Chief Constables' Council
(9-10 July 2025)

*S31(1)**

Session 7 – Joint DDaT and Science and Innovation Committees

NPCC
National Police Chiefs' Council

Back to Agenda

Science and Innovation
Digital, Data and Technology

Chief Constables' Council
July 2025

Chief Constable Jeremy Vaughan KPM NPCC Science and Innovation Lead

Chief Constable Rob Carden NPCC Digital, Data and Technology Lead

Ch ie fs ' P rio rit ie s in 20 22

Auto-redact. multimedia	77%	Network+ for prevention	45%	Authenticating images	45%
Auto-redaction text	73%	Integrity screening	45%	Assessing portless devices	45%
Rapid Video Response	68%	Stopping electric vehicles	45%	National science college	41%
Face recognition in PND	64%	Remote knife detection	45%	Finding concealments	27%
Innovation fund	50%	Video MH assessment	45%	Next generation PPE	23%

Chief Constables' Council July 2025

Growth of a S&T System

1. Have a system that engages suppliers, evolves innovation, reduces fragmentation, and ensures effective S&T reaches the frontline
2. Empower leaders to make informed decisions about problems, solutions and future risks.
3. Addresses the limited funding and poor funding profile (70:20:10)

Innovation and delivery of new national policing digital capabilities

NPCC National Police Chiefs' Council

PA

Strategic direction:

- Policing Vision 2030
- Government Mission – Safer Streets
- NPCC Science and Technology Strategy
- NPCC National Policing Digital Strategy 2025

Innovation & Delivery Model

Continuous improvement

Science and Innovation Coordination Committee (SICC)

Innovation

Engage

'Collaboration for ideas / solutions generation'

'Innovation pipeline management' progressing potential solutions

- Regional Innovation
- NSIB down-selecting
- SICC prioritisation

Digital, Data and Technology Coordination Committee (DDaTCC)

Embed

Tripartite Commissioning Process (APCC - NPCC - HO)

National Prioritisation Model → **Business Case Development** → **Commissioning** – approval of business cases and allocation of funding → **Delivery** – Police and Public Protection Technology / Police Digital Service leading on design, procure, develop, scale and implement → **Live use** – deploy the capability and realise benefits

Business case updates

Informing Principles & Standards
- NDAB National Data & Analytics Office
- PIAB Secure by Design
- NTB Future State Architecture

Business as usual: Expansion and development of existing programmes / capabilities

- Home Office Commissioning Board
- Enterprise Solution Design Authority (ESDA)
- PAG – Police Assurance Group
- Individual programme boards and Police and Public Protection Technology portfolio management
- Charges Oversight Board (MTA re-charge & value for money)
- Police Live Services Board / Digital, Data and Technology Coordination Committee

Evolve

From baseline to Blueprint – local solutions evaluated, iterated and prepared for national prioritisation decision

LOCAL POLICE

Local development and delivery route for non-national capability solution

Strategic Outcomes:

Supporting the Policing Vision 2030 of having the most trusted and engaged policing service in the world by working together to make communities safer and stronger.

Outcomes and Benefits

- Better end-to-end visibility of process/activity
- Standardised processes/ better end-to-end control
- Clear responsibilities and governance
- Better spend/value for money
- Quicker deployment of solutions
- More effective solutions
- Enabling and scaling innovation

Features:

- An **accessible** approach that supports forces in developing new solutions
- A **transparent** approach with consistent criteria for decision making
- A **coherent** approach with clear ownership and responsibilities
- An **efficient** approach with standardised processes to accelerate / simplify
- A **responsible** approach that makes best use of public money

*Ideas/projects can end or be redirected at any stage.

NPCC
National Police Chiefs' Council

Our Mission: To engage widely, evolve strategically, and embed the best S&T in a way that is trusted by the public

ENGAGE

We will grow a **vibrant and connected** community, engaging all sectors and collaborate by default.

We will be **clear about our needs** and how to work with us, seeking new ideas, innovations, and forms of delivery.

EVOLVE

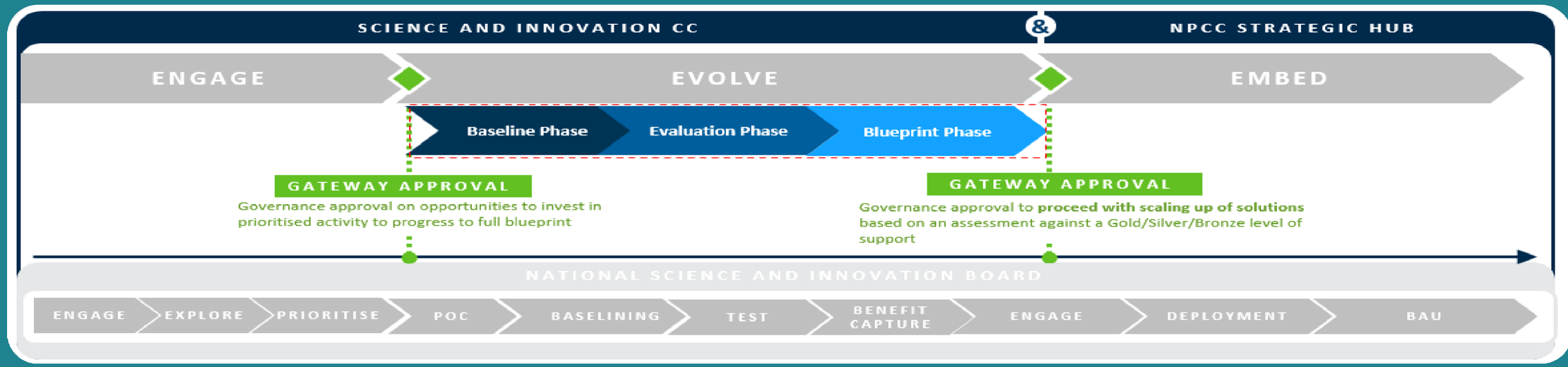
We will **prioritise and conduct high quality S&T** that deliver what policing needs now and in the future.

