NPCC
National Police Chiefs' Council

National Policing Digital Strategy

2025-2030

Association of Police and Crime Commissioners

POLICE DIGITAL SERVICE

Contents

1	Foreword	4-5
2	Executive summary	6-7
3	The big picture in 2025	8-11
4	Our digital ambitions for 2030	12-13
4.1	Ambition 1: Protecting the public	14
4.2	Ambition 2: Seamless citizen experience	15
4.3	Ambition 3: Enabling officers and staff through digital	17
4.4	Ambition 4: Collaborating with the private sector	18
4.5	Ambition 5: Embedding a whole public system approach	19
5	How we get there	20-21
5.1	Sector strategy alignment	22-23
5.2	Governance	24-25
6	Our enabling pillars	27
6.1	Enabling pillar 1: Data and analytics	28
6.2	Enabling pillar 2: Strategic alignment	29
6.3	Enabling pillar 3: Modernised core data and technology	30
6.4	Enabling pillar 4: Connected technology	31
6.5	Enabling pillar 5: Risk and security	33
6.6	Enabling pillar 6: Talent in digital, data and technology	34
6.7	Enabling pillar 7: Open digital marketplace	35
6.8	Enabling bodies	36
7	Roadmap	38-41
8	Key considerations in delivery	43
8.1	Digital culture and skills	44
8.2	Responsible use of digital, data and technology in policing	45-46
8.3	Capabilities	47-48
9	Call to action	49
10	End notes and references	50
	Appendix – consultation	51
11	End notes and references	52

1 Foreword

Gavin Stephens
National Police Chiefs' Council

Rob Carden
Digital, Data and Technology Coordination Committee

Emily Spurrell
Association of Police and Crime Commissioners

Andy Dunbobbin
Police and Crime Commissioner for North Wales

Jonathan Evison
Police and Crime Commissioner for Humberside

Introduction to report from Chief Constable Gavin Stephens (NPCC Chair), Chief Constable Rob Carden (NPCC DDaTCC lead), Emily Spurrell (APCC Chair), Andy Dunbobbin & Jonathan Evison (APCC DDaT joint leads).

The UK policing model is world-renowned and sets the standard for law enforcement globally. However, the model as we know it, was designed at a time when the technology available was far simpler.

Today, the world around us has changed beyond recognition, becoming increasingly digital and presenting new, evolving pressures that our current system was simply not built to tackle.

The challenges we face are stark; outdated legacy systems which are costly to maintain, poor quality data that cannot be utilised and a fragmented policing model built before borderless cyber-crime even existed. This, combined with severe digital skills gaps, a lack of interoperability and a rising tide of public demand leaves us vulnerable as a service.

This strategy was initially published to drive digital transformation and make the changes needed. Since then, significant external influences have led to changes across policing that have both driven and disrupted the aims of this strategy, not least with the COVID-19 pandemic and the cost-of-living crisis which followed.

These factors, along with the growing need for a modernised police service have prompted a mid-point review of this strategy, to ensure it remains fit for purpose.

As part of this review, an extensive consultation process has taken place, gaining feedback from over 200 individuals within the law enforcement community (from a variety of roles), representing over 130 organisations across local policing, wider public sector and industry.

This has ensured diversity of thought, provided a clarity of focus and identified key areas of focus moving forward. This document should now be used in local, regional and national policing prioritisation and decision-making processes, to build on the Policing Vision 2030 mission of making our communities safer.

Police reform and rapid advancements in technology offer a once-in-a-generation opportunity to deliver significant, tangible change across policing.

- **To maintain public safety in a manner which is productive, whilst managing heightened public expectation and scrutiny, we must evolve and harness this opportunity, embracing innovation and new ways of working to ensure a service that is fit for the future.**
- **Over the last decade, digital technology and data and analytics have become integral to policing's ability to deliver an effective and efficient service. However, the way in which we deliver it is fragmented, and must be improved.**
- **Local policing will always be pivotal to ensuring we can tackle crime and respond swiftly to emergencies, protecting those most vulnerable and building the trust and confidence of our communities. However, to protect public money and maximise the impact of investments, we must change our approach to Digital, Data, and Technology (DDaT), striking a balance which respects local control whilst realising efficiency and effectiveness, nationally.**

We must work together collaboratively, across local policing, national law enforcement organisations and private industry to identify ways of delivering scalable, national services at pace.

- **Digital capabilities should be built once and well on behalf of all forces wherever possible, saving duplication of money and resource - all of which can be reallocated and used more effectively.**
- **As part of this, we must cohere policing requirements where possible and share our challenges with industry, to help solve problems that risk public safety at the earliest appropriate opportunity and manage ever-increasing demand.**
- **To deliver ongoing value for money, we must ensure transactions between police and industry are successful, with lessons learned and action taken from those which are not.**
- **All of this requires a collaborative, open-minded approach, working smarter nationally to drive improvements locally.**

Digital advancements will continue to move rapidly, and the challenges we face as a service will continue to evolve and increase as that happens. Together, we have a duty to take meaningful, collaborative action, driving the necessary changes to ensure that together, we can stand up to those tests long into the future.

- Some of those changes may be difficult and may force us to rethink our current ways of working entirely, but they are changes we need to make.
- This strategy provides a clear, refreshed summary of the digital ambitions we have, with clear measures in place to track our progress and tangible action. It outlines what we want to achieve by 2030 and the actions that must be taken to ensure we get there. Let us embark on that journey, together.

2 Executive summary

High level overview of the National Policing Digital Strategy

The National Policing Digital Strategy 2025-2030 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"*.

This document acts as the **strategic north star for all things DDaT in policing** by providing the direction, purpose and high-level roadmap necessary for responsible organisations. **Local forces and national sub-boards across policing are enabled to set out detailed plans on how they will deliver the roadmap and wider strategy from their own perspective**. NPCC, APCC and Home Office are accountable for the success of this strategy in partnership with a range of supporting and delivery organisations.

How to use the National Policing Digital Strategy

1. Review local, regional and national strategies and delivery plans relating to DDaT and continue to refresh them, as required, to align with this 'north star' document.
2. **Ensure all DDaT related priorities and investment decisions align with the delivery of the 7 Enabling Pillars** *(note that workstreams should align with delivering the Digital Enablers, not the Digital Ambitions, as these are the high-level outcomes of successfully delivering the strategy).*
3. Work with APCC and NPCC colleagues leading DDaT to coordinate focus around the Underpinning Priorities to ensure the most effective sequencing of activity.

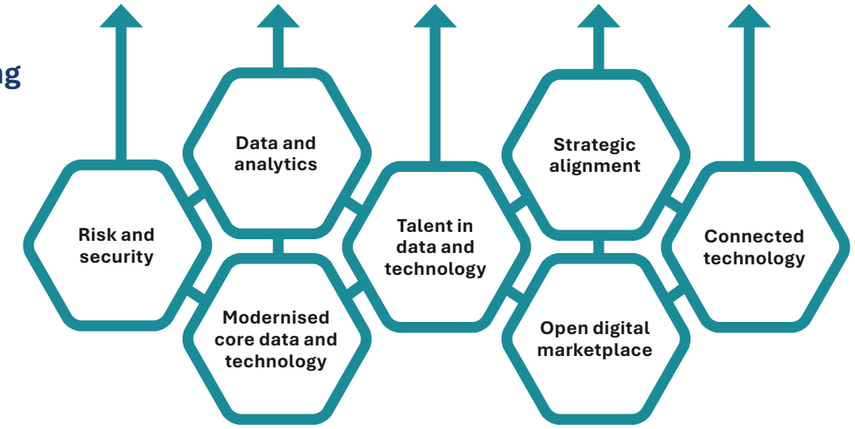
Through prioritising investments to deliver the digital enablers (and their underpinning priorities) we can successfully achieve the change we seek, to deliver the outcomes articulated in the Digital Ambitions by 2030.

At the national level, strategic investments will be made supporting provision of national systems and services that enable operational policing to deliver public safety, for example providing infrastructure or access to cloud services at scale and cost. These systems will be supported by clear standards, accessible platforms and wraparound support with future sustainability roadmaps.

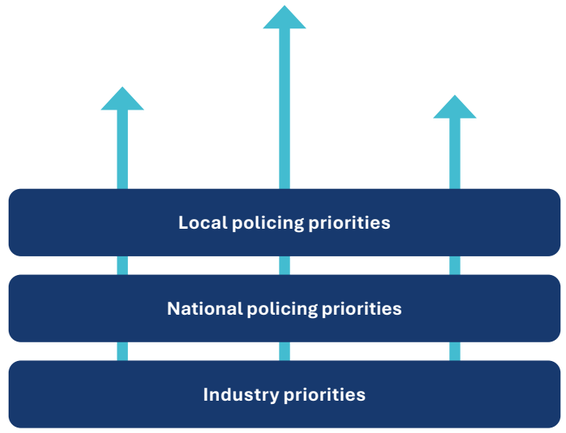
By 2030 policing will have access to modern solutions to enable them to protect the public, industry will have access to clear requirements to build those solutions, and the public will find it easier than ever to engage.

Our digital ambitions

Our enabling pillars



Our underpinning priorities



3 The big picture in 2025

The as-is landscape of digital challenges impacting policing

Beyond policing, the global digital landscape is rapidly advancing and embraced across many sectors. Supported by high quality, accessible and representative datasets, new technologies such as AI have enabled whole industries to transform their operations by enabling automation, enhancing data analytics, and improving decision-making. This global digital expansion has brought challenges, including cybersecurity threats, data privacy concerns, and the need for robust digital infrastructure to support ongoing innovation.

