NATIONAL POLICING DIGITAL STRATEGY

DIGITAL, DATA AND TECHNOLOGY STRATEGY 2020–2030

3

1 4

2 5

Getty Images/Sean Cook

FOREWORD

Policing in the UK is world leading and sets the standard for law enforcement agencies across the globe. However, our service is under new pressures.

We need to respond to more complex criminality, requiring more specialist skills, with an accelerating demand from cyber-crime, set against an enduring challenge around efficiency, effectiveness and funding. The borderless nature of crime is also challenging our current policing model.

Drop of Light / Shutterstock.com

Policing does not operate in a vacuum and cannot stand still in the increasingly digital world we work and live in. The challenges and opportunities that digital disruption present to policing are rapidly becoming defining issues for the service. We must move now and move quickly. While it may feel like the pace of technology change is already overwhelming, it is only going to get faster. We have however made progress in the last few years, particularly around mobile technology and migration to cloud services, but we need to do more to meet growing digital demands.

Information is the lifeblood of policing therefore we must make the most of the masses of data made available to us enabling intelligence-led preventative policing and investigation, while continuing to meet citizen expectations regarding how we handle their data. Digital ethics is a significant issue for the service and one where we need to work in collaboration with government and representative groups to ensure we have the appropriate policy framework and public engagement in place to maintain the trust and confidence of the public.

To protect people from harm in our rapidly changing world the service must modernise. We must develop capabilities to address the digital challenge and deal with the complexity of modern criminality through the exploitation of new technologies. Modernisation of the service will require a significant change in our policing system and we must consider what elements of digital transformation will be better delivered locally, regionally and nationally but with a clear convergence around a common roadmap.

Digital transformation is central to our 2030 digital policing ambition to drive improvements in data, technology and, most importantly, the skills of the people that lead, manage and use it. To do this we need to prioritise and focus our efforts across the service and be clear on what is needed to deliver it. We must make the best of local, front-line innovation and creativity; while finding the means to scale and deploy nationally and at pace. We must also recognise that we have a considerable legacy technology estate therefore investments must take account of the maturity and starting point of all forces.

This strategy sets out a new digital ambition for our service through a set of tangible digital priorities for policing and it outlines the key data and technology building blocks required to deliver them. In doing so, it builds on the *Policing Vision 2025* and other relevant cross government strategies which supports our core mission to make communities safer.

The Digital Policing Strategy 2030 has been developed by the service in response to the digital challenges facing us, but ultimately for the benefit of the public we serve. The service is committed to its delivery and it will be at the heart of our digital transformation both locally and nationally. We all need it to work. Working together, we are confident that the challenges associated with this modernisation are surmountable as part of a concerted and coordinated movement across the policing service.

Ian Dyson QPM
IMORCC Chair

Martin Hewitt QPM
NPCC Chair

Katy Bourne OBE
APCC Chair

1 THE BIG PICTURE

Policing is at a critical juncture. We either improve how we harness digital opportunities from existing and emerging technologies, or we are at risk of becoming overwhelmed by the demand they create and lose the chance to enhance and modernise our policing services.

The pace of technology continues to advance and digital adoption is accelerating. Policing does not exist in a vacuum: we must respond to evolving demands on our service, and overcome the internal challenges that currently hamper us.

We cannot continue as we have been doing - impeded by complex decision-making structures and hampered by the challenges of modernising a legacy infrastructure. The time is right for us to make fundamental and transformational choices: the way we work, harness data, exploit technologies, collaborate with partners, and organise ourselves.

Change will never be this slow again

The pace of change has never been this fast, yet it will never be this slow again. We are living through remarkable advances in mobile, cloud, artificial intelligence, sensors and analytics. *As society becomes increasingly connected – with people spending more and more time online,*[1] and our dependence on digital technologies and channels grows – our police service needs to catch up, and keep up, with a constantly evolving digital landscape.

A majority of UK citizens expect us to adopt technology to keep them safe from traditional crime.[2] They also expect this adoption to take place at a quicker rate than criminals who are exploiting advanced technologies to cause harm.[3]

Digital adoption is expanding the availability of data

Over the last two years, *90 percent of the data in the world was generated*.[4] This growth of data goes hand-in-hand with an increasingly sophisticated ability and need to analyse large datasets to discover trends, and use of artificial intelligence to quickly support decision making with insights drawn from vast quantities of information.