We will enhance and diversify **scientific expertise** across policing to underpin growth and improve resilience.

EMBED

We will establish mechanisms to ensure **great ideas can rapidly scale and embed** into policing practice.

We will **evaluate S&T's impact** on policing outcomes, building an evidence base for future investment decisions.



NPCC
National Police Chiefs' Council

What is in it for the Chiefs?

System Integration
- Problem Book and Innovation repository
- RIL Network – Funding – OPSCA Guidance

Operational Effectiveness
- Accelerate uptake of AI
- Promote agile innovation - pilots that are scalable
- Health and Wellbeing

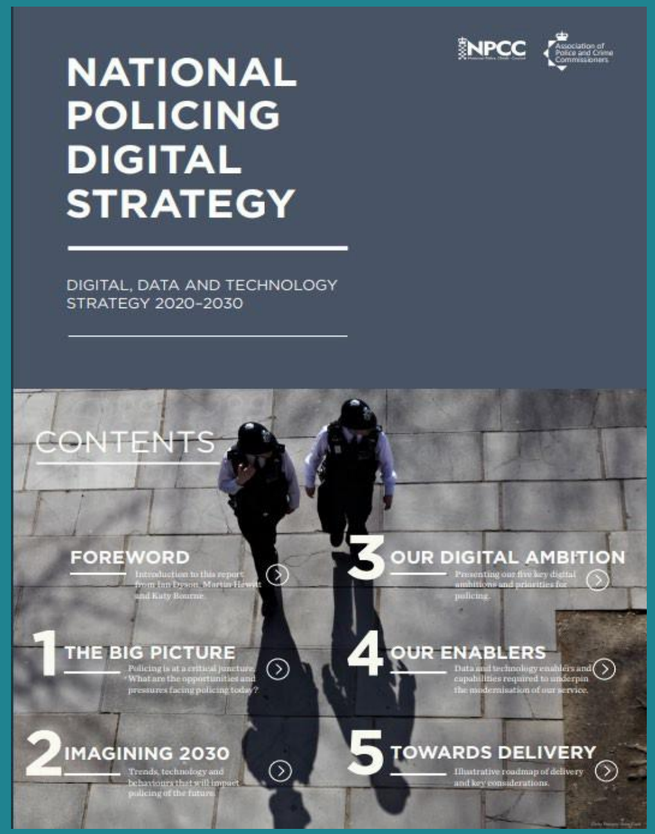
Partnerships and Collaboration
- Strengthen links with academia – P-ACE's
- Development of mechanism to better engage industry

Evidence-Based
- Development of Evaluation Strategy

NPCC
National Police Chiefs' Council

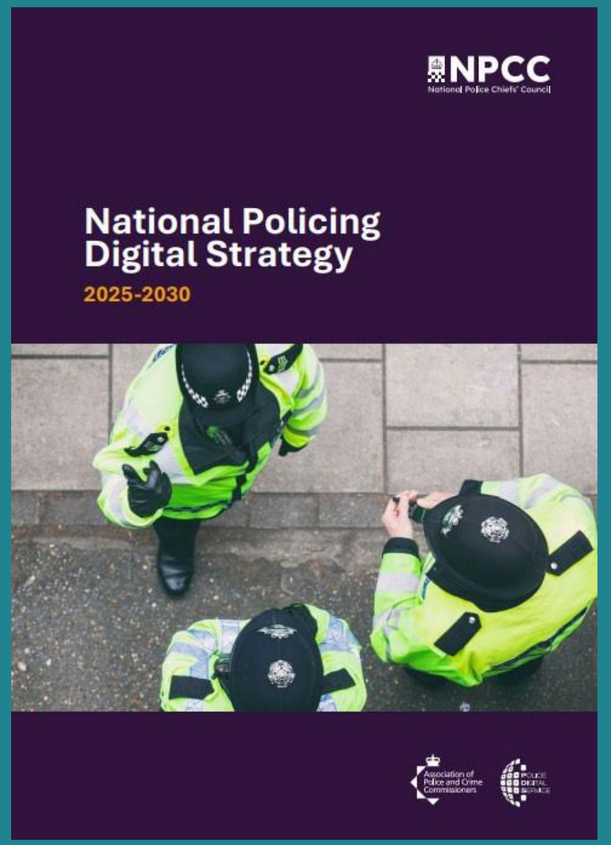
National Policing Digital Strategy 2020-2030

- 2020 pre-pandemic perspective, prior to rapid evolution of technology and criminality
- Fragmented force IT model, with national systems overlay now costing £2Bn p.a.
- Legacy technology, security risks and limited funding blocking new capabilities
- Lack of confidence in national programme delivery and escalating costs to build and run
- Right ambition, but limited impact in delivering progress



National Policing Digital Strategy 2025 - 2030

- Refreshed 2025-30 vision, a “North Star” for all things digital, local and national.
- Endorses NCoP delivering our digital services under policing management and control
- Implemented by Cyber / Technology / Data plans, transforming Vfm and embracing innovation
- Emphasises importance of our people, data, system interoperability and tackling legacy.
- Puts public safety at the core of DDaT prioritisation and delivery



NPCC
National Police Chiefs' Council

Where is our money (£913m 25/26) going?...

- Financial Year 25/26 MLE funding allocation **£860m / 94%,** (but **£594m/ 65%** ESN / Airwave)
- HO PPPT **£288.8M / 32%** - LEDS £109m / HOB £45m / NSAP £24m / PND £35m / Other £56m

So, what's left for innovation and supporting forces...

- National Police Capabilities **£53m / 5.8%** (PDS / DPC / NPAS / Drones / CSA / RPA / Etc)
- Unfunded bids NIM Review / ANPR Infrastructure / PDS / Cyber Strategy
- June Portfolio Assurance Group – MAPPS / LECP costs increasing (£18.5m / £8m)

And no ESN/Airwave underspend this FY, (£129m used 24/25); escalating 25/26 MTA costs to forces, up to £201m from £171m, (One-off £20m HO subsidy)

NPCC
National Police Chiefs' Council

What are we doing...