Policing, in contrast to other less regulated sectors (such as finance, retail or manufacturing) has lagged behind adopting new ways of working with technology and data. Organisations such as Police Digital Service (PDS), Office of Police Chief Scientific Advisor (OPCSA) and Blue Light Commercial (BLC) have entered the digital space to help policing solve challenges by supporting with national infrastructure and capability. Whilst some progress has been made around areas such as contact management, remote working and migration to cloud services, there are still significant challenges to overcome around prioritisation, people, legacy systems and budget. These hinder the pace, flexibility and agility of delivering solutions which can drive tactical solution development by forces, rather than strategic national adoption.

The sector's challenges are categorised under the headings below, with each accompanied by iconography for easy reference. These challenges are addressed later in the document, with icons indicating where each challenge is tackled.

- **Prioritisation**
- **Financial**
- **People and skills**
- **Data**
- **Legacy system maintenance**
- **Business change**

CHALLENGE

Prioritisation

Forces can struggle to balance short-term operational objectives with longer-term strategic priorities for investment in digital. Fuelled by a focus on local needs, the response to which is often urgently sought and, as a result, consumes the opportunity for a sector wide approach to tackling capability challenges. This also hinders effective prioritisation of risks and opportunities at local, regional and national levels, each with different risk appetites. Digital decision makers may lack a seat at the executive level, and so may not feel empowered, resourced or responsible to make more strategic choices around digital ownership and investment planning.

CHALLENGE

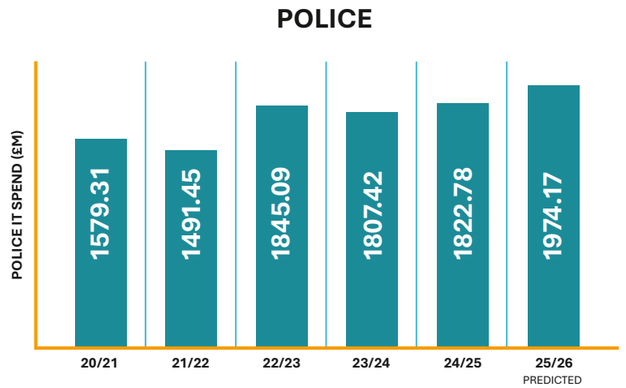
People and skills

The global demand for digital roles has grown, intensifying the challenge for policing to recruit and retain a skilled digital workforce. High turnover rates and competition for digital talent are made worse by the inconsistent ability for forces and delivery organisations to internally describe and then build up the skills needed in policing, compounded by inflexible police pay-structures, leading to an insufficient in-house resource pool. This shortage hinders the force's ability to execute and sustain long-term digital transformation initiatives due to a reliance on costly contingent labour or third-party supplier provided resource.

CHALLENGE

Legacy system maintenance

In the financial year 2024-2025, the policing sector spent ~£1.8 billion[1] on IT, with a significant proportion of that spend, allocated to maintaining on-premise infrastructure. Reliance on these diverse and often siloed legacy systems, and the way data is stored within them, has remained largely unchanged. **It is estimated in 2025-2026 that the total policing spend on IT will be ~£2 billion** of which ~£590 million will be spent on resources to maintain these systems. This significant expenditure represents missed opportunities for investment in more modern, secure and strategically aligned solutions, to benefit the sector by providing greater economic value by utilising the data in more effective, efficient and compliant ways, often not possible with legacy solutions.



CHALLENGE

Financial

We allocate approximately 11% of our annual policing spend to DDaT budgets. Despite this investment, short-term budget cycles, a capital-expenditure focus, leadership turnover, shifting priorities, and complex procurement challenges hinder progress. These constraints lead to inconsistent digital transformation, often leading to extensions of contracts with incumbent suppliers due to a lack of time and resource to explore more strategically valuable opportunities. This 'vendor lock-in' challenge may necessitate a higher initial outlay than other options to solve, but may equally represent greater returns on investment to the taxpayer, translating into improved policing outcomes and public safety.

Given these challenges, it is essential to highlight the value for money and savings considerations that must underpin all Digital and Technology activity. This provides further mandate for governance mechanisms such as the Live Services Board and FinOps, ensuring that spending decisions align with strategic priorities and long-term efficiency.

There exists an imbalance in the distribution of resource around the national coordination of DDaT in policing as opposed to that found within the Home Office. With only a handful of funded national roles to represent and manage DDaT on behalf of policing, this results in the strategy being managed less effectively.

CHALLENGE

Data

After our people, data is our second most important asset. We aim to continually improve our services through cutting-edge technologies such as AI, but without effectively capturing, cleaning, managing, using, and sharing data at all levels of the service, we won't achieve the full range of benefits from our collective investment of time, resource and public trust.

Advanced data capabilities remain a challenge due to poor digital literacy, inconsistent data-led decision making and inadequate technology platforms. The lack of engineering, analysis and science focused roles in the sector have resulted in continued challenges relating to poor data quality, disproportionate retention and siloed data. These continue to prevent policing from realising the full potential value from our data and capability investments.

Through ad-hoc local implementation of non-integrated force specific point solutions to local (rather than national) blueprints, the flow of data often stops within force boundaries, preventing policing from meeting recommendations set out in the 2004 Bichard Inquiry Report to enable better data sharing to prevent harm.

CHALLENGE

Business change

National digital strategies and solutions can suffer from failing at the last, hardest hurdle; of implementation and ongoing continuous improvement. Poor change management support and a reluctance to modernise local ways of working stifle efforts to embed valuable national solutions. This has been observed in the National Enabling Programme, where forces were left with the solution but no change support to embed and realise benefits. Behavioural and business change are essential to ensure that business and DDaT leaders can co-develop strategically aligned, consistent and effective ways of working to support digital decision making, rather than leaving IT departments to operate in a vacuum of resource and direction.

Through not having effective change practices, we have struggled to clearly articulate the benefits of DDaT investments, reducing confidence levels among funding sources. This has led to an inconsistent approach to investing in the police's ability to exploiting sustainable digital capabilities.

With so much complexity and challenge, we must give direction and guidance on how to harness the power of digital, data and technology to better protect the communities we serve.

4 Our Digital Ambitions for 2030

The original 2020 National Policing Digital Strategy stated, “The pace of change has never been so fast, but it will never be so slow again” and five years on this still rings true.

The current state of digital, data and technology presents an opportunity to explore but also creates a risk of distraction. Whilst there have been significant changes in the science and technology landscape, policing must retain a clear link between DDaT and public safety, whilst tackling the challenges outlined earlier.

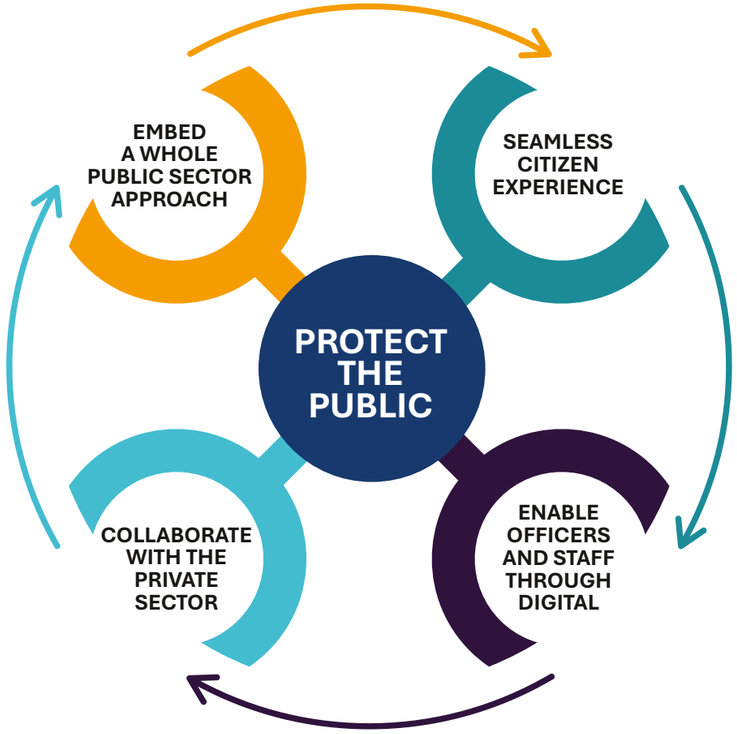
Police Vision 2030

Our fundamental policing mission[2] is to be the most trusted and engaged policing service in the world, working together to make communities safer and stronger. This overriding imperative requires any strategy in policing to have a clear link to the central pillar of keeping our communities safe by **protecting the public**, which this strategy enshrines as its core Digital Ambition, supported by four others that embody the NPCC Science and Technology strategy.

How do the Digital Ambitions fit together?

Although all ambitions directly relate to protecting the public as the core ambition, they operate in a cycle, each adding further value to the next. We must achieve them all, to successfully deliver this strategy.

