Embed

This page is from APP, the official source of professional practice for policing.

First published 17 June 2025

11 mins read

Purchasing strategy

- **Objective:** Ensure that, wherever possible, the force is procuring and developing interoperable products that can be iterated at pace.
- **Decision maker:** Project lead.
- **Questions to proceed to the next stage:** Does the data-driven technology (DDT) address the issue? Does the DDT represent value for money?
- **Advice can be sought from:** police and crime commissioner (PCC), the force's head of resources, the chief scientific advisor, an intellectual property rights professional, Police Digital Service (PDS), Forensic Capability Network, BlueLight Commercial and the College of Policing.
- **Documents to be completed:** Procurement contracts, business case, purchasing strategy, landscape review.

Project leads can refer to the HM Treasury **Guide to developing the project business case** when setting out the procurement arrangements for a project and key activities.

Project leads can make contact with the **OPCSA**, who will support police forces in their procurement decisions. Project leads can also seek support from the **Police Digital Service** for security and data management advice if the DDT is likely to be national in scope and require central support.

Project leads can consider engaging with other forces to see whether economies of scale can be realised in procurement, and to ensure that interoperability within and between forces is explored.

HM Government has identified the benefits of a **clear purchasing strategy** that identifies what components, resources, support and delivery mechanisms will be needed to embed a successful DDT. This will also help project leads to decide whether to develop, buy or use a combined approach to deliver the DDT and how to achieve the best value for money. The **HM Government**

Technology Code of Practice gives further guidance on these matters.

The **UK Government Security** group carries out threat assessments of current and future possible security risks associated with the installation of visual surveillance systems across the government estate. When project leads are considering such systems and risk-assessing new technology, this will provide a useful reference point.

HM Government has issued **guidelines on the procurement of AI** software, as has the **National Cyber Security Centre**. These can be considered by the project lead as part of the procurement process.

Evaluation prior to deployment

- **Objective:** Review the results of both alpha and beta tests to ensure that the DDT is robust, accurate, effective and ready to proceed to live deployment. Develop supporting policy documentation.
- **Decision maker:** Project lead, data protection officer (DPO), senior information risk owner or officer (SIRO).
- **Questions to proceed to the next stage:** Have the tests met their success criteria? Has the DDT been deemed effective to deploy in an operational context? How will outputs be actioned? How long will the outputs be retained? Does the use of the DDT still meet the ethical standards?
- **Advice can be sought from:** Relevant internal and external panels, committees and groups.
- **Documents to be completed:** Test and evaluation report, updated impact assessments, deployment authorisation checklist, operational practice guidance, performance metrics.

As part of the lifetime management of a DDT, project leads should arrange for the development of a clear evaluation plan at the outset of projects. This will help the gathering of appropriate data – including baseline measurements – throughout the project lifespan, so that the emerging risks, benefits and efficacy can be continually assessed. The plan should also help to clarify any assumptions, intended outcomes and effects.

Project leads should take steps to ensure the quality and independence of the evaluation, for greater transparency and public scrutiny, through established advisory groups.

Evaluation

Evaluation should comprise of three elements.

Technical evaluation

- Focused exclusively on the operation of the data-driven tool itself.
- Typically requires assessing the accuracy of the DDT in carrying out its objective and whether there are any false positives or false negatives resulting from the tool.

Process evaluation

- Focused on identifying the strengths and weaknesses of the processes of the data-driven tool if necessary, making recommendations for adjusting the structure and/or implementation of the project.

Outcome evaluation

- Providing an overall assessment of the outcomes of the project in terms of its benefits, merits and worth.
- May be a longitudinal process taking place over several months or even years.

There should be clear success criteria for the evaluation. If it fails to meet these, the DDT should not be rolled out more widely without further development and retrial.

The College of Policing's **Policing evaluation toolkit** sets out design and implementation strategies that can be used by practitioners to develop evaluations.

Testing prior to deployment

Project leads should ensure that DDTs are tested in a controlled environment before full deployment. Testing should provide clear evidence, as far as is possible in a controlled environment, that the DDT:

- is robust, accurate and effective for its intended purpose
- works better than existing approaches and/or delivers a new policing capability

If either of these criteria are not met, the project lead will need to make decisions or recommendations about whether the project should return to the development stage for redesigning or should not proceed.

The test stage should ideally be separated into:

- alpha testing – ‘lab-based’ tests against historical data, to ensure that the tool is technically functional
- beta testing – operational tests in a real-world environment

Where there is no historical data available for testing – for example, because it is new data being collected – testing on live data should take place in a way that does not have an impact on members of the public.

Once alpha and beta tests have been completed, and when the project lead is confident that further redevelopment is unnecessary at this stage, a comprehensive review of the test results should take place. This is the final checkpoint before live deployment.

Assessment

Project leads should arrange for an assessment of the DDT following deployment. The College of Policing’s **evaluation toolkit** provides guidance on this. The assessment should focus on the effectiveness of the technology and the use of the DDT in its operational policing context. Some DDTs may perform well in a test environment but, for various reasons, fail to produce their intended outcomes when deployed operationally.

The approach to assessment and evaluation needs to be considered at the outset of the project, so that appropriate information is gathered during development and deployment. This would also allow for the development of small tests of change or pilots that could be externally assessed to inform business cases and shape wider-scale implementation.

