificial intelligence in the public sector (Gov.UK) June 2019
- NPCC Principles for Using Artificial Intelligence in Policing – July 2023
- Principles for the security of machine learning NCSC – Aug 2022
- Covenant for using AI in Policing V1.1 – Sept 2023
- NPCC AI Playbook
- NPCC AI Checklist
- PDS AI & Copilot DPIA/Blueprint and Guidelines

Failure to comply with the policy could result in impact on:

- Legal compliance
  - Breach of Data Protection Act 2018 or other applicable law
  - Loss of Court Cases due to evidential issues
- Finance
  - Data Protection Fines of circa 17.5 million pounds or 4% of turnover for personal data breaches
  - Cost of managing, investigating and recovering from incidents
- Personal
  - Risk of harm to individuals if information is subject to unauthorised disclosure, inaccurate, or unavailable.
- Reputation
  - Loss of reputation and public confidence in the police.
  - PSD may investigate any inappropriate uses of AI.

4.0 ROLES AND RESPONSIBILITIES

Director of Data, Strategy & Technology

- Oversees the development, review, and communication of the AI policy.

AI Force Lead

- Liaises with national bodies and internal stakeholders to align with best practices.
- Represents the Force at National AI Committees and Boards.
- Ensures policy and process compliance across the force and coordinates required updates in response to legal, technological, or operational changes.

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.

AI Project Team
- Ensures staff are aware of the risks, benefits, and ethical considerations of generative AI

Learning & Development
- Develops and delivers training on responsible AI use.

Line Managers / Supervisors
- Ensure their teams understand and comply with the policy.
- Act as a conduit between their teams and the central AI support for any issues/questions.
- Escalate any misuse or incidents to the DPO or AI Lead

Digital Services Team & Cyber Security
- 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 Warwickshire Police Staff and Officers (Inc Specials/Volunteers/OPCC)
- Use only Force authorised AI tools in accordance with the AI Policy and this guidance.
- Avoid inputting prohibited or any information classified above Official Sensitive into AI systems.
- Verify all AI-generated content before use and maintain transparency in formal outputs that AI has been used.
- Report any concerns, errors, or breaches promptly to their supervisor or the DPO.

5.0 PROHIBITED USE OF EXTERNAL AI SYSTEMS

The Force has taken the decision to block access to externally hosted GenAI platforms such as ChatGPT/DeepSeek/Grok/Claude etc. and other AI based software such as Grammarly due to the global hosting and data reuse nature of these platforms.
The reality is once data is entered into these services, we as a Force lose all control of that data, the data is used to train the LLM's and risks other users of those LLMs being able to extract that data via prompts.

While we know many colleagues will make use of these products in their personal lives, we cannot allow any Force derived personal, special category or law enforcement data to be input in these external no Force endorsed systems for these reasons.
We risk both reputational and financial harm should personal or sensitive operational data linked to the Force be exposed on these platforms.
This means that no one to whom this Policy is applicable should use these services on personal devices to undertake any such Force work as defined above, and this would be treated as misuse of Force data.

The Force has, and will continue to, implement suitable AI products that we have more control over and assurance of. These include systems hosted within our own cloud/on prem environment as well as externally hosted systems/ or 3rd party software that meet our governance requirements for example CoPilot and Briefcam.

5.1 What MUST 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 and approved.
2. Do not send any data outside of the Force to make use of things unapproved AI models such as ChatGPT/Gemini/Grok/Claude etc on personal devices.
3. Think before use – is the use of AI in this case, sensible, appropriate and ethical?
4. Check the results and verify the sources of the information/outputs – AI is not 100% reliable and you must always read, check and verify anything produced
    a. If using AI for technical assistance such as "vibecoding", ensure that you are knowledgeable in that area and able to fully validate any output ensuring stability and security.
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 then heavily edit or for background 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", or add the Force authorised AI Logo (found on The Bear).
6. Report any concerns – raise any issues, mistakes or breaches as soon as possible with your supervisor and the Information Assurance team. The sooner we know about issues the sooner we can mitigate the impact.
7. Generative AI is not authorised for use in the Criminal Justice system for the creation of evidential materials. This means it must not be used in the preparation of witness statements, MG forms, or any other evidential reports.
   However, Generative AI may be used to support investigators in understanding evidence or assisting with the investigative process, provided it is not involved in the generation of any official evidential documentation. Please accompanying guidance document for more details