- **We can better protect the public through the public themselves having a better seamless citizen experience when they engage with the service.**
- **We can provide a more effective seamless citizen experience through enabling officers and staff through digital, data and technology training, tools and support.**
- **We can operationally enable officers and staff through digital more fully, through collaborating with the private sector to create or provide the required digital resources.**
- **We can collaborate with the private sector at scale, in an affordable, efficient and sustainable way through embedding a whole public sector approach to make the policing sector a more cohesive, attractive and intelligent customer to work with.**
- **We can embed a whole public sector approach through ensuring protecting the public is at the heart of all our decision making, to drive alignment and prioritisation.**



4.1 Ambition 1 Protecting the public

This ambition draws all other ambitions with the Peelian principle[3] that 'the basic mission for which the police exist is to prevent crime and disorder.' It reinforces the fundamental duty of policing to act in the public interest, ensuring the safety and well-being of all communities. We will harness the power of digital to proactively identify and manage the risk of harm to better protect the public. By delivering earlier, more precise and targeted preventative and reactive policing approaches, utilised by neighbourhood and specialist police teams, we can reduce the impact and likelihood of offending on the public.

Vision

- **Core technology**
  Exploit seamlessly interlinked core police systems namely; Records management, Command and control, Enterprise resource planning and others, to enable policing to drive value across its digital estate to improve policing outcomes.
- **Core data**
  Ethically and accurately capture and convert every single piece of intelligence and evidence available to policing, into universally re-usable pan-police datasets, to help manage threat, harm and risk across all policing use cases.
- **Core security**
  Secure all police networks to enable the confidentiality, availability and integrity of police data.

Success statements and benefits

- **We will have prioritised effective and accurate data capture, cleaning, sharing, management, and use across policing and with partners.**
  - This will provide greater autonomy to frontline officers and staff who are closest to the policing challenges and need the most accurate information, enabling them to make faster, more proactive, efficient and effective, data driven decisions to reduce opportunities for harm.
- **We will have established clear and consistent measures and methods to evaluate the value of local DDaT solutions against strategic objectives which ultimately support public safety.**
  - This will enable policing to rapidly understand which solutions are unlikely to provide a strategically satisfactory return on investment, allowing early termination and recovery of funds to be reinvested in initiatives more likely to succeed in delivering strategic outcomes to enhance public safety.

How will this be delivered?

See sections **How do we get there** and **Our enabling pillars**.

Success measure

Yearly improvement in police digital, data and technology capability linked to protecting the public.

4.2 Ambition 2 Seamless citizen experience

We will provide citizen-centric digital services, offering the public a choice of accessible engagement options while responsibly connecting data across departments and organisations. Enhancing our intelligence and building public trust through our visible commitment to protecting the public and their data rights.

Vision

- **Public contact**
  Enable local communities to connect with their local force through a range of direct and self-service digital engagement channels that are inclusive and widely accessible.
- **Integrated data**
  Connect citizen data across departments and organisations to add value without incurring any additional friction to the public or their data rights.
- **Open data**
  Responsibly manage and securely share data with partner organisations to enable better public services whilst maintaining public trust and confidence.

Success statements and benefits

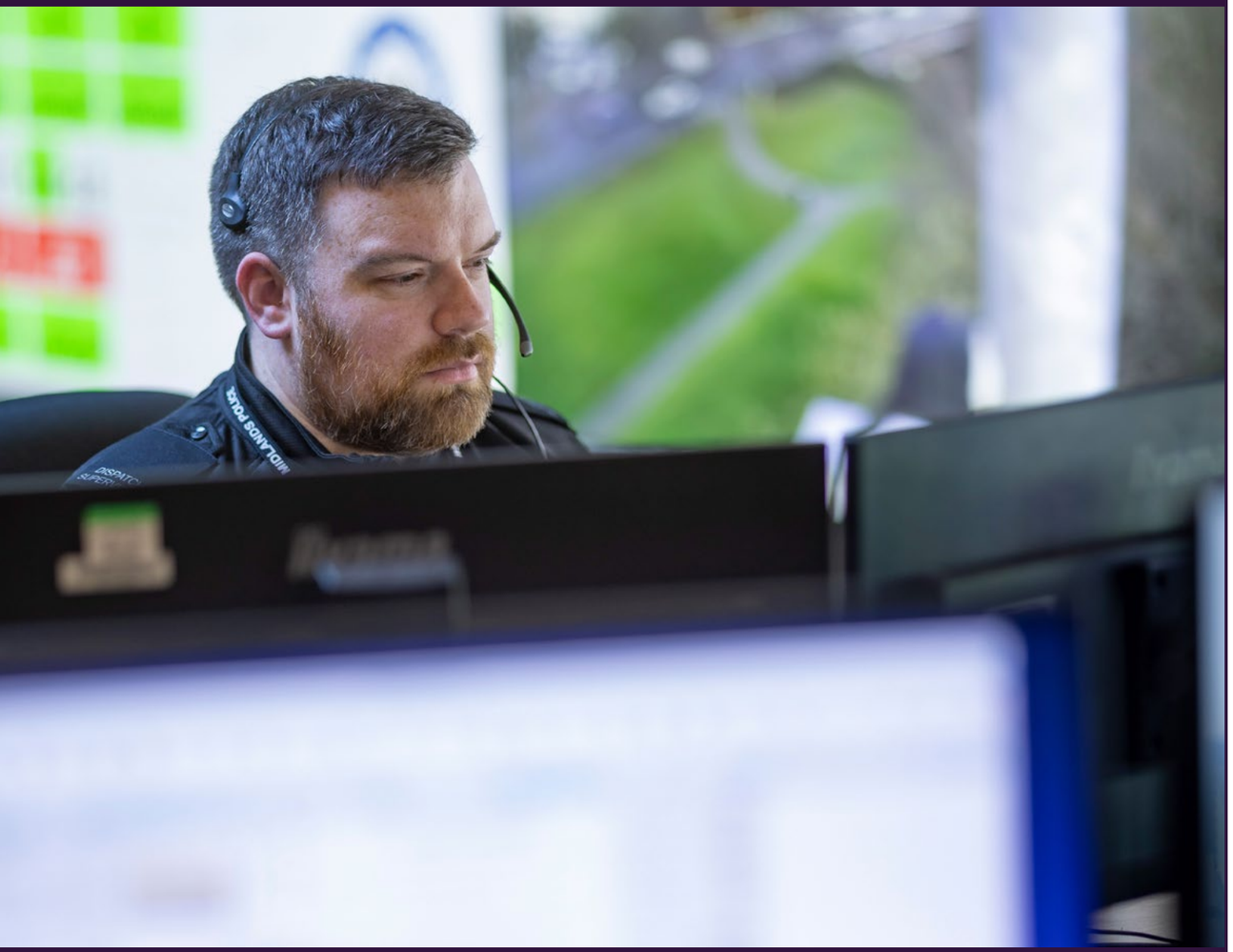
- **We will ensure that the end-user experience is prioritised from problem definition through to solution designs, implementation and continual improvement of the end-to-end solution.**
  - This will minimise barriers to accessing police services, enhance inclusivity, and strengthen engagement between the public and the police. It will also enable higher-quality interactions, leading to more effective resolutions and increased levels of public trust and confidence.
- **We will have embedded a culture of collective responsibility in the design, production, and consumption of DDaT solutions to promote ethical, environmental, economic, equality and security considerations.**
  - This will reduce the cost and complexity of retrofitting secure, legal, ethical and sustainable features to solutions. It will allow resources and focus to be redirected towards frontline policing initiatives while leveraging Open Data principles to promote transparency and drive innovation in public safety.

How will this be delivered?

See sections **How do we get there** and **Our enabling pillars**.

Success measure

Yearly increase in public satisfaction and confidence in effectively and efficiently engaging with police services through digital platforms.



4.3 Ambition 3 Enabling officers and staff through digital

We will equip our entire team, from leaders to front-line staff, with the necessary digital knowledge, skills, and tools to enhance their confidence, competence, and productivity in using digital solutions to proactively solve complex challenges.

Vision

- **Digital tools**
  Equip all officers and staff with necessary fully interoperable digital solutions and training to fully carry out their role to the best of their abilities.
- **Process efficiency**
  Provide every opportunity for officers and staff to focus on critical, value add manual tasks, making greater use of their specialist skills and knowledge.
- **Digital leadership**
  Continuously enhance the skills of all levels of leadership to ensure consistency and quality in critical digital decision making and governance.

Success statements and benefits

- **We will have ensured that DDaT solutions are successfully embedded within forces and integrated into flexible business processes, ensuring officers and staff receive required training to maximise their effectiveness.**
  - This will enable a greater range of benefits to be realised from a smaller number of digital solutions, enabling teams to become proficient in their use, resulting in more time to focus on improving policing outcomes.
- **We will have developed an empowered and driven digital workforce across all levels who are able to leverage DDaT in an efficient, effective, and responsible way both now and in the future.**
  - This will create opportunities for new digital ways of working to better meet demand, address risks and provide a more effective service to the public.
- **We will have ensured senior leaders are both digital leaders and intelligent digital customers when playing a critical role in guiding data and technology use, through accountability in selection, evaluation and implementation.**
  - This approach will establish a cohesive set of digital requirements and datasets, promoting consistent digital practices that enhance data accuracy, improve accessibility for the public, and build trust in how the police use them.

How will this be delivered?

See sections **How do we get there** and **Our enabling pillars**.

Success measure

Yearly improvement in levels of DDaT; training, skills and productivity (time savings, data and technology utilisation, process improvement and public engagement) across operational policing.