- Portfolio Assurance Group (Business Cases – HOB / MAPPS)
- National Live Services Board – NSIRO issues (DVI) / system costs / development
- PDS Board – Data and Analytics
- Police Efficiencies and Collaboration Programme – Technology Strategy, Enterprise Architecture design, Data Reform
- Tri-Partite Commissioning – Improve prioritisation of pipeline, financial controls, portfolio management

NPCC
National Police Chiefs' Council

National Prioritisation Model

Many tripartite governance entities address national DDAT capabilities and funding

Commissioning Board
Portfolio Assurance Group
Charges & Oversight Board
Live Services Board

DDAT requirements can come from anywhere in the policing landscape

1 *Proactive engagement with all stakeholders*

2 *Summarised as four main categories of demand*

- New Requirements
- Innovation
- Programme or Project
- Live Service / Capability

3 **Business Partners**

4 **Form and Dashboard**

5 **Lifecycle**

6 NPCC Internal Governance

Collectively agreed policing DDAT priorities submitted

7 HO Commissioning

HO will need to facilitate access to tools & information

Innovation and delivery of new national policing digital capabilities

NPCC National Police Chiefs' Council

PA

Strategic direction:

- Policing Vision 2030
- Government Mission – Safer Streets
- NPCC Science and Technology Strategy
- NPCC National Policing Digital Strategy 2025

Innovation & Delivery Model

Continuous improvement

Science and Innovation Coordination Committee (SICC)

Innovation

Engage

'Collaboration for ideas / solutions generation'

'Innovation pipeline management' progressing potential solutions

- Regional Innovation
- NSIB down-selecting
- SICC prioritisation

Digital, Data and Technology Coordination Committee (DDaTCC)

Embed

Tripartite Commissioning Process (APCC - NPCC - HO)

National Prioritisation Model → **Business Case Development** → **Commissioning** – approval of business cases and allocation of funding → **Delivery** – Police and Public Protection Technology / Police Digital Service leading on design, procure, develop, scale and implement → **Live use** – deploy the capability and realise benefits

Business case updates

Informing Principles & Standards
- NDAB National Data & Analytics Office
- PIAB Secure by Design
- NTB Future State Architecture

Business as usual: Expansion and development of existing programmes / capabilities

- Home Office Commissioning Board
- Enterprise Solution Design Authority (ESDA)
- PAG – Police Assurance Group
- Individual programme boards and Police and Public Protection Technology portfolio management
- Charges Oversight Board (MTA re-charge & value for money)
- Police Live Services Board / Digital, Data and Technology Coordination Committee

Evolve

From baseline to Blueprint – local solutions evaluated, iterated and prepared for national prioritisation decision

LOCAL POLICE

Local development and delivery route for non-national capability solution

Strategic Outcomes:

Supporting the Policing Vision 2030 of having the most trusted and engaged policing service in the world by working together to make communities safer and stronger.

Outcomes and Benefits

- Better end-to-end visibility of process/activity
- Standardised processes/ better end-to-end control
- Clear responsibilities and governance
- Better spend/value for money
- Quicker deployment of solutions
- More effective solutions
- Enabling and scaling innovation

Features:

- An **accessible** approach that supports forces in developing new solutions
- A **transparent** approach with consistent criteria for decision making
- A **coherent** approach with clear ownership and responsibilities
- An **efficient** approach with standardised processes to accelerate / simplify
- A **responsible** approach that makes best use of public money

*Ideas/projects can end or be redirected at any stage.

NPCC
National Police Chiefs' Council

Next Steps...

- Use DLRS principles of 'control and then manage' DDaT for policing
- Partner with S+ICC & OPCSA to build innovation model and use prioritisation to widen the pipeline
- Work with PDS & HO to drive 'convergence', reduce costs and achieve VfM in advance of NCOP
- Continue to 'fix' the delivery issues, free up money
- Deliver the NPDS 2025-2030

National Law Enforcement Data Programme

Digital, Data & Technology

Where we have come from…

LEDS Reset

LEDS entered a Programme reset following a letter from Police Chiefs articulating significant concerns and minimal confidence in the delivery of the replacement of the PNC.

Autumn 2020

Red Team Review

Following the Red Team review, the programme exited reset with a number key recommendations from the review team:

- Focus on product-centric delivery
- Increase involvement of Law Enforcement users within the delivery
- Streamline and mature governance processes

LEDS First Delivery

Implementing these recommendations with a focus on improving delivery, LEDS delivered the first iterations of LEDS Drivers, Property and Audit in March in 2022.

March 2022

Digital, Data & Technology

Where we have come from…

From setback to success…

Illustrating the programme's journey – from 2021 programme reset, to its current reputation for delivery and achievement.

Past

- Programme reset due to "Red Rating"
- Lack of shared understanding of outcomes between Home Office and police
- New strategic product-centric approach required

Present

Award winning programme…

Home Office
Technology Innovation Award - Winner

NTA
National Technology Awards 2025 – 2x Winner

Government Project Delivery AWARDS

From setback to success…

What we have achieved to date

LEDS BY NUMBERS:

1.4m

Transactions on LEDS per month

36%

Of LEDS users onboarded

8%

Of Policing transactions through LEDS

134,000

Entitlement users within forces

KEY MILESTONES & ACCOMPLISHMENTS:

BS10008 Certification

All enquiry services have been built, developed and deployed

LEDS Property is Master of Data

Person Pioneers roll-out complete and now working with Early Adopters

LEDS Drivers decoupled from PNC

293 Change Releases successfully implemented (Property & Drivers)

NDI SRG for Drivers Early Live Support Complete

Data Compliance Logging Service and Broadcasting MVP go-live

Evidential Output MVP go-live

What will LEDS deliver by March 2026?

Delivery

- ✓ All Enquiry functionality will be delivered
- ✓ All non-EI Product Delivery will be delivered (Vehicles, Person, Audit, NSS, Common Services, SRG Gateways)
- ✓ All Repeatable EI interfaces and extracts delivered by LEDS

- ✓ All SRGs will be delivered
- ✓ LEDS Development for Target State FES (Final Endpoint Switchover) Interfaces (PFI, NDNA, IDENT1, ViSOR, NFLMS & Bichard7) complete, Integration testing started.

