Evolve

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

First published 17 June 2025

10 mins read

Design stage

- **Objective:** To identify the most suitable analytics methods to complete the project, understand different types of approach, determine what data should be used and identify potential constraints.
- **Decision maker:** Project lead, with input from the data protection officer (DPO) and senior information risk owner or officer (SIRO).
- **Question to proceed to the next stage:** Do the benefits outweigh the risks regarding moving to the next stage and is there a clear plan to mitigate any unacceptable risks and potential harms?
- **Advice can be sought from:** Relevant internal and external panels, committees and groups – in particular, the designated DPO, force lawyers, equalities advisors and information security officers (ISOs).
- **Documents to be completed:** Project design report.

This section sets out how to take the identified data-driven technology (DDT) and ensure it is fit for a policing purpose.

At the design stage, project leads should:

- clarify the problem they are seeking to address (identified in the engage phase)
- understand the different types of approaches and solutions available
- determine the training data (ensuring that the data is of a suitable quality and legally acquired), technology and people resources that should, and should not, be used to develop the DDT
- identify constraints and trade-offs

This is about designing the approach and methodology for developing the DDT, rather than the design of the DDT itself, which is part of the next stage.

It is also critical that appropriate levels of challenge are built into the plans for developing the tool. A range of strategies, such as ‘red-teaming’ (adopting a deliberately adversarial approach), should be

considered to develop sufficiently robust review processes.

It is also crucial at this stage to establish the likely quality and quantity of data needed to support a DDT of the type being explored, as well as the steps required to make sure that these are in place, such as data cleaning or creating synthetic data sets.

The National Police Chiefs' Council (NPCC) is developing a catalogue of science and technology cases that summarise a selection of scientific, policy, legal and value-for-money solutions. These can be searched by decision makers to learn about projects and solutions developed elsewhere.

Project leads should undertake a landscape review before engaging with wider industry, by ensuring that research is conducted with partner organisations, such as:

- the Office of Police Chief Scientific Adviser (OPCSA)
- the Police Digital Service (PDS)
- the Forensic Capability Network
- BlueLight Commercial
- the College of Policing
- the Home Office Public Safety Group

Project leads should attend events held between policing, partners and industry to explore the problem areas in relation to their DDT and to collectively propose solutions.

Innovative activities can be commissioned to enable host forces, partner organisations, suppliers, academia and the third sector to rapidly build a blueprint. Having addressed all legal and ethical considerations, this can then be evaluated against viability, desirability, feasibility, impact and sustainability criteria to assess how effectively it solves the policing challenge. Forces can then purchase accredited solutions that meet the blueprint, regardless of supplier.

Technology innovation is a longer-term process. In making decisions about procurement, replacing systems or changes to practice, project leads should focus on establishing understanding and the willingness to experiment in an agile fashion – for example, in small-scale test runs.

Alternative approaches to commercialisation

Organisations that can be approached to commercialise DDT innovations include:

- BlueLight Commercial
- the Defence Science and Technology Laboratory (Dstl)
- the Defence and Security Accelerator (DASA)

Sources of external funding for developing and testing DDTs include:

- the Home Office
- the OPCSA's STAR Fund
- the OPCSA's Test and Learn Fund
- the College of Policing Centre for Police Productivity
- NPCC's AI Board

Formal validation

Prior to deployment of a DDT, the project lead should carry out a formal validation to establish its effectiveness and reliability, and to ensure it is capable of achieving the outcome it was designed to achieve. This should include the completion of risk management exercises and, where the DDT relies on algorithms, an algorithmic transparency report. If the deployment is classed as a national police system, project leads should apply the requirements of the **National police information risk management policy**.

Project leads should develop a set of performance metrics that will be used to assess the benefits of the operation or the ongoing use of the DDT. These should be bespoke to the individual DDT.

As part of internal governance regimes, senior leaders should ensure that their organisation has formal validation systems, processes and procedures in place in respect of each DDT.

Rigorous testing of new AI technologies, which have a direct effect on individuals, is necessary to ensure that platforms do not unintentionally discriminate against groups of people. One way of doing this is to collect demographic depersonalised data on the individuals concerned, then use this data to assess how the model performs.

At the design and testing stage, there is a risk of bias entering the system due to the nature of the police data that the algorithms are trained on. Police data can be potentially unrepresentative. For example, a large proportion of crimes go unreported so police data may not reflect the true nature of criminality.

Appendix A of the Department for Science, Technology and Innovation's **Review into bias in algorithmic decision-making** sets out bias mitigation strategies and links to detailed explanations of how these work.

Project leads should complete a project design report that details the project's key features, structure, criteria for success and major deliverables. As part of formal validation, project leads should complete an evaluation of the DDT prior to deployment. Parameters for evaluation would include:

- cost versus benefit
- usability
- interoperability
- legal and ethical compliance
- security and privacy
- workforce impact

Project managers should complete risk management exercises. If the DDT relies on algorithms, they should also complete an algorithmic transparency report.

The project lead should adopt a user-centred design approach and should refer to the **Government Design Principles**.