4.4 Ambition 4 Collaborating with the private sector

We will collaborate with the private sector to ensure they have a role in enhancing public safety, through securing effective contracts that deliver timely and budget-compliant solutions. Through early engagement in problem definition and solving, we will leverage industry expertise to address issues innovatively using data and technology. This approach will support policing to be an 'intelligent digital customer' by lowering barriers to enter the market and avoiding risk of 'vendor lock-in' through use of key artefacts, such as the Police Industry Charter[4].

Vision

- **Buy once**
  Provide industry with ability to engage with, and sell, sustainable services or reusable capability platforms (rather than single use point solutions) into, policing once and for all of policing (rather than 43+ times) with nationally aligned and efficient contract cycles.
- **Adopt standardised solutions**
  Leverage private sector collaborations to engage early, in compliance with Procurement Act 2023 regulations, to scope policing problems before moving on to identifying desirable, feasible, viable, sustainable and scalable solutions which comply with technical and security standards.
- **Strengthen partnerships**
  Build strong private sector relationships, developing effective methods of sharing people, skills and knowledge to support a joined-up approach to recruitment, retention and upskilling within policing and industry.

Success statements and benefits

- **We will have driven a collaborative and coordinated relationship with, and among, industry partners to explore a shared eco-system approach to solving problems.**
  - This will create a vibrant and competitive marketplace, enabling industry organisations to combine their strengths to help policing better understand its challenges and collaboratively develop solutions that benefit the public whilst providing best value for taxpayer money.
- **We will have a standardised and streamlined approach to procuring DDaT solutions on the national, regional and local levels to reduce inefficiencies, risks, and barriers caused by forces not working in a consistent way in many areas.**
  - This will make policing a more attractive market for industry investment by lowering costs and eliminating duplication of effort. Forces will benefit from economies of scale while gaining consistent access to top-tier solutions to empower officers and staff in delivering exceptional service to the public.
- **We will have a stable workforce of digital specialists sufficient to meet all the digital needs of policing**
  - This will ensure digital solutions can be rapidly translated from ideas to action to quickly address threats, risk and harm to public safety.

How will this be delivered?

See sections **How do we get there** and **Our enabling pillars**.

Success measure

Annual improvement in levels of satisfaction from industry and policing around collaborative delivery projects being on time, on budget and on quality.

4.5 Ambition 5 Embedding a whole public system approach

We will promote openness and alignment between policing and public sector partners. By integrating local digital needs with national digital requirements, we will empower grass roots innovation to successfully scale at pace, to provide valuable data insights and digital tools to help us protect the public with partner organisations.

Vision

- **Public sector collaboration**
  Partner with other public agencies using shared data to seek shared beneficial outcomes for the public, through regular strategic alignment.
- **One sector**
  Cohere policing requirements into a single intelligent 'digital police customer' able to reap the benefits of operating at scale with one, consistent voice and approach to identifying best practice across public and private sector.
- **Service integration**
  Establish effective arrangements to co-consume modern capabilities across the policing and wider public sector in an effective and efficient way.

Success statements and benefits

- **We will have regularly reviewed and updated this strategy (and sub-strategies relating to Business Change, Data and analytics, Information Assurance and Technology) to enable local forces, national organisations and wider industry to understand their role in contributing to its success.**
  - This will help reduce the burden and expense of all local and national policing organisations constantly reviewing the DDaT landscape for strategic change, instead focusing on this strategy.
- **We will have a National Centre of Policing with one integrated national DDaT function with one central data management hub and prioritisation model.**
  - This will provide scalable efficiencies which can be flexed and reconfigured based on the demands and use case requirements of law enforcement, improving productivity and speed of police capability delivery.
- **We will have adopted unified national standards, patterns and enterprise architecture approaches when developing local solutions, ensuring strategic interoperability, scalability, and inclusive digital accessibility.**
  - This will accelerate the innovation and implementation of digital solutions that have proven successful on a smaller scale or different sector. The associated reduction in costs and barriers will promote nationwide sharing of effective capabilities and data to improve policing outcomes for the public.

How will this be delivered?

See sections **How do we get there** and **Our enabling pillars**.

Success measure

Increase in number and speed of capabilities which are successfully scaled from local to national rollout.

We know where we are as a sector, and through these Digital Ambitions, we have a clear vision of where we need to be. We can reach our destination by 2030 through implementing a set of core Enabling Pillars to provide the required infrastructure to support these Digital Ambitions.

5 How we get there

There are five **Digital Ambitions**, supported by seven **Enabling Pillars**, achieved through sets of **Underpinning Priorities** tailored to local (and regional) policing, national policing and industry organisations.

The success of this strategy will be measured by achieving the digital ambitions. These will be achieved by successfully delivering the enabling pillars, which in turn will be achieved through successful delivery of the underpinning priorities.

Our digital ambitions

- PROTECT THE PUBLIC
- SEAMLESS CITIZEN EXPERIENCE
- ENABLE OFFICERS AND STAFF THROUGH DIGITAL
- COLLABORATE WITH THE PRIVATE SECTOR
- EMBED A WHOLE PUBLIC SYSTEM APPROACH

Our enabling pillars

- Data and analytics
- Strategic alignment
- Risk and security
- Talent in data and technology
- Connected technology
- Modernised core data and technology
- Open digital marketplace

Our underpinning priorities

- Local policing priorities
- National policing priorities
- Industry priorities

5.1 Sector strategy alignment

The two overarching strategies for policing in DDaT are the NPCC Science & Technology Strategy and this NPCC Digital Strategy. The other strategic documents relating to digital, data, or technology within the sector support this visionary strategy, which has the purpose of acting as a strategic policing north star for digital. These documents provide useful examples of initiatives that align and compliment with this strategy's Digital Ambition outcomes.

1 Protecting the public

- **a** Employ drones, body-worn cameras, and real-time surveillance tools to enhance operational efficiency (Policing Vision 2030 / NPCC Science and Technology Strategy).
- **b** Use geospatial and crime trend analytics to predict and respond to hotspots and emerging threats (Policing Vision 2030 / Future Operating Environment 2040).
- **c** Deploy AI for forecasting crime trends and optimising resource allocation (Policing Productivity Review / NPCC Science and Technology Strategy).
- **d** Introduce predictive models to prevent crime and proactively address public safety challenges (Future Operating Environment 2040).

2 Seamless citizen experience

- **a** Develop user-centric, digital public engagement platforms to improve access to police services and reporting mechanisms (Policing Vision / MOJ Digital Strategy 2025).
- **b** Use mobile apps and portals for seamless communication between the police and the public (Police Industry Charter).
- **c** Ensure technology and data systems are interoperable across forces and aligned with national strategies through the adoption of minimum acceptable standards (NPCC Science and Technology Strategy / MOJ Digital Strategy 2025).

3 Enabling officers and staff

- **a** Upskill officers and leaders in digital literacy and technology use to meet modern policing demands with a workforce equipped with digital skills (Police Industry Charter / CPS 2025 Strategy / Power of Information).
- **b** Create specialist roles for managing advanced technologies and data analysis (Policing Vision 2030 / Policing Productivity Review).
- **c** Create secondment opportunities and mobilise private sector volunteers to address the skills gap in policing (The Power of Information).
- **d** Leverage robotic process automation (RPA) to streamline administrative tasks and free officers for frontline duties (NPCC Science and Technology Strategy).

4 Collaborating with the private sector

- **a** Partner with industry and academic institutions to co-develop innovative solutions (Police Industry Charter / NPCC Science and Technology Strategy).
- **b** Enable local innovation to scale nationally through coordinated technology adoption strategies (Policing Productivity Review).
- **c** Foster partnerships with academia and the private sector to access cutting-edge cyber technologies (Police Industry Charter / Policing Vision 2030).
- **d** Provide industry with clearly defined and accredited minimum acceptable standards, developed in conjunction with policing, to build their products and compliant services upon (Police Industry Charter).
- **e** Replace outdated and inefficient systems like the Police National Computer with cloud-based, scalable, and interoperable solutions (Policing Productivity Review / NPCC Science and Technology Strategy / The Power of Information).

5 Embed a public system approach

- **a** Build advanced data analytics platforms to inform strategic decision-making and operational planning (Police Industry Charter / HMCTS Data Strategy v3).
- **b** Improve data quality and standardisation to enable seamless sharing across forces and agencies (Police Industry Charter / MOJ Digital Strategy 2025 / The Power of Information).
- **c** Create national data repositories and standards (The Power of Information).
- **d** Balance the adoption of surveillance tools with the protection of privacy and public trust (NPCC Science and Technology Strategy / Future Operating Environment 2040).
- **e** Establish ethical frameworks for AI and data usage to ensure fairness, explainability, and accountability (NPCC Science and Technology Strategy / HMCTS Data Strategy v3 / NPCC AI Covenant).

5.2 Governance

National

The APCC, Home Office and NPCC are committed to supporting this strategy through prioritising DDaT investments through a tripartite commissioning and charging model.