Adoption

- ✓ All SRGs and External Interfaces adopted
- ✓ All Non-Policing Organisations Adoption complete for LEDS
- ✓ All Forces will be consuming LEDS
- ✓ LEDS is the system of use for the majority of users

Compliance

- ✓ Programme DPIAs completed
- ✓ BS10008 Full Certification, SIP3 & LEDS Disaster Recovery Solution

EPT Transition

- ✓ Transition to EPT complete for Property, Drivers, Vehicles and Common Services
- ✓ Transition to EPT in progress for Person, Audit, NSS

WHAT DOES THIS MEAN…?

- ➢ To the **USER**, LEDS is the main system they interact with. And PNC access has been removed.
- ➢ Users can **SEARCH, VIEW AND UPDATE** data across all data sets.
- ➢ Users can **MANAGE ALL DATA IN VEHICLES, DRIVERS AND PROPERTY** and all high-volume transaction data in Person.
- ➢ All batch file sharing, data extracts and interfaces (with the exception of

Digital, Data & Technology

FES) will be fed by LEDS.

What will be remaining after March 2026?

FES Interface Security testing, Partner Integration Testing, OAT/UAT and Cutover

Progress to LEDS 2

WHAT DOES THIS MEAN…?

- The vast **MAJORITY** of users will be able to **COMPLETE ALL THEIR ACTIONS** on LEDS.
- A small subset of users with very bespoke activities, will need to continue to input data on to PNC to keep LEDS and PNC consistent.

Key Recommendations from commission on multi-modal systems

Buying the right thing

Market Immaturity and Information Asymmetry

Recognise that there is a lack of information available to inform procurement choices and almost all of it is in the possession of vendors, who are commercially motivated. Seek advice from the NPCC AI portfolio to level the playing field.

AI is only part of the solution

It is rarely as simple as "plugging" an AI into your data. Often significant investment will be required to clean up and/or re-platform existing data, if operational benefits are to be realised. AI solutions will have significant dependencies on storage, compute and talent.

You shouldn't try to re-invent the wheel

Find out which other forces have attempted the thing you're trying to do. Learn lessons from their experience even if the solution they chose isn't suitable given your force's specific circumstances. The NPCC AI Portfolio can help you identify who is doing what with AI.

Achieving a return on investment

Understand what you are trying to achieve and target the highest value use cases first before making procurement decisions. Have a plan for measuring the benefits of the solution.

Understanding the Costs

Consider the Total Cost of Ownership (TCO)

Avoid nasty surprises by asking the right questions up front. How will license fees increase beyond year 1? How are upgrades paid for? Will more infrastructure be required as data volumes increase? Do you need to employ AI experts?

Solution / Organisation maturity is a factor

It takes time for an AI solution to learn to get good at its job and for an organisation to use it in an optimal manner. Factor this into benefits realisation plans.

Negotiating a good deal / avoiding a bad deal

AI models need to learn, and your data has value. Who's paying?

AI solutions require learning-by-doing. This is of high commercial value to suppliers; factor this into commercials. Performance should naturally improve over time as the state-of-the-art evolves.

Be aware of the costs of getting "locked in"

Technical integration of systems makes leaving harder. Lock-in and dependency are a strategic goal for suppliers. Negotiate for flexible contracts and be aware of the costs of terminating them.

Commercial risk should be shared by the buyer and the supplier

In an immature market with low maturity solutions, unexpected setbacks are inevitable. Negotiate so that the costs of "unknown unknowns" are shared between your force and the supplier.

Understanding Risk

Could you explain how your AI works? (Ethical Risks)

Checking that an AI solution makes the same decision as a human does not go far enough. You must understand the method by which an AI solution derives its answers to ensure that systemic biases in data are not being perpetuated or amplified.

Do you know where your data is? (Technical Risks)

In order to make informed decisions around information security you need your supplier to clearly indicate where your data is stored and processed. What becomes of data used for training, augmentation or prompts; does the use of AI present a risk of leakage?

Does your AI play by the rules? (Regulatory Risks)

Ensure that your force is equipped with the information to make proportionate decisions regarding the application of existing regulation (e.g. GDPR) and that you understand how you'd satisfy (e.g.) a requirement for traceability from an inquest.

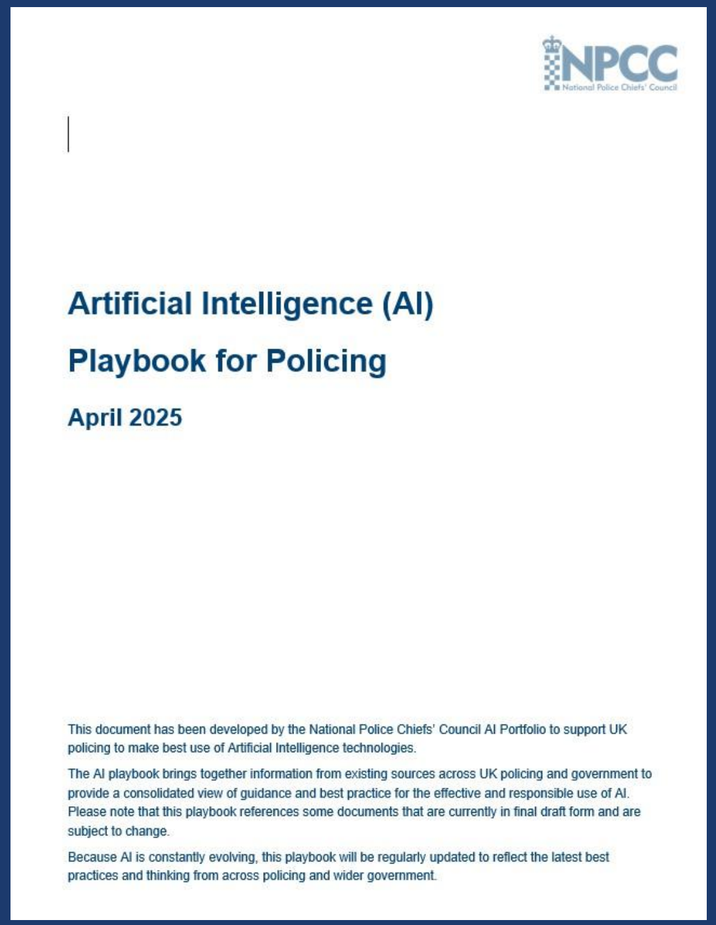
To ensure responsible adoption of AI, forces should abide by the **Covenant for Using AI in Policing** and the **Responsible AI Checklist for Policing**

National Police Chiefs' Council

What has the system delivered over the last twelve months?

