Ongoing monitoring

Guidance on the continuous monitoring of artificial intelligence (AI) and evolving technologies

First published 17 June 2025

4 mins read

If your force decides to adopt the tool or system as business-as-usual, the evolving nature of the technology means that you will need to put in place arrangements to continue testing it periodically. This will enable you to see if any unwanted patterns or biases have crept into how it operates.

It is advised to appoint an ongoing product manager to monitor for problems such as data drift or concept drift, to track the vulnerabilities identified through the validation and evaluation, and to ensure the resilience of mitigation put in place. For more information go to Implementation page of the **Machine learning guide for policing**.

Thresholds should be put in place that, if breached, will trigger human review, retesting and retraining, as well as re-referral to your ethics committee or ethical scrutiny mechanism. Even if thresholds have not been breached, there should be regular intervals established at which the tool or system will be retrained and retested, with the frequency and extent of testing proportionate to the risks posed by the tool.

If your force is licensed to use the tool or system by a supplier, watch out for upgrades and other changes that could have an impact on performance and compliance. The force will need to have contingency plans if an unacceptable risk is identified and the cascade effects on other systems of stopping the AI will need to be mapped and understood. Make sure there is a process in place for escalation of complaints concerning the AI from both within the organisation and outside.

AI and the workforce

The officers and staff who use these tools and systems will need to:

- know how to use them in line with force policy
- understand risks and limitations to avoid over-reliance
- remember that humans make the decisions, not the AI

Reminders of these limitations can be built into the design of the tools or systems – for example, by accompanying AI-generated answers with a disclaimer that they may not be fully reliable, complete or unbiased. Officers and staff will also need to know the data that a tool or system's outputs are derived from, as well as the associations and correlations it makes, so that they can make informed decisions on how to use its outputs and explain those decisions when required.

As AI becomes increasingly integrated across forces and the wider service, it is advisable that all officers and staff acquire basic AI literacy. Officers and staff can access **e-learning on AI fundamentals** (you will need to log in to College Learn).

Even when used appropriately, AI tools and systems can generate inaccuracies that may affect operational decisions. Chief constables are responsible and accountable for the technologies they procure and authorise for use in their force, including their safety and integrity.

Chief constables will need to satisfy themselves that there are clear and effective decision-making processes in place for each operational setting in which the AI will be deployed. To fulfil that duty, forces will need to develop a suite of policy procedures that detail the framework and standard operating procedure for AI tools and systems introduced to the force.

This will need to include policy documents that outline the command structure for deployment, including force-level strategic oversight, decisions to deploy (if the tool or system is to be deployed for specific operations, rather than continuously), and deployment on the ground. The 'Developing operational practice guidance' section of the **Data-driven technologies APP** provides information on how to approach this. The **NPCC AI Playbook** also discusses the roles and responsibilities in deploying AI. Go to the **Getting started** section and **Roles and responsibilities** section for more information.

Force policy will also need to set out the required level of human oversight and quality assurance for each AI-derived tool or system, as well as contingencies for failure and avenues for users of AI to raise concerns. The **Responsible AI checklist** includes considerations that should inform the approach to quality assurance (for more information, go to sections B and C of the checklist). High risk uses of AI by forces, such as live facial recognition, should be underpinned by expert legal advice.

The aim of these measures is to ensure that the force fully equips and properly supports officers and staff when they use AI. They do not, however, release officers and staff from their own

responsibilities to adhere to the law, professional standards, and policing's Code of Ethics in their use of AI. Their use of these tools also needs to be underpinned by their professional judgement on when to follow or depart from what AI recommends.

Tags

Artificial intelligence