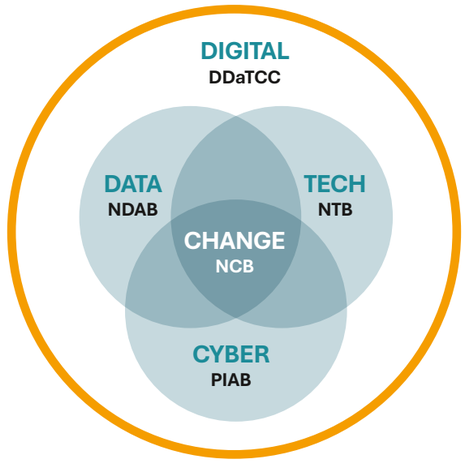
The process to progress the new capabilities and services required to implement the DDaT strategy are governed at the national level by:

- **The Public Safety Portfolio Commissioning Board (PSPCB) to review recommendations for strategic investments to provide resources required to deliver change.**
- **The Portfolio Assurance Group (PAG) to support and recommend the policing benefits of the commissioning proposals when at business case stage.**
- **The National Live Service Board (NLSB) to oversee the performance and benefits delivery of services and systems to policing.**
- **The Charges Oversight Board (COB) to oversee ongoing business cases for annual costs to run strategic police capabilities.**

NPCC NATIONAL POLICING DIGITAL STRATEGY	
What	Achieving the ambitions
Why	Protecting the public
How	Implementing the pillars
Through	Delivering the priorities
Who	Local, national and industry
When	Achieved by 2030

DDaTCC are supported by their four sub-boards, who collectively oversee and sponsor individual DDaT elements at the national level:

- **National Data and Analytics Board**
  Focuses on driving value from data analytics capabilities and ensuring privacy compliance.
- **National Technology Board**
  Oversees the improvement of existing and adoption of new technologies.
- **Police Information Assurance Board**
  Ensures information security and compliance.
- **National Change Board**
  Manages the adoption and enduring capability of digital initiatives across forces.



The NPCC DDaTCC sub-boards are collectively responsible for defining the digital policing approach to Data & Analytics, Information Assurance, Technology and Business Change through strategic plans to articulate how they will deliver what is contained within this National Policing Digital Strategy.

There is a tripartite commissioning process in place to progress the new capabilities and services required to implement the DDaT strategy – incorporating governance from, APCC, Home Office Public Safety Group and NPCC. This process will include the National Prioritisation Model (NPM) as a single co-ordinating gateway for policing to prioritise new national DDaT services, the Portfolio Assurance Group (PAG) to support and recommend the policing benefits of the commissioning proposals when at business case stage, and the National Live Service Board (NLSB) to oversee the performance and benefits delivery of services and systems to policing when they have been implemented.

This strategy integrates with other strategic documents and initiatives, providing direction for policing regarding DDaT in the law enforcement and criminal justice landscape.

Local

There exists a close, symbiotic relationship between national and local DDaT policing systems. Local are reliant on national for output, and national are reliant on local for input, for example the Police National Database. This system collates data from numerous local systems and presents it at the nationally accessible level. All these systems are ultimately funded by the tax payer and so should represent the best value for money in providing the best possible policing outcomes.

To most effectively adopt digital solutions and the benefits they can provide, local forces must commit to following the standards, patterns and blueprints set at the national level. Policing is already doing this in some areas, for example adopting the NPCC Cyber Strategy to 'defend as one' to enable secured access to resources. Without this commitment, this strategy cannot possibly succeed.

Industry

Digital leaders within and beyond policing have noted that progress since the launch of the National Policing Digital Strategy in 2020 has been hindered by competing local priorities, complex national governance, the burden of legacy systems, and a lack of interoperability. To ensure the success of this strategy, the following key points must be addressed:

- **This strategy's success relies on local police forces, regional and national bodies, aligning and effectively collaborating to break down silos in its implementation.**
- **Local police forces, regions and national bodies need to leverage industry expertise to deliver compliant systems and services to do this. Securing reliable and effective contractual arrangements to enable progress.**
- **Industry requires clearly defined and accredited minimum acceptable standards, developed collaboratively with policing, to guide the development of compliant systems and services. These will aid in transparency and accountability to build trust and ensure successful outcomes for all collaborating parties.**

NPCC DDaTCC will support development and maintenance of these standards to ensure police compliance with them through a quality assured management system, supported by wider policing and industry partners, to enable a competitive and vibrant market.

6 Our enabling pillars

Enabling Pillars and capabilities required to underpin the Digital Ambitions

This strategy sets out seven Enabling Pillars that underpin the digital transformation of our service and allow us to improve our capabilities to successfully deliver the five Digital Ambitions.

The Enabling Pillars represent the technical, commercial and governance infrastructure required to support the Digital Ambitions.

Creating the required technical, commercial and governance infrastructure to enable enduring achievement of the Digital Ambitions requires local police forces, national bodies and industry to work together on delivery and implementation of each Enabling Pillar. This five-year digital construction project will be achieved by each party delivering on their respective priorities by 2030, harnessing their unique skills, resources and position to help guide prioritisation and investment of resource, required to achieve effective police reform of DDaT.

6.1 Enabling Pillar 1 Data and analytics

To ensure transparency and build trust with data, a unified approach to data analytics is essential—driven by internal needs for strategic alignment, national mandates for data-driven policing, a national data analytics strategy, and the local imperative for efficiency and resource optimisation.

In support of this, The National Police Data and Analytics Board (NPDAB) has identified five key pillars for data and analytics capabilities: Data Foundations, Data Responsibility, Data Availability, Data Skills, and Data Analytics

Local priority – **Digital quality** – Services or solutions implemented should have a net benefit on data quality within policing as a whole.

National priority – **Collect once** – Reducing the burden on local policing to provide timely quality data by harnessing the power of analytical tooling to draw meaningful operational insights.

Industry priority – **Automation by default** – Productivity should be prioritised in solution design, to ensure where human intervention is required, this is to add value whilst still being able to scale with demand.

The following roadmap is a snapshot of sequencing required to achieve these Underpinning Priorities, to deliver this Enabling Pillar:

Data and analytics roadmap sequence			
1	2	3	4
Creation of **National Data and Analytics office**		Create **digital literacy curriculum** and pathways	Implement pathways into **workforce learning and development**
	Creation of **national strategy for Data and Analytics**	Creation of **platform to collect policing data** centrally	Implement capability to draw **analytical insights from national datasets**
Review existing and upcoming solutions in policing for **automation opportunities**	Liaise with policing end users to **validate investment case for change**	Update solution development priorities to value maximising productivity for officers and staff	

6.2 Enabling Pillar 2 Strategic alignment

We must align on a national vision for digital policing. This should be borne from the architectural principles we apply and should guide our investments.

Local priority – **Local strategy alignment** – Local Police Force Digital, Data and Technology strategies should align to the ambitions and enablers of this strategy, to enable a national enterprise architecture for policing. This approach will promote a focus on 're-purpose, before buy, before build' for digital solutions.

National priority – **National strategy alignment** – All national strategies involved in the provision of digital, data and technology components should ensure reference to and be in alignment with this strategy.

Industry priority – **Roadmap compatibility** – Products and services offered to policing should have a roadmap that aligns to the national strategy.

The following roadmap is a snapshot of sequencing required to achieve these Underpinning Priorities, to deliver this Enabling Pillar:

Strategic alignment roadmap sequence		
1	2	3
Align local and regional DDaT strategies to this strategy	**Create/refresh national sub-strategies** regarding Data and Analytics, Technology, Cyber Security and Business Change	**Adopt across local, regional and national policing** the national digital sub-strategies
Align national strategies to this strategy		
Align solution development with this strategy	**Refresh existing solutions in alignment** with strategic direction	**Provide fully strategically aligned solutions** to policing
		Align local **Policing and Crime Plans with Medium Term Financial Strategies** to support delivery of DDaT strategy

6.3 Enabling Pillar 3 Modernised core data and technology

We must take every opportunity to reduce the complexity, environmental impact and cost resulting from legacy data and technology infrastructure. We seek to modernise our DDaT estate, both physical and virtual, ensuring systems, datasets and core equipment are fit for purpose.

Local priority — **Leaving legacy** – Phased transition from outdated digital infrastructure and datasets to modern solutions which meet minimum acceptable digital standards, at the earliest commercially viable opportunity.

National priority — **Digital standards** – Manage system of minimum acceptable digital standards across policing, promoting sustainability, interoperability, transparency, and responsibility.

Industry priority — **Fit for future** – Develop digital products and services which align with minimum acceptable digital standards.

The following roadmap is a snapshot of sequencing required to achieve these Underpinning Priorities, to deliver this Enabling Pillar:

Modernised core data and technology roadmap sequence		
1	2	3
Baseline all existing data and technology, **mapping all relevant technical, commercial and operational data**	**Implement national standards** in any new procurements or existing contracts to measure performance	Implement a **phased transition from legacy infrastructure** as to modern solutions which meet standards as appropriate
Signpost (and create as required) **minimum acceptable digital police standards**	Establish **body to curate standards and manage kitemarking** of technology and data solutions	Implement **kitemarking of acceptable solutions** which align to strategic standards
	Update existing core solutions to meet minimum standards	Plan **minimum acceptable standards kitemarking into future solution** development

6.4 Enabling Pillar 4 Connected technology

We must empower our officers and staff with data and information when and where they need it, with interoperability at the core of connected technology, enhancing operational effectiveness and engagement with citizens through direct insights and functionality. This will see policing realise greater benefit from advancements in technology such as those around the use of artificial intelligence.

Local priority — **Solve once** – Local innovations should prioritise seamless integration of data and technology to ensure they contribute towards a national architecture approach to greatest benefit realisation.

National priority — **Guide interoperability** – Invest in the development of seamless data sharing and integration between different systems and agencies.

Industry priority — **Commitment on standards** – Work with policing and other private sector organisations, to develop and implement national digital standards around interoperability as standard.