1. NPCC AI strategy – launched in September 2024
2. NPCC AI playbook
3. Joint RAI Checklist with PROBabLE Futures
4. Worked with the College to ensure symmetry with recent APPs and guidance
5. Joint Operating Procedures developed with CPS on the use of AI technologies that influence the CJS
6. Developed an early adopters community to drive adoption, identify blockages and develop workstreams to overcome these
7. Engaged with Europol and other International partners to reduce duplicated effort
8. Intensive engagement with officials to maximise use of cross-government investment

The NPCC AI Playbook



Artificial Intelligence (AI)

Playbook for Policing

April 2025

This document has been developed by the National Police Chiefs' Council AI Portfolio to support UK policing to make best use of Artificial Intelligence technologies.

The AI playbook brings together information from existing sources across UK policing and government to provide a consolidated view of guidance and best practice for the effective and responsible use of AI. Please note that this playbook references some documents that are currently in final draft form and are subject to change.

Because AI is constantly evolving, this playbook will be regularly updated to reflect the latest best practices and thinking from across policing and wider government.

- Designed to work with the recent APPs on data-driven technologies and Data Ethics
- Is designed to be interactive, outlining relevant sections for specific users with the following sections:
- Chapter 1: Overview, setting out why AI is relevant to policing.
- Chapter 2: How to set an effective AI strategy for your force.
- Chapter 3: How to design good AI governance (including RAI)
- Chapter 4: Considerations on AI security.
- Chapter 5: What to think about in the AI delivery lifecycle.
- Chapter 6: What skills do you need for your force to be successful.

NPCC
National Police Chiefs' Council

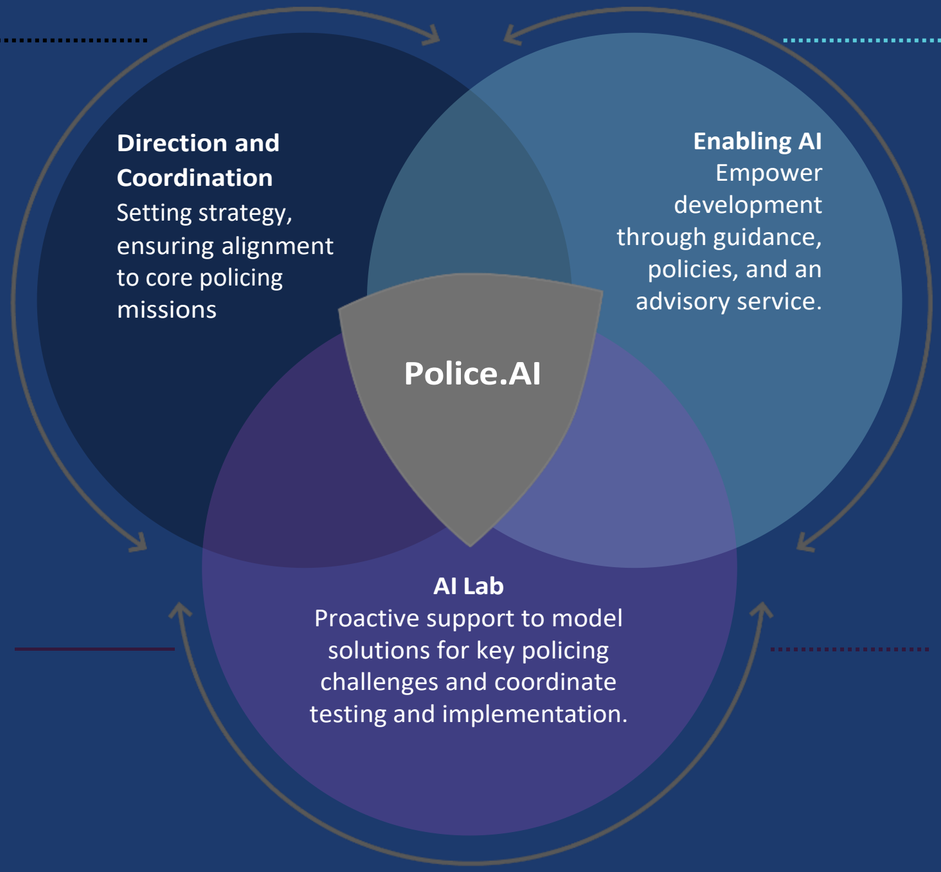
Things to expect in the coming months

1. Blueprinted Copilot Chat (17th of July)
2. Guidance on procurement of Copilot
3. National Copilot trial (September)
4. Targeted support through a taskforce approach to support forces to overcome barriers identified by early adopters (including business case, technical evaluation, impact evaluation and data protection processing support)
5. Focused activity on RAI, using the checklist effectively
6. Sustained activity to identify AI threats more accurately and to rollout deepfake detection capability
7. Enhancing our collective situational awareness on who is doing what, and is it effective to inform local decision-making
8. External facing algorithm repository in line with ATRS
9. Clarity on funding for support for forces to enable scaling of AI solutions

NPCC
National Police Chiefs' Council

What is Police.AI?

- Responsible for setting national direction aligned to key strategic drivers, working in line with the existing three pillars of productivity, effectiveness and threat.
- Accountable for ensuring that AI R&D is focused on policing's core missions.
- Providing a coordinating role in policing's response to the rapidly evolving technologies, collaborating with partners to coordinate national funding and investment.