Project leads should ensure that technology meets the needs of the user and, where required, enables interoperability within and between police forces. This is to:

- reduce cost, risk and complexity
- conform to published specifications for storage, sharing and security
- allow for compliance with data protection law
- ensure a common understanding of what good looks like

The specifications are outlined in the **Information management APP**.

Algorithmic transparency

The project lead should complete an algorithmic transparency report for every algorithmic tool they use that meets the government scoping criteria. These reports should be uploaded onto the

GOV.UK repository, where they will be accessible to the public and interested stakeholders.

The **Algorithmic Transparency Recording Standard** provides guidance on when a report is required and on the submission of reports.

Third-party suppliers

When using a third-party supplier to develop or implement the DDT, senior leaders can use the following criteria. These criteria will help them to check that there is a clear, documented agreement of responsibilities between the police force and the supplier, and that the supplier has done the following.

- Conducted an assessment as to the legal and risk implications of each capability separately, or collectively where a system is operated in tandem with other technologies.
- Provided information to the police force on the system functionality and infrastructure.
- Made it transparent that the outputs from the data manipulated by the technology are accurate and, as much as possible, free from bias. A force should always re-test the system using its own operational data. It is not sufficient to trust the data provided by the supplier.

Senior leaders should ensure that the design of purchased systems is secure. They should coordinate with suppliers to implement processes that protect the data where the system is networked or linked to other systems.

Senior leaders should ensure that there is a system and process for recording how the technology collects, uses and shares information. This should include a record of date, location, consent verification and provenance of the data.

Third-party suppliers that are commissioned to maintain the technology can work with police forces' IT departments to do the following.

- Implement policies and processes that protect the data from cybersecurity threats.
- Carry out penetration testing in line with the force's IT policies. These policies should be reviewed and evaluated to enable continuous improvement.
- Assess the level of cybersecurity risk associated with the solution and ensure that any risk is managed through the agreed governance process.

Decision to proceed

The decision to proceed should be made by the project lead with input from the DPO, ISO, SIRO and other relevant teams or groups. This should include experts in:

- data analytics
- legal compliance
- equalities
- frontline officers
- other business areas

Alongside the evaluation results, the overall decision to proceed should be informed by the data protection impact assessment (DPIA) and should be based on whether:

- the likely benefits outweigh the potential risks at this stage
- there is a clear plan to mitigate any unacceptable risks and potential harms
- the lawful basis for proceeding with the project has been established and clearly documented

Risks

The likely risks could be as follows:

- the data is not good enough or sufficiently good-quality data cannot be accessed
- there is not sufficient expertise (or clear access to it externally) for product development
- the data cannot be managed in a secure environment that would allow the right work to be done to it
- use of the DDT would not be an ethical, lawful or legitimate use of police powers
- the integrated impact assessment (which would include a DPIA, HRIA, EIA, BCIA and CIA) has identified unacceptable risks that cannot be managed appropriately within the parameters of the project
- the expected benefits of the DDT are not being realised or are not significant enough to justify the resource investment required to continue with the project

If senior leaders do not feel that there is a clear plan to mitigate these risks, the project lead can return to the prioritisation stage to redefine the problem or bring the project to a close.

Workforce implications

- **Objective:** To identify and manage the impact of the new technology on the workforce.

- **Decision maker:** Project lead.
- **Question to proceed to the next stage:** Can we manage the training and development needs of officers and staff? Is there sufficient HR capacity and capability? Have affected staff been engaged in the development process? How are outputs presented to users?
- **Advice can be sought from:** HR professionals.
- **Document to be completed:** Training plan.

Training and development

In the development stage of the DDT, project leads should ensure they engage with officers and staff who will be using the technology, to understand their needs and views in relation to technology.

Senior leaders should ensure that officers, staff and volunteers who will be using or monitoring DDTs receive appropriate training and development, with a particular focus on equality, human rights and data protection obligations.

This should include specific training and development for the human-in-the-loop about the limitations of the technology and how the technology arrives at its recommended course of action. This training should also provide information on how to recognise and address any risk of inaccuracy or bias, or other risks associated with the use of the DDT. The human-in-the-loop should be aware of any potential changes to the intended use of the DDT and should raise this with the senior officer in charge of the operation where this occurs. This includes factors associated with the following:

- project drift: if the use of the technology moves outside the original operationally agreed parameters
- status drift: if the use of the technology moves from being overt to covert
- critical and spontaneous incident response: how to deal with any unforeseen incident
- error management: how to deal with any errors that emerge in the operation of the technology

Intellectual property issues

- **Objective:** To ensure that intellectual property is protected.
- **Decision maker:** Senior leaders, project lead.

- **Questions to proceed to the next stage:** What type of intellectual property applies? Is the intellectual property protected? What is the scope of protection? How long does the protection last? Who owns the intellectual property?
- **Advice can be sought from:** Force legal department.
- **Documents to be completed:** No specific documents need to be completed in relation to intellectual property. However, the ownership, responsibilities and requirements of intellectual property will need to be embedded as part of the contract or agreement terms and conditions, in consultation with the force commercial procurement lead and force legal department.

When developing a new DDT, the project lead should consider ownership of intellectual property rights (IPR). The Government Office for Technology Transfer's **Guide to managing intellectual property and confidentiality** provides guidance to support the project lead.

Tags

APP