The following roadmap is a snapshot of sequencing required to achieve these Underpinning Priorities, to deliver this Enabling Pillar:

Connected technology roadmap sequence		
1	2	3
Create **Migration to Cloud strategy** for policing and commence roadmap for adoption	Create **innovation development pathways** aligned to national blueprints and patterns	Adopt a **national police enterprise architecture** approach
Create **innovation blueprints** to describe acceptable innovation product for national implementation	Establish a capability to create and manage a **police API catalogue**	Incorporate police **API requirement** into all police procurement processes around digital
Create **Industry Interoperability Standard** outlining clear requirements for APIs in all solutions	**Capture benefits** of API implementation in policing vs manual or screen scraping robotic process automation work	

6.5 Enabling Pillar 5 Risk and security

We must maintain public trust by securing our data and by applying a consistent, proportional approach to risk across digital policing.

Local priority – **Balancing risk** – Manage risks effectively by cultivating the necessary skills and culture to secure our data and technology.

National priority – **Defending as one** – Protecting policing against attacks, detecting security events and minimising the impact of incidents.

Industry priority – **By design** – Implement Secure by Design practices from the outset of any product development cycle, ensuring detection use-case enablement is integrated into the development process to contribute towards cyber resilience.

The following roadmap is a snapshot of sequencing required to achieve these Underpinning Priorities, to deliver this enabling pillar:

Risk and security roadmap sequence			
1	2	3	4
Conduct cyber risk assessments to **identify where gaps exist in security** posture across all of policing	**Achieve full compliance** with national cyber standards across policing and police suppliers	Establish **police digital twin (or equivalent) capability** to run security, organisational and range of other tests in a low risk environment	Identify and manage security (and other, e.g. organisational) risks through **digital foresight planning, scenario planning using digital twins (or equivalent)** capability
Adopt **unified security policies** across policing	Develop **national cyber landscape protection and response** capability with direct access into all of policing		AI-driven analytics for **proactive threat management**
Collaborate with industry on **secure data-sharing protocols**	Develop **innovative cybersecurity solutions** tailored for policing		Create capability to **ensure kitemarking of solutions against stringent security certifications** and standards

6.6 Enabling Pillar 6 Talent in digital, data and technology

We must identify, develop, and position the current and next generation of data and technology talent across our workforce to help inform and enable our transformation.

Local priority – **Thinking digital** – Developing DDaT teams and empowering the wider workforce, including senior leaders, to consider relevant impact factors and consequences in digital decisions.

National priority – **Benchmarking skills gap** – Mapping the skills gap required to meet digital policing requirements.

Industry priority – **Skills investment** – Industry collaboration with policing to support digital workforce recruitment and retention.

The following roadmap is a snapshot of sequencing required to achieve these Underpinning Priorities, to deliver this Enabling Pillar:

Talent in digital data and technology roadmap sequence			
1	2	3	4
Identify all required digital policing roles both within DDaT and wider workforce, both now and in the foreseeable future	**Identify training, skills and knowledge required** for roles across officers and staff, including leaders in both DDaT and wider workforce	Establish which **professional standards** are required across DDaT roles	Develop a **national model built into the overall enterprise architecture** for digital policing
Standardise the role descriptions for DDaT teams and benchmark against industry	**Benchmark the skills gap** which exists across the policing workforce	Create capability to develop and **deploy technical resource** to fill skill gaps as forecasted and on demand	

6.7 Enabling Pillar 7 Open digital marketplace

We must cultivate a vibrant, competitive and open digital market that drives value and innovation to solve real-world policing challenges in a responsible way.

Local priority – **Engage early** – Engage with industry and national policing bodies to collectively define policing problems, enabling the digital marketplace to collaborate on developing problems through pre-market engagement[5] into effective solutions for policing, with users at the centre.

National priority – **Intelligent customer** – Single strategic approach to industry collaboration around policing requirements, benefits, priorities, and procurement.

Industry priority – **Bridging the gap** – Collaborating with SME's, trade associations and other members of industry to collectively solve policing challenges and scale strategically supported innovations into production.

The following roadmap is a snapshot of sequencing required to achieve these Underpinning Priorities, to deliver this Enabling Pillar:

Connected technology roadmap sequence		
1	2	3
Share local policing commercial, technical and operational data with national policing		Engage local DDaT with national industry engagement to **define problem areas of interest** with industry
Develop a **'Police Industry Engagement' capability**	**Centrally express policing problems** and requirements for industry to focus upon exploring	Provide Police Industry Engagement remit to **establish an open digital marketplace, adhering to required police standards**
Work with trade associations and wider industry to **identify collaboration partners**		

6.8 Enabling bodies

Police reform

Police reform plays an important role in improving policing performance, through creating a central policing body able to harness advancements in DDaT through enhanced procurement processes and targeted allocation of funding enabling forces to provide a higher quality of service to the public. Reform acts as a welcome catalyst to enable much of the transformational change sought by this strategy, and will itself necessitate this strategy being updated to reflect the structural alterations required. These changes affect only the 'how' of this strategy, without altering its focus on the 'what'.

Local policing support

At the local level Chief Constables are responsible for the operational deployment of new technologies to manage threat, harm, and risk. Together with the Police and Crime Commissioner (PCC), they ensure use is fair and lawful, balancing ethics, right to privacy, unbiased treatment and consent, with the absolute right to a fair trial. Thus, decisions are decentralised across 43 forces and contingent on Chief–PCC relationships. This local discretion is essential to effective delivery.

PCCs act as representatives of local communities and have the primary responsibility for holding Chief Constables to account for the provision of an efficient and effective police service. Their scrutiny and oversight are a critical element of the shared responsibility with Chief Officers for decisions about new technologies. PCCs are supported nationally by the Association of Police and Crime Commissioners (APCC) who work with the NPCC to share best practice and identify opportunities for joint working and resource pooling[6].

This devolved model of policing means Chiefs and PCCs hold joint responsibility for the effective investment of the local resources required to achieve the Local Digital Priorities highlighted in this strategy.

National policing support

The National Police Chiefs' Council (NPCC) Digital, Data and Technology Coordination Committee (DDaTCC), Association of Police and Crime Commissioners (APCC) are accountable for overseeing the coordination and successful delivery of the National Policing Digital Strategy within UK policing. Through working alongside the Home Office and its enabling and delivery functions, DDaTCC has created the National Prioritisation Model (NPM) to guide local, regional and national decision making around the commissioning of DDaT services and solutions to promote public safety and operational efficiency. This model supports the effective delivery of DDaT required to enable delivery of success across other NPCC coordination committees, including new solutions matured via the Science & Innovation Coordination Committee.

Organisations such as the Police Digital Service (PDS), Home Office DDaT, Crown Prosecution Service (CPS), His Majesties Courts and Tribunals Service (HMCTS) and Blue Light Commercial (BLC) are examples of the organisations involved in supporting the delivery of essential DDaT capabilities.

Engagement with these organisations is vital to ensure an effective DDaT delivery vehicle for policing. Through a collaborative approach, technical, cyber and commercial risk can be effectively managed, to allow local forces to focus on driving the best possible policing outcomes to protect the public.

Industry support

Industry have the support of national bodies within policing and industry bodies outside of policing (for example via trade associations), who can provide helpful information and signpost useful resources to support making the sector a more vibrant and competitive digital marketplace. The Policing Industry Charter[4] sets out foundational principles to foster collaboration between policing and suppliers, ensuring ethical, legal, transparent, and mutually beneficial commercial relationships that support policing priorities and deliver value to the public.

What do we need?

Whilst several Priorities can be achieved at pace, others require more resource and planning to deliver by 2030. Where investment is required, this document should be referenced to align the request to the strategic Enablers and Priorities.

The strategic Enabling Pillars do not exist in a vacuum. There is a clear need to address the requirements for; sound financial and operational control, a forward facing digital culture and clear process for decision-making to take into account strategic priorities in line with competing local demands.

Through policing making use of the National Prioritisation Model (NPM) in conjunction with the Charges Oversight Board (COB) and National Live Service Board (NLSB), these strategic enablers can support the pace required to deliver all of the Enablers and Priorities to help us reach the Ambitions by 2030.

7 Roadmap

This roadmap contains a summary of all the Enabling Pillar priorities in a single place, with dependencies highlighted as appropriate to indicate where careful sequencing is required for successful delivery. Delivery of this strategy will be monitored every quarter by NPCC DDaTCC and reported upon through the annual DDaTCC delivery plan. This strategy will be updated as necessary to reflect the changing landscape of policing and areas of renewed focus for coordination. This will ensure effective implementation of the Enabling Pillars to successfully achieve the Ambitions by 2030.