- Reduce the lag from innovation to scaling through expert scanning, evaluation and support to effectively implement AI technologies.
- Support robust evaluation of AI technologies to understand business benefits, enabling economies of scale.
- Drive Responsible AI adoption and transparency leading to improved public trust
- Coordinate AI central spend and be a vehicle to provide assistance (economic or expertise) to enable effective adoption of AI technologies

- A collaborative approach with academic, commercial and wider system partners to deliver cross-system benefits
- Delivering bleeding edge R&D ensuring that UK policing is at the forefront of AI development. Delivering R&D that will support the rapid evidence-based implementation of solutions in to policing.

- Through a federated model, support local policing to deliver genuine impact with AI technologies.
- Be responsible for the technical evaluation and future proofing of AI technologies, ensuring they deliver genuine business impact that is long-lasting, maximising ROI
- Responsible for the coordination of testing and delivery of AI solutions targeted at policing's key missions

NPCC
National Police Chiefs' Council

Data Reform: National Data Integration & Exploitation Capability

Chief Constable Chris Todd

Agenda

1 Strategic Context

2 CDMH Progress Update

3 Purpose of the Preliminary Market Engagement

4 Stakeholder Engagement Summary

5 Next Steps

6 The Ask

Strategic Context

NDAO /Forces	Operational Data Exploitation and Integration (Nectar, ILAS, Prometheus)
PND / LEDS	Data for Intel and Operational Purposes
PDS NPCE	Operational Application Dev. Environment
CDMH	Data for Strategic & Policy Analytics & Perf. Reporting
Other	TOEX, Police.AI etc

A multiplicity of Data Integration and Exploitation Initiatives being progressed in parallel across Policing, using different tooling, serving different needs, but often using the same base data.

HMG & Policing Interest in Foundry Product

Significant risk of:
- **Duplication**
- **Dilution** of effort
- **Architectural incoherence**
- Excessive **costs**

What are the best options to meet the **data integration and exploitation** needs for **all Policing purposes**?

Significant stakeholder concerns about single solution:
- **Unclear** business needs/reqts
- Potential for use of **existing** capabilities and tooling
- **Vendor lock-in** and **cost** risks
- **Deliverability**

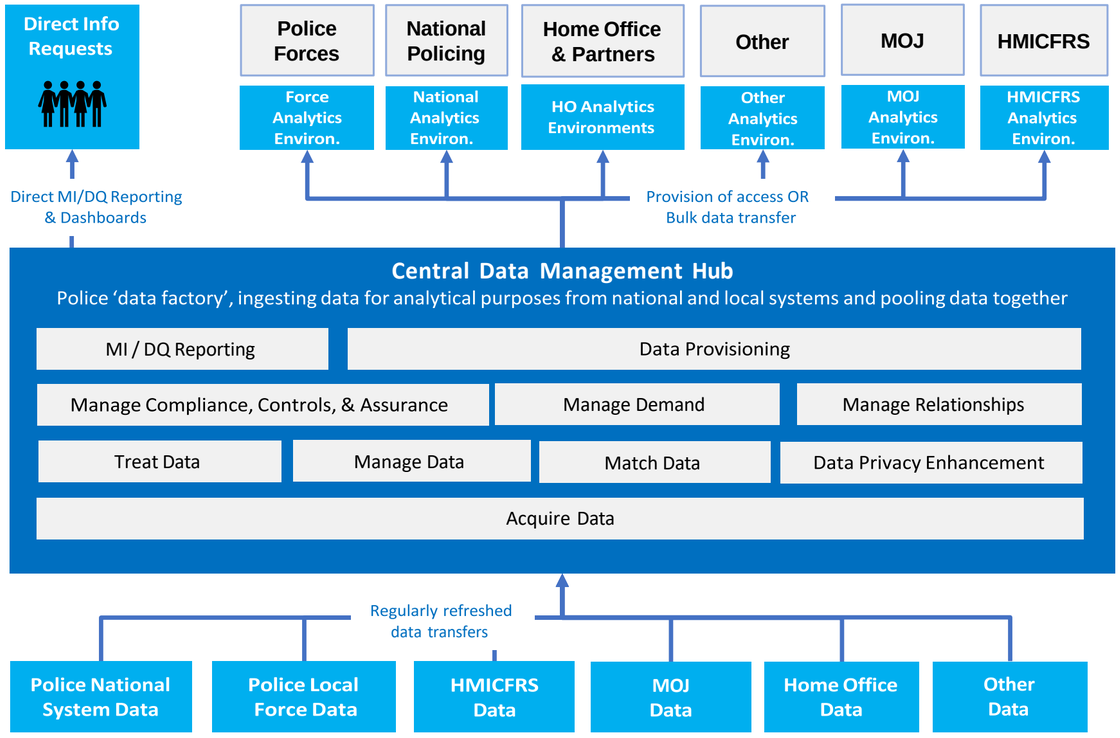
Tiger Team established May 25 to rapidly:

- Capture business needs across Policing.
- Conduct preliminary market engagement to inform solution thinking.
- Review potential of existing capabilities
- Mobilise a working group who will define a recommended future state and pathway by Nov 2025.

CDMH Progress Update

An overview of CDMH was shared with NPCC Coordination Committee Chairs in Dec 24.

Since October 2024, the Data Reform workstream (part of PECP) has been conducting discovery activities on a potential national Policing data hub to acquire, process, and provision Police data **for analytical and reporting** purposes.



CDMH Activities

- Planned Data Reform Workstream Board will include Aimee Smith (co-chair of NPCC National Police Data & Analytics Board) along with wider Policing and PCC representatives.
- Proposed solution and service offering under development - to be ultimately reviewed by NPCC Data Board and Commissioning Board (via PECP)
- CDMH high level requirements have been captured and Force analysis and reporting activities documented
- Ongoing discovery work with six Forces to understand implications of acquiring data from Force data warehouses
- SOBC business case in final stages of development

Current CDMH Status

Further work on CDMH has been temporarily slowed until implications of a market engagement exercise to consider a single National Data Integration & Exploitation Capability become clear (as this would significantly alter current scope of CDMH to include operational and intelligence data integration needs). We're aware that local forces are integrating data for operational purposes and are currently pausing to explore better alignment.

