Introduction

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

First published 17 June 2025

10 mins read

Introduction

Data-driven technologies (DDTs) focus on the processing of a wide variety of digitised data, including biometric data, to inform policing decisions. Examples of DDTs include artificial intelligence (AI), machine learning and automated decision-making.

As stated by Chief Constable Andy Marsh, CEO of the College of Policing:

“We can make huge gains in productivity by turning to technology so that we can spot crime trends without officers having to trawl through thousands of pieces of data.

Using data-driven insights and innovation will mean officers can make their organisations more efficient and effective so that more time can be spent on front-line policing to keep the public safe.”

The **National Policing Digital Strategy 2020-2030**stems from policing’s ambition to embrace digital capability in support of tangible, positive and measurable outcomes for both law enforcement and the public in achieving the Policing Vision 2030 by having the most “trusted and engaged policing service in the world by working together to make communities safer and stronger”.

The breadth of potential DDTs is huge. The extent to which this APP is followed should be determined by the potential impact that the technology could have on individuals or communities, as well as the associated potential risk. This would be particularly evident in the case of contentious technologies. The APP is not intended to introduce unnecessary bureaucracy or stifle innovation where the estimated impact on individuals or communities is judged to be nil or minimal.

The **National Police Chiefs’ Council (NPCC) science and technology strategy** sets out a ‘science system’ for how the police should understand, commission and use science and technology, including DDTs, in policing. This APP is structured in line with this strategy and provides more detailed guidance about how the science system should be applied by a police force

when using DDTs for overt use. This APP does not offer guidance on the deployment of DDTs in a covert capacity, as this requires consideration of a wider legislative framework.

The strategy sets out the three stages that should be undertaken in the introduction of a DDT:

- **Engage**: Understand the nature of the problem to be solved. Get public support and other relevant support for the need to take action to solve a particular problem. Seek views on what technology solutions might be available, practical, appropriate, legal and ethical in the context of the force's digital maturity.
- **Evolve**: Take the chosen DDT and adapt it to work in policing and to address the problem identified.
- **Embed**: Deploy the DDT in policing and check that it is being used fairly and effectively.

If new information emerges as a result of evaluation findings, or if the internal or external environment in which the DDT is being used changes, it may be necessary to revisit stages of this approach.

Definitions and terms

- Algorithms are clearly specified mathematical processes for computation. An algorithm is a set of rules that, if followed, will give the intended result.
- Artificial intelligence (AI) refers to technologies with the ability to perform intellectual processes that would otherwise require human intelligence, such as visual perception, speech recognition and language translation.
- Biometric data is personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual that allows or confirms the unique identification of that individual, such as facial images, fingerprints or DNA.
- Business continuity impact assessment (BCIA) is a process that helps organisations to understand how an activity could affect the wider operations of the force.
- Data-driven is a way of making decisions based on the analysis and interpretation of data stored from digital sources.
- Digital maturity is an organisation's ability to quickly respond to the developments and shifting trends of technology.
- Human-in-the-loop is the process of combining machine and human intelligence to inform decision making.

- Human rights impact assessment (HRIA) is a process that analyses the impact of an activity on human rights.
- Risk is the potential for significant physical, material or non-material harm. This implies that there is a more than remote chance of some harm occurring. Where there is ‘high risk’, it implies a higher threshold, either because the harm is more likely, or because the potential harm is more severe, or a combination of the two.
- Validation is the process of providing objective evidence that a method, process or device is fit for the specific purpose intended and that the results can be relied on.

Governance of DDT development

- **Objective:** Establish internal governance arrangements separate from operational decisions and engage with external governance and regulatory bodies.
- **Decision maker:** Senior leaders, project lead.
- **Question to address:** Are robust internal governance arrangements in place and documented?
- **Advice can be sought from:** Engagement with ethics committees or other suitable advisory structures and police and crime commissioner (PCC) and NPCC portfolios.
- **Documents to be completed:** Governance schematic, minutes of meetings.

Senior leaders should establish appropriate internal governance arrangements for the procurement, deployment policy and evaluation of DDTs. These should include:

- provisions for the oversight by the chief constable and PCC (or equivalent)
- sufficient independence and accountability to allow for objective decision-making, while striking a balance with operational need
- provisions for engagement with, and oversight from, ethics committees or other suitable advisory structures

The level of risk, complexity and operational effect associated with the individual DDT will determine the level of scrutiny, oversight and engagement required.

Risk management

Project leads should employ effective risk management processes by:

- scoping, mapping, identifying and addressing any risks, particularly risks to rights and freedoms of individuals, opportunities or issues that may become associated with the adoption of a DDT
- continuing to reassess and evaluate risks throughout the lifecycle of the initiative

Project leads should take account of any changes to the proposed use of the DDT and should ensure that they revisit the engage stage if necessary.