Pillar 1 Data and analytics

Step 1	Step 2	Step 3	Step 4
Creation of National Data and Analytics office		Create **digital literacy curriculum** and pathways	Implement pathways into **workforce learning and development**
	Creation of **national strategy for Data and Analytics**	Creation of **platform to collect policing data** centrally	Implement capability to draw **analytical insights from national datasets**
Review existing and upcoming solutions in policing for automation opportunities	Liaise with policing end users to **validate investment case for change**	Update solution development priorities to value maximising productivity for officers and staff	

Pillar 2 Strategic alignment

Step 1	Step 2	Step 3
Align local and regional DDaT strategies to this strategy	**Create/refresh national sub-strategies** regarding Data and Analytics, Technology, Cyber Security and Business Change	**Adopt across local, regional and national policing** the national digital sub-strategies
Align national strategies to this strategy		
Align solution development with this strategy	**Refresh existing solutions in alignment** with strategic direction	**Provide fully strategically aligned solutions** to policing
		Align local Policing and Crime Plans with Medium Term Financial Strategies to support delivery of DDaT strategy

Pillar 3 Modernised core data and technology

Step 1	Step 2	Step 3
Baseline all existing data and technology, mapping all relevant technical, commercial and operational data	**Implement national standards** in any new procurements or existing contracts to measure performance	Implement a **phased transition from legacy infrastructure** as to modern solutions which meet standards as appropriate
Signpost (and create as required) minimum acceptable digital police standards	Establish **body to curate standards and manage kitemarking** of technology and data solutions	Implement **kitemarking of acceptable solutions** which align to strategic standards.
	Update existing core solutions to meet minimum standards	Plan minimum acceptable standards kitemarking into future solution development

Pillar 4 Connected technology

Step 1	Step 2	Step 3
Create Migration to Cloud strategy for policing	Create **innovation development pathways** aligned to national blueprints and patterns	Adopt **national police enterprise architecture** approach
Create innovation blueprints to describe acceptable innovation product for national implementation	Establish a capability to create and manage a **police API catalogue**	Incorporate police **API requirement** into all police procurement processes around digital
Create Industry Interoperability Standard outlining clear requirements for APIs in all solutions	**Capture benefits** of API implementation in policing vs manual or screen scraping robotic process automation work	

Roadmap continued

Pillar 5 Risk and security			
Step 1	**Step 2**	**Step 3**	**Step 4**
Conduct cyber risk assessments to identify where gaps exist in security posture across all of policing	**Achieve full compliance** with national cyber standards across policing and police suppliers	Establish **police digital twin (or equivalent) capability** to run security, organisational and range of other tests in a low risk environment	Identify and manage security (and other, e.g. organisational) risks through **digital foresight planning, scenario planning using digital twin (or equivalent)** capability
Adopt unified security policies across policing	Develop **national cyber landscape protection and response** capability with direct access into all of policing		AI-driven analytics for **proactive threat management**
Collaborate with industry on secure data-sharing protocols	Develop **innovative cybersecurity solutions** tailored for policing		Create capability to **ensure kitemarking of solutions against stringent security certifications** and standards

Pillar 6 Talent in digital, data and technology			
Step 1	**Step 2**	**Step 3**	**Step 4**
Identify all required digital policing roles both within DDaT and wider workforce, both now and in the foreseeable future	**Identify training, skills and knowledge required** for roles across officers and staff, including leaders in both DDaT and wider workforce	Establish which **professional standards** are required across DDaT roles	Develop a **national model built into the overall enterprise architecture** for digital policing
Standardise the role descriptions for DDaT teams and benchmark against industry	**Benchmark skills gap** which exists across the policing workforce	Create capability to develop and **deploy technical** resource to fill skill gaps as forecasted and on demand	

Pillar 7 Open digital marketplace		
Step 1	**Step 2**	**Step 3**
Share local policing commercial, technical and operational data with national policing		Engage local DDaT with national industry engagement to **define problem areas of interest** with industry
Develop a 'Police Industry Engagement' capability	**Centrally express policing problems** and requirements for industry to focus upon exploring	Provide Police Industry Engagement remit to **establish an open digital marketplace, adhering to required police standards**
Work with trade associations and wider industry to identify collaboration partners		

Review cycle

NPCC and APCC are committed to reviewing this roadmap on an annual basis, to coincide with the annual NPCC delivery plan cycle where policing priorities are published. This will enable further clarity to the roadmap to be added as the future unfolds.

Having this clarity will support Home Office agreement on the annual basis of DDaT areas of operational focus (e.g. in 2024 these were automation, facial recognition, AI and digital forensics). Policing and Home Office will agree these on a national basis and reflect them in commissioning board decisions for that year, referencing this strategy for alignment.

8 Key considerations in delivery

Critical elements to take into account when using this strategy to deliver change

In moving from intent to action we must be aware that data and technology investments cannot be made in isolation or considered in a vacuum. For policing to maintain its mandate to 'police by consent', the ethical questions around the responsible application of digital need to be carefully explored and governed. Likewise, the return we gain from such investments will not be realised unless we develop our people and a culture of change to transform the service in the right way.

8.1 Digital culture and skills

Our people must be at the heart of this digital transformation; they will be central in embedding new ways of working, embracing new technologies and forging new collaborations. We must foster a culture that recognises the power of digital to improve the way we operate and protect our society. In order to guide the most effective strategic decision making, this cultural change must be driven from the top.

Our digital leaders of tomorrow will need to endorse and demonstrate a genuine understanding of how to place digital at the centre of modern policing – this will require significant investment in their development.

To achieve this, we must break down silos between traditional technology and business change functions, be open to new models of citizen engagement, and explore how our service model should respond. Fundamentally, it means being prepared to challenge established ways of working.

This strategy highlights key culture, skills and structural implications arising from digital:

Culture

1 We need to invest in leadership in order to build and maintain a culture of partnership, being purpose- led and innovative.

2 We need to encourage more front-line innovation, providing supporting structures to capture and scale ideas and technologies from proof of concept to production.

3 We should foster a 'one-team' mentality – encouraging collaboration across forces and with public and private sector partners (for example, demonstrated as the 'defend as one' principle in the cyber sub-strategy).

Skills

1 Our leaders must become 'digital leaders' through learning embedded as a core thread within the College of Policing development curriculum.

2 We need to invest in upskilling our workforce to increase baseline digital capability, and over time develop digital fluency.

3 We must utilise nationally consistent guidance to officers and staff that encompasses the identification, collection, assessment and prioritisation of digital material in investigations.

Structure

1 We need to continue to evolve our governance, strategies and organisational structures to ensure that they are fit to deliver our digital transformation.

2 We must review our sourcing strategies and talent models to create a modern, flexible and digitally fluent work environment that will attract and retain new talent.

3 We need to improve data sharing and integration, establishing interoperable solutions that enable the transfer of learning and knowledge between forces and public sector partners.

8.2 Responsible use of digital, data and technology in policing

The ambitions of this strategy cannot be achieved if public confidence in police use of new digital and data technologies is not maintained. The principle of 'policing by consent' is particularly relevant and will become even more so given the ethical challenges provided by continuous technological advancement. This requires policing to engage with public concerns regarding the use and storage of data, privacy breaches, data accuracy and bias, and the quality of decision making informed by algorithms.

We are committed to maintain public confidence in police use of new digital and data technologies through the adoption of rigorous standards, local and national ethical frameworks, and independent oversight and scrutiny to support accountability and transparency.

At the local level, Police and Crime Commissioners are representatives of local communities and have the primary responsibility for holding Chief Constables to account for the provision of an efficient and effective police service. The scrutiny and oversight role of PCCs is a critical element of the shared responsibility with Chief Constables for decisions to deploy new technologies. Chief Constables are responsible for the operational deployment of these new technologies to manage threat, harm, and risk. Together with the PCC they must ensure that use is fair and lawful, balancing ethics, right to privacy, unbiased treatment and consent, with the absolute right to a fair trial. Thus, decisions about deployment are decentralised across 43 Forces and rely on the local Chief Constable – PCC relationship.

At the national level, PCCs and Chief Constables will need to be heavily engaged (through their representative bodies in the APCC and NPCC) to establish governance and ethics frameworks for new technologies such as AI and facial recognition. These technologies are associated with risks which demand public oversight, as well as public communication, both of which should be exercised by PCCs and Chief Constables working in partnership.

The College of Policing sets out the Code of Ethics, Data Ethics and Data-driven Technology Authorised Professional Practice (APP) to guide responsible decision making in this area, on how we will prioritise public service, lead with courage, and, respond with respect. These can be applied to all actions and decisions; from identifying a suspect through digital intelligence gathering, through to delivering digital training relating to giving evidence in court.

Through working with the Home Office (in the tri-partite relationship) the APCC and NPCC are committed to jointly delivering a national ethics framework that meets the highest standards.

This strategy confirms continuing support to:

1 Comply with the Public Sector Equality Duty (PSED) by giving due consideration to eradicating bias in DDaT workstreams. This should be achieved through establishing and working with local ethics committees, alongside adherence to relevant policies and guidance (e.g., Data-driven Technology APP) to maintain procedural fairness.

2 Collaborate with national policing partners such as the Association of Police and Crime Commissioners (APCC), College of Policing (CoP), Office of Policing Chief Scientific Advisor (OPCSA) and wider NPCC coordinating committees. This will support the identification of relevant minimal acceptable standards to be adhered to and embedded in DDaT decision making at all levels.

3 Provide clear lines of accountability on data and algorithm use at the top of all policing organisations, including accessible complaints and redress processes.

4 Safely test the operational deployment of new capabilities which approach ethical and legal boundaries. To do this we will establish appropriate testing environments before we consider scaling solutions and approaches across forces.

5 Work with independent, non-policing bodies, such as the Responsible Technology Adoption Unit (RTAU) within the Department for Science, Innovation and Technology (DSIT), to ensure data-driven technologies used by policing are used responsibly to support society and businesses, with their benefits robustly explored to ensure a net gain in productivity.

6 Champion efforts from other policing bodies which support achieving the Digital Ambitions, for example the Police Industry Charter[4], or the Data-driven Technology APP.