Purpose of the Preliminary Market Engagement

The preliminary market engagement is an information-gathering Request for Information exercise aimed at better understanding the range of capabilities, delivery models, and innovations available from industry to address current problems and unlock the full potential of our data by using it in new, transformative ways. Information provided will help shape our thinking on the requirement. The PME is not a tender and will not result in any commitment to suppliers or solutions from this process.

1

What problem are we trying to solve?

What are the issues with Policing's data landscape and national systems?

2

What are the Policing requirements for a National Data Integration and Exploitation Capability?

What would a solution need to look like to solve the problem?

3

How could the market help?

What could this solution look like? What is currently feasible?

Stakeholder Engagement Summary

Stakeholders: Crime, SOC, CT, Intel, PND, DDaT CC, NPTC, HO PPPT

Consolidated Feedback…

1. Recognition of the Gap

- Unanimous agreement that a gap exists. Gaps include:
  - Lack of a coherent national strategy
  - Siloed systems and inconsistent data standards
  - Underutilised local capabilities

2. Vision for the Future

- Layered, modular architecture
- Federated control with local empowerment
- Central capability with tailored services
- Ethical, transparent AI and tooling
- Data-driven decision-making to support prevention

3. Top Priorities

- Clear problem definition and use cases
- Avoiding vendor lock-in
- Data governance and ownership clarity
- Investment in internal capability and staff

4. Concerns About PME

- Timing and readiness: PME is premature without a clear requirement
- Market influence: Risk of being sold solutions that don't fit
- Reputational risk: If the ask is vague, it could undermine credibility
- PME should reflect a shared vision, not fragmented needs.

Illustrative (paraphrased) quotes…

"Larger forces have the local requirements covered. Not the same for smaller forces"

"Must not leave PND under-invested in again"

"One solution cannot solve all the requirements"

"Need to start incremental delivery now"

"Must build trust between officials and chiefs; align on vision and delivery"

- **Revised PME Doc**
- **Shape future Programme**

Next Steps

Completed activity

Future activity

MAY 25

Cross HO/Policing Tiger Team convened to deliver Preliminary Market Engagement (PME) for a National Data Integration and Exploitation capability.

JUNE 25

Preliminary Market Engagement (PME) published (12/06).

Engagement with existing internal capabilities (e.g. Solar Blue/SUNUP/NPCE).

JULY 25

Deadline for supplier responses (10/07).

Review supplier responses.

AUG 25

Preliminary Market Engagement outcome report and findings document completed.

Tiger Team stands down. Further activity handed to BAU Data Reform team.

Decision to progress with CDMH, pivot to National Data Integration and Exploitation Capability or progress both.

NOV 25

Preliminary Market Engagement exercise completed.

Future state defined by project team.

Recommendation on implementation options to Commissioning Board.

DEC 25

Detailed update on Preliminary Market Engagement exercise and recommended way forward presented at Chiefs' Council meeting.

The Ask

1. Are Chiefs' Council members happy for the following stakeholders to represent the voice of Chiefs' Council for the duration of the preliminary market engagement and related work?
    - **CC Rob Carden (DDaT CC)**
    - **CC Louisa Rolfe (Crime CC)**
    - **CC Chris Todd (SRO)**
2. We recommend that the team provide a more detailed update to Chiefs' Council on progress of the PME and outcomes of the process. Are members happy for this update to be included in the December Chiefs' Council meeting agenda?
3. We recommend that a Chiefs' Reference Group is set up to advise on this work going forward. Do members support this approach?

What is the Problem we are trying to solve

Environmental Factors

Political

- Increased scrutiny of policing from civil society, NGO's, special interest groups, and courts
- Pressure for rapid change, quick results
- Changing political priorities

Social

- Rising level of technological proficiency of criminal networks
- Rising awareness of privacy concerns amongst civil society
- High profile data breaches resulting in negative publicity and loss of public confidence

Economic

- Increasing pressure on departmental budgets with need to focus on economies of scale and value for money.

Technical

- Trends in crime have shifted, sources of relevant data have evolved, and volume of data has increased, requiring ways of working and legacy system infrastructure to rapidly evolve in order to keep up.

Strategic Factors

Governance

- Fragmented control and direction of national analytics exploitation strategy and investment
- Competing priorities between disparate Police and Home Office teams and directorates

Data Standards

- The quality of the data across policing and the CJS is insufficient, due to data entry at source, and a lack of consistent standards and definitions
- Significant variation in maturity of data capability across Forces

Legacy Initiatives

- Proliferation of data improvement and exploitation projects across Govt.
- Seed funding does not fully consider through-life cost of ownership
- Budget focus (systems and datasets) is often domain-specific

Data Strategy

- Absence of a coordinated strategy and national approach to innovation leading to fragmented approach from local Forces which is difficult to scale, commercially inefficient, increases complexity and technical debt

Value Stream Factors

Opportunity Ident. / Use Cases

- Limited view of the value of Policing data (including justification for investment)
- The large number of datasets in Policing make it hard to know where to go to get business questions answered.
- Siloed system infrastructure inhibits an end-to-end view of an offender or victim journey and limits broader insights.

Data Integration & Processing

- Existing systems and datasets are not nationally exploitable,
- Low maturity of privacy enhancing approaches restricts access to granular data
- There is an absence of well-integrated, accessible and conformed data to support analytical exploitation
- Analysts having to undertake ad-hoc data processing
- Multiple requests to Forces for data resulting in admin burden

Data Exploitation (Analytics)

- HMG lacks a consistent, data-driven approach toward measuring efficacy of policies applied at a national level.
- Significant variation in maturity of analytics capability across Forces
- Limited ability to offer transparency / explainability of algorithmic processing
- 100s of overlapping tools, disparate capabilities and available tools not being fully used (with over-reliance on spreadsheets)

Application of Insight

- Thresholds and remit across local, regional &national are unclear owing to the evolving threat landscape
- SOC system tasking is a standalone process divorced from other threat assessment processes
- High-end tradecraft not trickling down to volume policing
- Productivity-related processes for Policing is also disjointed and inefficient, with limited process automation currently in place.