6.0 GOVERNANCE

6.1 AI Usage Principles

- **Data Protection and Security**: We prioritise the protection, privacy and security of personal data (both service user and staff). All data collected will be handled in compliance with relevant regulations and used for improving or delivering our services and complying with legal obligations.
- **Transparency:** We are committed to transparency in how our systems operate. We will inform users about the capabilities and limitations of our AI technologies. Where appropriate will consult more broadly on the use and impact of AI.
- **Explainability:** AI systems must provide a level of explanation proportionate to their purpose, risk and potential impact. Where AI informs a decision affecting an individual or the public, the

responsible decision-maker must be able to understand and explain the relevant output, its limitations and how it contributed to the decision. An inability to provide an appropriate explanation may prevent the system or use case from being approved.

- **Bias Mitigation:** We will work to identify and mitigate biases in our AI systems to ensure fairness and inclusivity in all aspects of our services.
- **Accountability:** We take responsibility for the outcomes of our AI systems and are open to feedback and accountability mechanisms from users and stakeholders.
- **Continuous Improvement:** We will strive for continuous improvement in our AI technologies through research, development, and collaboration with experts in the field.
- **Ethical Use:** We will adhere to ethical principles in the development and deployment of AI, avoiding harm to individuals, communities, or society as a whole.
- **Accessibility:** We will design our AI systems to be accessible to all users, regardless of their abilities or background, and will ensure compatibility with assistive technologies.
- **Education and Awareness:** We will promote education and awareness about AI technologies, their potential impact, and how users can make informed decisions about their use.
- **Regulatory Compliance:** We will comply with all relevant laws and regulations governing AI technologies.

6.2 AI Approval Process

All introductions of new AI capabilities or operationally impactful use cases in Warwickshire Police must go through a clear governance and approval process**.** This ensures we assess risks, legal compliance, and ethical implications **before** deploying AI, and maintain oversight throughout its use.

The Force has clear and established routes in regard to change projects, procurement and assurance activities and these remain as is.

Therefore, any AI project that requires involvement from the procurement team/change team or Information Assurance or represents a significant and new use of Force data will require:

- Report to Business Review Board
- Report to Change Board
- Information Assurance – AI DPIA and Responsible AI Checklist Completion, 3rd Party Supplier Checklist
- Cyber Security Review.
- Initial review of the above by the Data, Application and AI Board – who will check for validity/alignment to strategic priorities and fit with current project resourcing.
- Consultation with the Ethics Board – to gather critical feedback for consideration. Please note that not all AI usage will require this step please see section 6.5 Ethics below.
- Final review of the above by the Data, Applications and AI Board**.**
  The decision of the DAAIB is final. No AI solution may be rolled out without its endorsement. If approved, the project can then proceed to technical review.
- For any Criminal Justice usage – that being information which may be evidential in nature, there is a national approval process called the JoP which includes CPS and Police AI colleagues, the Force cannot approve any such uses without approval of the JoP.

6.3 Post-Approval Oversight

Once deployed, AI tools will be subject to ongoing oversight and periodic review:

- The owning department must monitor the AI's performance, its outputs, and any incidents or near-misses. Any unintended outcomes or **"**drift" in the AI's behaviour should be reported to the DAAIB. For example, if an AI starts showing bias in results or users encounter concerning errors, it should trigger a review.

- The DAAIB will conduct a formal post-implementation review (typically after an initial trial period) to ensure the tool is delivering expected benefits, implementation and adoption is as expected and not causing unforeseen issues. Thereafter, regular check-ins (e.g. annually) may be required, especially for high-risk AI systems.

- Significant changes to an AI system (new features, new data sources, etc.) or proposals to repurpose it for new tasks must go through re-approval.
  AI use is not "set and forget" – it requires life-cycle governance.

6.4 External Use and Collaboration.

If the Force engages in collaborative projects involving AI (e.g. with other forces or third parties), or if using cloud-based AI services, the same governance principles apply. Ensure data sharing agreements are in place and partners adhere to equivalent standards.