8.3 Capabilities

Capabilities are the 'things that forces need to do' to deliver a complete policing service to citizens. Capabilities are delivered irrespective of organisational structure differences across forces and therefore serve as a useful tool to highlight the impact of digital on forces. Models such as the Law Enforcement Capability Model (LECM) exist to help forces set out the strategic, core and enabling capabilities for policing.

This strategy depends on changes to all of the data-centric capabilities outlined in the LECM model. Namely performance, analysis, intelligence, data and information management. Improvements to these data-centric capabilities are critical to enabling more effective delivery of operational LE capabilities such as neighbourhood, response, investigation, and safeguarding.

However, the current definition of these data-centric LECM capabilities reinforces existing organisational silos, rather than encouraging cross-functional collaboration. Societal change, heavily influenced by digital trends, changes the nature of demand for policing from that which can be responded to by individual functions within the force, to that which is capability led and requires input from a number of different functions.

In order to maximise our investments in digital, we have defined a new set of Digital Capabilities that transcend traditional functional silos:

Knowledge provision and disruption

- **The provision of timely, contextual and accurate crime prevention advice based on insights from analytics; as well as the use of digital disruption techniques to disrupt identified criminal activity.**

Reporting

- **The ability to receive and create incident and intelligence reports through multiple channels from the public, our partners and the front-line.**

Data management and sharing

- **The storage of data in accredited data management systems which comply with national data management and handling standards and processes – allowing interoperability between forces and partners.**

Data acquisition

- **The ability to acquire data, maximising the potential provided by digital technologies in support of public safeguarding and crime prevention.**

Data preparation

- **The ability to access, cleanse and manipulate vast amounts of data efficiently and effectively and make this available for decision making processes, analytics and intelligence development activities.**

Process automation

- **The ability to automate predictable processes, as well as automated demand analysis and response to improve quality of decision-making, tasking and assessment.**

Analytics

- **The ability to provide insights from acquired data in the form of predictions, estimations and conclusions.**

Infrastructure and technical governance

- **Infrastructure which provides scalable storage and computing capabilities whilst enabling interoperability between forces and partners.**

Continuous improvement and innovation

- **The ability to continuously improve and innovate, promoting a culture of change and adaptation at the pace of the operational environment.**

Service sustainment

- **An effective governance structure in place which leads the delivery of projects. Assuring compliance with standards and policy for in-flight and newly implemented projects. Undertaking benefits management to ensure projects are delivered to the required scope, time, quality and budget.**

All of these Digital Capabilities can exist on various levels of maturity across policing. An approach to collectively benchmark these across forces to identify, share and leverage best practice and standards is supported, to ensure a collective 'levelling up'.

Digital Capabilities are critical to the realisation of our digital policing ambition. In focusing efforts, we will be able to maximise the return on our investment in skills, data and technology by avoiding development in silos that pit functions in competition with one another. We must integrate and then mainstream these Digital Capabilities within policing.

Sustainability

With the UK government's commitment to Net Zero by 2050 and the College of Policing identifying climate change as a key challenge, the NPCC, in partnership with the APCC and BLC, launched a decarbonisation programme in November 2021. Overseen by a Sustainability Governance Board, this includes representatives from APCC, NPCC, BLC, and OPCSA. One area of focus for the programme is around the emissions created through the digital supply chain – not just if a smart-lightbulb is energy efficient, but also the energy efficiency of the digital infrastructure powering the 'smart' element. This initiative aims to embed sustainable practices in UK policing, reducing the carbon footprint and aligning with national climate goals while enhancing operational resilience and efficiency.

9 Call to action

We are rightly proud of our Policing Model which provides both local responsiveness and strong accountability, however policing must continue to unlock the value of digital data and technology while maintaining public trust and confidence in its ethical and responsible use.

Over the last decade, digital technology and data and has become integral to policing's ability to deliver an effective and efficient service. The service must continue to rely on data and technology to transform our ability to capture evidence and protect the public.

In every sphere of policing, including digital, a balance must be struck which respects local control whilst realising efficiency and effectiveness through appropriate regional and national intervention. While the balance varies between policing functions, the need for prioritised investment in digital, data technology continues to be a strong and growing requirement, along with it, the need to find new ways of managing demand.

To deliver ongoing value for money, we must ensure collaborations between police and industry are successful, with lessons learned and action taken from those which are not. In such a fragmented landscape, we must cohere policing requirements where possible and share our challenges with industry, to help solve at the earliest appropriate opportunity.

The policing landscape will change, as it always has. Police reform creates the opportunity for a national policing organisation focused on providing digital capabilities which are effective and efficient at serving the sectors data and technology needs, guided by the NPCC Science and Technology and Digital strategies.

Our Digital Ambitions, Enabling Pillars and Underpinning Priorities are clearly defined and designed to be used by the sector – informing the decisions we make at every level across policing. We hope this strategy is also helpful to our partners and industry – providing a clear summary of what Digital Ambitions we have, what we have to do by 2030, and the importance we attach to working towards them by delivering the Enabling Pillars.

10 End notes and references

Appendix A – Consultation

This refreshed strategy involved extensive consultation with the policing community. Over 224 individuals from 124 organisations across local policing, national law enforcement, government and industry were engaged with between 2023 – 2025.

Organisations consulted

Local Policing, Regional Policing, National Policing, National Law-Enforcement, Police and Crime Commissioners, Policing Community, Government, Industry (Police, Security, Defence and wider), Trade Associations, Academia.

Events hosted

Date	Audience	Engagement
2023	Police	Survey and Workshops
2023	Industry	Survey and Workshops
01/09/24	Police	Surveys
22/10/24	Police	Workshops
22/10/24	Industry	Workshops
24/10/24	Police	Workshops
05/11/24	Industry	Workshops
18/11/24	Police	Workshops
10/12/24	Police	Presentation
10/12/24	Industry	Presentation

Roles engaged

ROLE TITLES			
Aggregation and distribution	**Data lead**	**Enterprise architect**	**Innovation lead**
CDIO	Data platforms and analysis	Head IT Strategy	IT Director
CEO	Data Privacy	Head of Architect and Assurance	IT Strategy and Innovation Manager
Chief Architect	Data Quality	Head of Business Development	NPCC Lead
CIO	DDaT Lead	Head of Data	Police and Crime Commissioner
Cloud Services	DDaT Strategy Lead	Head of DDaT	Portfolio Director
Consultancy Services	Deputy DDaT Lead	Head of Dept	Programme Director
Cyber Intel/data security	Deputy Programme Director	Head of Innovation	Research and Innovation Lead
Cyber Intelligence	Development Manager	Head of IT Strategy	Technical Design Authority
Cyber Security	Digital Forensics	Head of Operations	Technical Lead
Data Analytics	Director	Head of Strategy	Technology Change

References

1 National Police Chiefs Council and Home Office provided financials on total police spend on IT between 2020-2025

2 Police Vision 2030

3 Peelian Principles attributed to Sir Robert Peel, who established the modern police force in London in 1829

4 Police Industry Charter (Blue Light Commercial)

5 Pre-Market Engagement (PME) as defined within the Procurement Act 2023

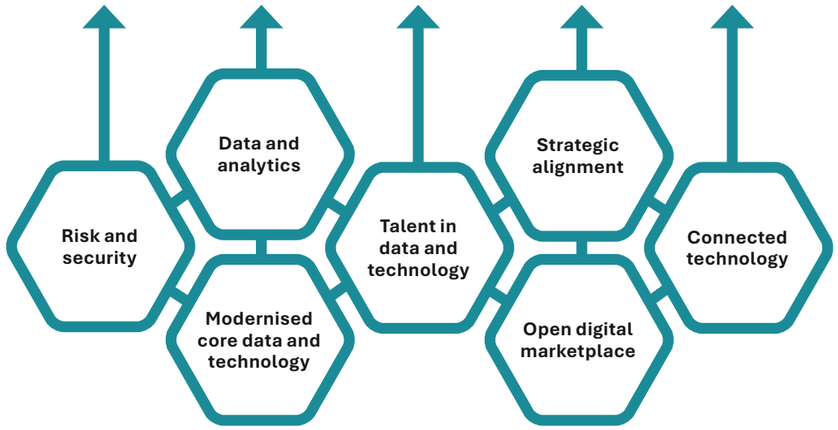
6 Extracts from ‘Technology Rules? The advent of new technologies in the justice system’

11 Key takeaways

Empowering policing to embrace digital, data and technology capability to deliver safer communities through measurable results

Our digital ambitions

Our enabling pillars



Our underpinning priorities

NPCC NATIONAL POLICING DIGITAL STRATEGY	
What is the expected outcome?	Achieving the five Digital Ambitions
Why are these outcomes important?	They ultimately ensure policing can best protect the public *Note: Activities should align with delivering the Enablers and Priorities, not the Ambitions themselves, as these are the high level outcomes of successfully delivering the strategy*
How can people make use of the strategy?	By implementing the seven Enabling Pillars into local, regional and national DDaT activities
Through what means?	Focussing upon the relevant Underpinning Priorities for each key stakeholder group
Who should be using this?	Local policing, national policing organisations and industry
When will this strategy be achieved?	Through following the Roadmap to delivery by 2030

- **Prioritise investment in strategically aligned DDaT activities**
- **Foster collaboration with industry**
- **Balance local control with national efficiency**
- **Reach out for support**

NPCC
National Police Chiefs' Council

Further information

For more details please contact us
via email at **DDaTCC@npcc.police.uk**

or visit our website at
www.npcc.police.uk

Association of Police and Crime Commissioners

POLICE DIGITAL SERVICE