Enabling Factors

Data Governance

- Inconsistent interpretation of Data Protection legislation
- The responsibility for data assets is cloudy, police lack the resource capacity to manage data assets
- Fragmented or inconsistently applied data management standards
- Slow stakeholder review and approval timescales around acquisition and use of data.

Information Technology

- No de-coupled layer for business logic (logic embedded in core code).
- Duplication of common data capabilities across security levels
- Legacy ITcannot easily be adapted to run analytical tools and packages.
- No overall enterprise architecture model for analytics and exploitation
- Limited current systems and data fragmentation results in shadow IT, tactical systems or manual processing

Security

- Insufficient accountability and auditing of users - internal threats, also known as insider threats
- Security and access control complexity across multiple systems at different levels of protective marking
- Onerous security design and testing arrangements make adoption or trialling of new technologies expensive and time-consuming.

X-Cutting Factors

People

- Policing lacks the internal capacity and capability required to monitor, collect, analyse or share data effectively
- Training gap on multiplicity of tools
- Recruitment &retention an issue

Process

- Lack of automation (data acquisition, data processing, data analytics, insight dissemination and decision support)
- Inconsistent data and analytical processes at low level of maturity

Culture

- Limited reward or recognition for maintaining good data practices
- Low data literacy
- Limited data-driven decisions

Organisation

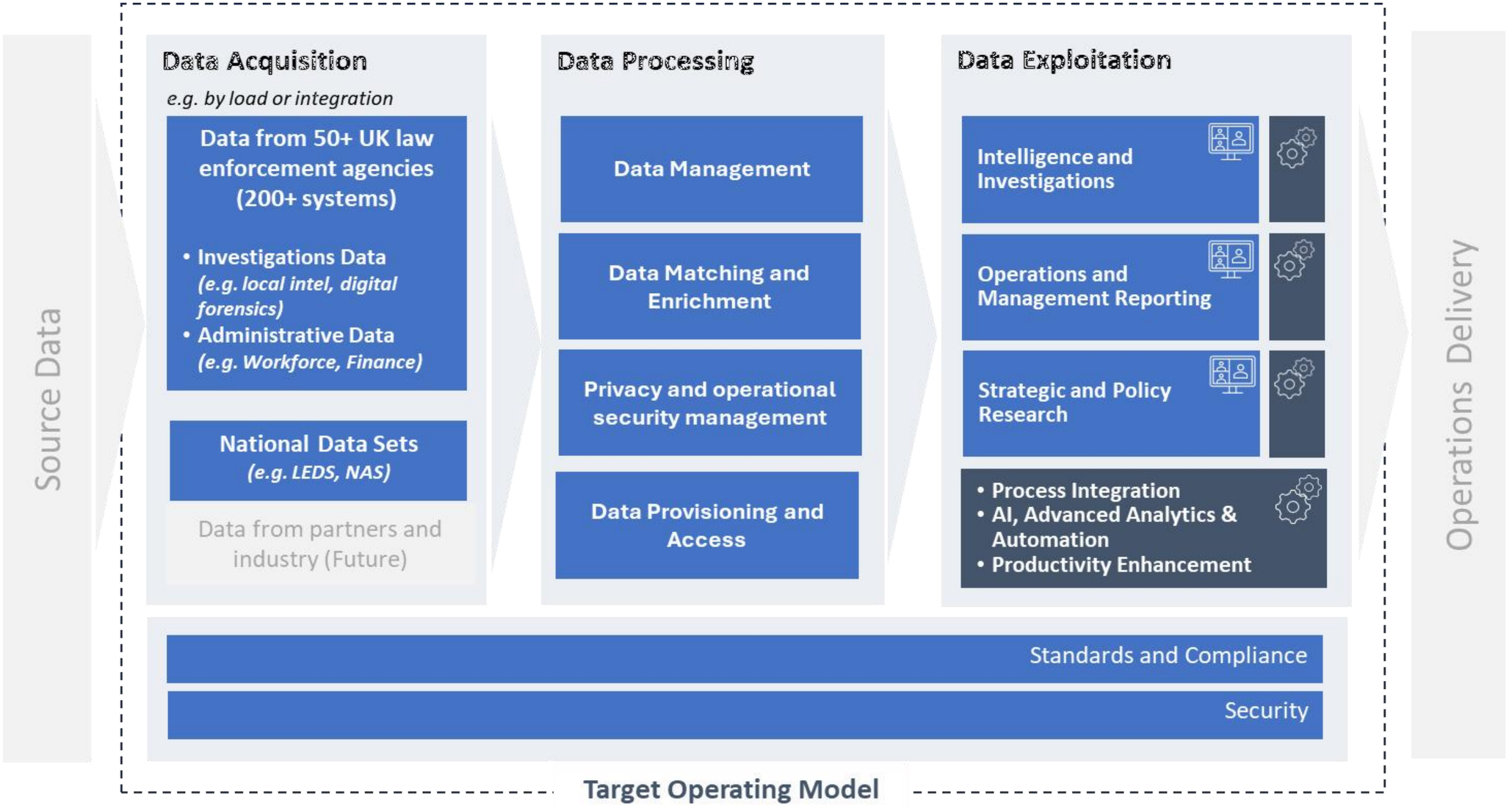
- Poor track record in delivering major programmes
- Limited ability to leverage academia and industry knowledge

Commercial & Fin.

- No common funding / cost recovery model
- Multiplicity of contracts resulting in poor economies of scale
- Limited shared funding approaches (first passenger buys the bus)

NPCC
National Police Chiefs' Council

National Data Integration & Exploitation Capability Scope



Facial Recognition withheld in full **S31(1)**