Selecting and working with suppliers

Artificial intelligence (AI) specific considerations for partnering with a supplier

First published 17 June 2025

3 mins read

For forces going down the route of partnering with a supplier, the **Data-driven technologies authorised professional practice** (APP) emphasises the need for an informed and strategic approach to procurement, and signposts resources that will help you. The following considerations are specific to artificial intelligence (AI).

Legality, safety and ethics

The PROBabLE Futures and National Police Chiefs' Council (NPCC) **Responsible AI checklist** is the recommended checklist for forces to use when assessing the responsible nature of AI technologies or the specific application of that technology. It brings together technical, operational, legal and ethical aspects, and it is living document that will be updated periodically.

The checklist is grounded in the principles set out in the **NPCC AI Covenant** and the **Data ethics APP**. It includes case studies that show how to apply it, with examples of product features and results that constitute red, orange and green flags.

As well as guiding your procurement process, the checklist should underpin the scrutiny of the project by a specific data ethics committee or whichever other mechanism you are using. For more information go to the **Governance section** of this guidance.

Security

Note that the checklist focuses on legal and ethical use of AI. It is advised to seek robust assurances around the following aspects of information security, as adapted from Norfolk and Suffolk Constabularies' risk assessment questionnaire:

- whether the tool or system is secure by design
- whether force data will be encrypted both in transit and at rest, and at what level
- the extent of penetration testing and user acceptance testing performed to date

- the approach to change and version control
- the security controls to prevent force data going into the open internet
- if it is a shared resource used by several organisations, the controls that are in place to segregate users' data
- all the purposes for which force data will be used by the supplier
- whether force data will be stored, processed and managed in the UK and if the force's consent will be sought if any of these processes move outside the UK
- the real-time monitoring and response systems that will be in place

This is a non-exhaustive set of issues that you may want to ask about. Create your full list in collaboration with your information security team and supplement this with questions resulting from the bespoke risk assessment prepared by your information security team. Find out more in the **Risk section** of this guidance.

Being a discerning customer

When dealing with prospective suppliers, you should engage your force’s procurement expertise to establish the best routes to market and strategies for selecting and working suppliers. It is also helpful to be equipped with:

- a clear problem statement
- a clear understanding of budget and an awareness of the potential for hidden costs
- an assessment from your IT department on what data is available and the state it is in
- knowledge of which systems an AI tool or system will interoperate with
- a clear understanding of the balance of risk you want to agree with the supplier. Which risks does it makes sense for your force to own, and which should be owned by the supplier?
- strategies for avoiding vendor lock-in. These could include:
  - basing the relationship on rolling short-term contracts
  - requiring that tools are supplier-agnostic and technology-agnostic
  - requiring that intellectual property implications are fully assessed (for example, if any new algorithms are being generated or if an existing one is being retrained on your force’s data, which could give rise to new intellectual property)
  - request open source and open standards (standards that are freely available for adoption, implementation and updates, such as XML, SQL and HTML)

- stipulate in the contract when their involvement will end, as well as a requirement for them to upskill your force and to transfer any required knowledge before that point
- ensuring that any ongoing relationship is limited to maintenance and repairing faults

Further guidance go to GOV.UK **Guidelines for AI procurement**.

Tags

Artificial intelligence