Complaints procedures

Project leads should ensure that there is an effective process for receiving and responding to complaints about the use of DDTs. This process should be clearly communicated to, and accessible by, members of the public.

Review

To allow ongoing scrutiny, project leads should set up a process to ensure the regular review and assessment of the public benefit, risks, harms and positive or negative effects of the DDT. This

would include:

- a review and reverification following any upgrades to the DDT
- processes for the routine collection, publication and accessibility of data on the equality and human rights impacts of the use of the DDT

Policies

Once the decision has been made to use a new DDT, the project lead should review the impact on any existing force policies and take any necessary action to revise these or to develop any new policies required.

Developing operational practice guidance

When introducing a new DDT, the project lead should develop clear and publicly accessible operational practice guidance, with expert advice where required. The following documentation may be required for any use of the DDT.

Authorisation to deploy

Some DDTs will be deployed continuously following a one-off decision, albeit with ongoing review. Others will be deployed periodically for specific operations – for example, the use of live facial recognition for an event.

In the latter case, operational leads should consider ‘who’, ‘what’, ‘why’, ‘where’, ‘when’ and ‘how’ questions to evidence the requirement to deploy. This will allow review, scrutiny and authorisation from a senior responsible officer (SRO) or equivalent, as governed by standard operating procedures.

Deployment authorisation checklist

When a decision has been made to deploy the new DDT, a senior leader responsible for making the decision to deploy should complete a deployment authorisation that covers the following:

- the detail and approval of the legitimate aim of the DDT deployment
- the legal powers that are being relied on to support the deployment

- a clear, explicit and transparent explanation of how individual rights have been balanced against the benefits of using the DDT
- how and why the deployment is necessary (not just desirable) in accordance with the **Human Rights Act 1998**
- why it is proportionate to achieve the legitimate aim of the deployment
- if applicable, how the processing of personal data is strictly necessary under the **Data Protection Act 2018** for law enforcement purposes, including what the “pressing social needs” are
- why sensitive processing is needed to achieve the legitimate aim
- which of the Schedule 8 grounds are satisfied
- why the purpose cannot be achieved through less intrusive means

Prior to deployment, the decision to deploy, along with details of the DDT, should be formally recorded and made public. Where it is not possible to publicly disclose details of a sensitive project, these details should be securely shared with relevant oversight bodies or regulators, which could include:

- **Investigatory Powers Commissioner's Office**
- **ICO**
- **Biometrics and Surveillance Camera Commissioner**
- **Forensic Science Regulator**

Impact assessments

Prior to the use of any new DDT, project leads should complete an evidence-based assessment of the new technology. This should ensure the fairness and legality of its use and should assess the impact of its use on an individual’s rights and those of society.

These assessments may include a:

- Community impact assessment (CIA)
- Business continuity impact assessment (BCIA)
- Data protection impact assessment (DPIA)
- Equality impact assessment (EIA)
- Human rights impact assessment (HRIA)

Senior leaders should ensure that issues have been adequately identified, documented and mitigated, so that the use of the technology is both necessary and proportionate to the policing purpose.

Project leads should ensure that documents such as the DPIA, CIA and EIA are reviewed on a regular basis when a new DTT is embedded. They should also note whether there are any relevant changes to legislation, operational practices or societal views. A documented risk assessment should be recorded that includes specific operational risks associated with any new technology deployment, including decisions taken.

Ongoing monitoring

- **Objective:** Deployment of the data analytics tool in an operational environment, with clear oversight in place and ongoing review of its performance.
- **Decision maker:** Project lead.
- **Question to continue deployment:** Is the tool yielding results as intended without unintended ethical consequences?
- **Advice can be sought from:** Relevant internal and external panels, committees and groups.
- **Documents to be completed:** Updated impact assessments published, notice of deployment published performance metrics, deployment logs, register of deployments.

Senior leaders should decide who should act as the senior point of accountability in relation to the deployment of a DDT. This may continue to be the project lead responsible for embedding the DDT or someone else in the organisation more directly responsible for the relevant operational area. This individual should have sufficient decision-making power and seniority to take appropriate action following the identification of any serious issues and, if needed, to halt deployment.

Senior leaders should ensure that there is clear oversight of the DDT. This includes:

- regular reviews of how the technology is working in its operational context
- ensuring that it is continuing to operate within the various assessments of risk, safeguarding, necessity and proportionality

Learning from ongoing monitoring, both positive and negative, should be fed into processes of ongoing experimentation, innovation and improvement.

Deployment logs

The senior officer responsible for the deployment of the DDT should ensure that deployment logs are completed in the planning and execution of any new DDT deployment. For example, this includes logs completed by the silver and bronze commanders, and by technology operators.

Register deployments

Project leads should keep a register of all deployments that affect the public, and these should be published.

Register of technologies deployed

Senior leaders should keep a record of all data-driven technology, alongside the Record of Processing Activities (RoPA) set out in **Article 30 of UK GDPR** and **Part 3, section 61 of the DPA**. These should be available to members of the public.

References

- Scottish Government. (2023). **Independent review – Independent advisory group on new and emerging technologies in policing: final report**
- Scottish Government. (2023). **Policing emerging technologies report: Scottish Government response**

Tags

APP