By following this governance process, we aim to ensure AI is introduced safely, ethically, and with proper accountability. This rigorous oversight is critical to manage the complex risks of AI and to maintain public confidence.

6.5 Ethics

It is not envisaged that all uses of AI will require full ethical review, examples of things that will not need full ethics review are the use of Robotics such as RPA or similar functionality that is deployed within existing Force systems for improving workflows or simple productivity.
These will however still be subject to the assurance steps above and require human oversight, intervention and monitoring.

6.6 AI Documentation Requirements

For each AI project the following will be required as part of the complete assessment process:

- Board Reporting – Business Review/Change Board/DAAB/Ethics Board.
- DPIA for AI projects.
- Responsible AI Checklist.
- EIA
- Supplier Checklist (issued through procurement).
- Data Processing Contract (where applicable).
- Cyber Security Risk Assessment
- Technical Diagrams – Network/Infrastructure

7.0 DOCUMENT HISTORY

Please state which Head of Department or Chief Officer has been consulted on and approved this procedure:

Business Area Manager/Officer consulted	***Date Approved***
Jon Belcher (ChSupt) Director DSTI	***28/09/26***

The history and rationale for changes to this Procedure will be recorded using the chart below:

NAME	**CHANGE**	**DATE APPROVED**
Sara Smith, Head of Information Assurance	New policy	18/09/2025 (Exec Board)
Sara Smith – HoIA	Minor amendments for clarity on personal data/non evidential usage.	26/09/2026 (Digital Application and AI Board) Republished 02/11/2026

8.0 CONSULTATION

Digital Services
Cyber Team
HR
AS&I
Digital and Application AI Board

9.0 REVIEW

As a minimum, this policy should be reviewed in accordance with the timeframes set by the tier level process. The Head of Department/Chief Officer may request a review at any time prior to the standard review date being reached.

Appendix 1 - KEY DEFINITIONS[1]

There are many definitions available for Artificial Intelligence (AI). For the purposes of this document, we have adopted and expanded on the definition provided by the NPCC endorsed – 'Principles for Using Artificial Intelligence (AI) in Policing', written by Science & Technology in Policing. While we reference AI throughout this document, it is intended that reference to AI, covers all of the below.

What is Artificial Intelligence?

There is no definitive definition of Artificial Intelligence (Alan Turing Institute, 2021), and AI is often used to refer to related applications such as automation, neural networks, and machine learning. To bring clarity for policing, we adopt the following definitions:

- **Artificial intelligence (AI)** – Technology that allows machines to perform tasks that usually require human intelligence, such as understanding language or making decisions.

- **Machine learning (ML)** refers to algorithms that leverage new data to improve their ability to make predictions or decisions, without having been explicitly programmed to do so. ML is a widely used form of AI that has contributed to innovations such as speech recognition and fraud detection.

- **Advanced Data Analytics (ADA)** uses subject matter expertise and techniques that are typically beyond those of traditional business intelligence to extract insights and make recommendations from complex data. The techniques vary widely, from data visualisation to complex linear models to language analytics. An example is the use of Risk Terrain Modelling to quantify environmental factors that shape risk mapping and resource deployments.

There is other related AI terminology, which start to overlap with the above, but are included here for completeness. The above and below are considered the most common, but there are others. The additional definitions are:

- **Generative Artificial Intelligence (GAI)** is artificial intelligence capable of generating text, images, or other media, using generative models. Generative AI models learn the patterns and structure of their input training data and then generate new data that has similar characteristics.

- **Large Language Models (LLMs)** are a subset of GAI, where an algorithm has been trained on a large amount of text-based data, typically scraped from the open internet, and so covers web pages and - depending on the LLM - other sources such as scientific research, books, or social media posts. Examples include ChatGPT, Google Bard and Meta's LLaMA.

- **Natural Language Processing** is a computer's attempt to "understand" spoken or written language. It must parse vocabulary, grammar, and intent, and allow for variation in language use. The process often involves machine learning

[1] Taken from NPCC/PDS Cyber Security Framework for Artificial Intelligence.