Privacy and data governance policy

Project leads should ensure that a privacy and data governance policy is in place, which should include the following as a minimum:

- Details of named individuals who authorise the use of the DDT and their level of authority.
- Clear parameters that define how, when and where the DDT should be used.
- Where appropriate, details of the role or roles performing any human-in-the-loop function, taking action based on information gained from the DDT. The **Data ethics APP** gives more information on this function.
- Where relevant, the basis for the creation of person-of-interest databases and an audit trail that documents the origin of the data.
- In the case of facial recognition technology, any ‘similarity threshold’ (a configurable point at which two images being compared will result in an alert) parameters in respect of the DDT and the rationale for that threshold, including relevant evidence.
- How data protection obligations are managed and by whom – for example, storage, retention, deletion, destruction, subject access requests and cybersecurity measures in place.
- How issues related to the Equality Act 2010 requirements will be identified and reported to the software or technology developer and corrected.
- How privacy vulnerabilities are reported to the software or technology provider and corrected.
- Completed data protection impact assessments (DPIAs), where appropriate.
- Adherence to the **NPCC Data Governance Principles for Datasets** used or created by data integration and analytical tools.

Data analytics working group

Project leads should use a data analytics working group. This may be specific to the DDT under development or may have been established for a force’s wider programme of DDT development.

The **Responsible Technology Adoption Unit** suggests that when developing new or complex DDTs, it may be helpful to establish a specialised internal data analytics working group. The project lead should consider the following factors when establishing a working group.

Function

The working group should be involved throughout the lifecycle of a DDT. It should provide advice and challenge on proposed projects, including reviewing and authorising initial business justification documents and project proposals.

Members

The group should consist of:

- statistical or analytical experts, users of analytics tools and those using the outputs or in-house data
- data protection and legal expertise, including the designated data protection officer (DPO) and senior information risk owner or officer (SIRO) – go to **Information management APP** for details of these roles
- operational input – officers and staff who will use the technology

The group should also be able to draw on appropriate expertise, including:

- equalities law
- system developers
- community input
- governance
- media and communications

The benefits of an independent input into the working group from academia and civil society groups should also be considered.

External expertise

The group should bring in external expertise, when necessary, to ensure it is drawing on the latest academic research and best technical guidance available. For example, it could invite data scientists and academics with expertise in police technology to provide independent peer review of

specific project proposals or business justifications. Formal partnerships could be explored to design and test new methods, along with arrangements that allow for the independent evaluation of DDTs with academic rigour for high-risk activity.

All external experts must have signed a data-sharing agreement and be vetted to the appropriate level. Please refer to the **Vetting APP**.

Transparency

To ensure transparency, a programme lead might be appointed to oversee all force DDT projects. The programme lead should be responsible for maintaining and updating an internal list of DDTs that the force is developing and/or deploying. For particularly high-risk projects, details of the project should be made public where appropriate, including its rationale and business justification based on the evidence base. The intended benefits and any potential risks should also be communicated through force channels, as well as how these benefits will be monitored over time, and how these risks have been mitigated.

Communications

The working group should support the project lead in issuing proactive communications regarding new technologies, their use, results and next steps. Where the insights generated by the DDT are of wider value beyond operational use – for example, research and analysis purposes – the project lead should seek to share these insights across the force and with the wider policing community, typically through:

- relevant NPCC channels
- the College of Policing's **practice bank**
- public communications

National landscape

It is important that project leads ensure that the proposed DDT is consistent with the national landscape, ensuring that there is compatibility with developments elsewhere and there is no duplication. Project leads should engage with the **NPCC's Science and Innovation Committee** at the project management stage. There should also be engagement with the Home Office Police and Public Protection Technology (PPPT) function to ensure that the proposal is consistent with Home

Office projects.

Senior leaders should seek to engage with the appropriate NPCC board or portfolio relating to the specific product being developed. They should also share practice so that decisions can be made around investing at scale, including through:

- the **NPCC's Digital, Data and Technology Coordination Committee** (DDaTCC)
- the **NPCC's Science and Innovation Committee**
- national partners

The NPCC also requires senior leaders with responsibility for analytics in a force to attend meetings of the **Advanced Data Analytics Network** (ADA Network), which sets standards and shares practices around the development of these capabilities.

The **Police Digital Service** oversees a number of centrally delivered DDTs. Senior leaders, collaborations and NPCC portfolios can bid for the resources to develop models for specific use cases. The Police Digital Service (PDS) will ensure that standards are maintained and that practice is shared across policing.

The PDS have established a **national standards platform** on the Knowledge Hub in support of the **national policing cyber security strategy** and the **national policing community security policy**. The platform provides access to standards resources, including policies, guidelines, blueprint designs and templates for policing, partner agencies and industry to refer to and put into practice.

Other regulatory bodies

Senior leaders and project leads should also engage with, and be cognisant of Codes of Practice and guidance issued by, the following regulatory bodies:

- **Biometrics and Surveillance Camera Commissioner** (BSCC)
- **Information Commissioner's Office** (ICO)
- **Equality and Human Rights Commission** (EHRC)
- **Forensic Science Regulator** (FSR)

Tags

APP