The potential benefits are immense. Data-driven insight has the potential to be a 'force multiplier' – increasing the predictability, precision, pace and impact of our interventions, from simple chat bots that use historic data to better support citizens, to more complex systems that can provide insight into crime location and optimum resource deployment. This game-changing promise of big data and machine learning requires policing to treat data as a strategic asset in how it is captured, managed and analysed. It also requires a collective commitment to its secure flow across our forces and partners, with a proportionate attitude to risk, transparent debate, and a commitment to the ethical use of data.

CLICK HERE FOR NOTE REFERENCES

Threats and opportunities are being unlocked

Advanced technology is no longer the exclusive domain of big corporations and governments; falling costs are accelerating the pace of development, and disrupting our economy and society. It is increasingly affordable and accessible. In 1967, storing one gigabyte of data would have cost £800,000 – *today it costs less than £0.016*.[5] This democratisation of technology introduces opportunities for criminals, which in turn presents a major threat to public safety; *it is estimated that more than 90% of reported crime now has a digital element*[6] – enabling threats, increasing their complexity and generating evidence. We need a service that embraces the same sophisticated technologies to tackle the evolving demand.

Evolution of demand and response — traditional crime

The nature of "traditional" threats has evolved with digital platforms and technology. Almost every traditional crime now has a digital element to it in terms of both how it was committed, and how we can investigate it.

Organised Crime Groups across Europe can now use mobile encryption services and platform based business models to trade, taking advantage of multiple technologies (messaging applications and satellite navigation) to expand their market reach, increasing the societal financial burden and violence associated with it.

The accessibility of these adopted technologies allows such groups to enter other criminal markets, *increasing the likelihood of poly-criminal groups*.[7] Likewise, digital technologies are a key part of the solution in fighting organised crime. We are increasingly working with search engine companies to *provide targeted (preventative) messaging in response to search terms synonymous with gang related activities*.[8]

Building on Policing Vision 2025

This Digital Strategy for policing builds on the *Policing Vision 2025* to lay the foundations for a police service which is fit for 2030.

It sets out the:

- Ambition for how digital can transform key dimensions of the police service alongside the priorities that support this.
- Key data and technology enablers that will provide the foundation for digital transformation, with implications on our people, ethics and policing capabilities.
- Considerations for how policing mobilises and organises effectively to deliver the strategy over the next five years.

Getty Images/Orbon Alijja

Evolution of demand and response – new and emerging crime

While we cannot predict precisely how crime will evolve, new types of cyber-crime, fraud and digitally enabled sexual exploitation illustrate a fundamental change in the profile of demand that a modern police service must deal with. Technology is acting as an accelerator of harm as digital connectivity becomes more pervasive.

Cyber-crime is posing an increasing challenge to individuals, businesses and our democratic institutions – and although challenging to quantify, *estimates for the cost of this to the UK economy range from £4.6bn*[9] to *£27bn a year*.[10] New threats will rapidly evolve over the next 5-10 years, such as the *use of 'deepfake' videos to manufacture social unrest*,[11] and the hacking of autonomous infrastructure. Strengthening policing's ability to anticipate, and be more responsive to, such changes is a key consideration for this strategy.

Transforming our service

We must not mistake "digital" as an end in itself, but understand it instead as an enabler of our mission of preventing harm. It needs to be integrated into how our services are modernised, alongside our partners, and complemented by the skills our people need to do their jobs. We must better coordinate the upgrading of our service, and learn the lessons of the last 5-10 years to foster innovation and deliver transformation.

Our focus will not be limited to how we use data, or deploy digital capabilities and new technologies to improve our operations and services; we will also focus on how we protect our critical infrastructure with the right level of security to mitigate cyber threats.

Our digital journey is not starting from scratch, forces and national programmes are already delivering change through a number of in-flight activities. However, there is much to do if we are to deliver tangible change by 2025 and lay the foundations for 2030. Success will be apparent when we collectively stop talking about digital transformation because it has become the norm.

In 2018, the police service in England and Wales spent c.£1.4bn on technology and around 30% of technology staff spend is on resources to maintain on premise infrastructure. Our IT budget is approximately 11% of the annual policing spend so we have a clear obligation to maximise the benefit that we realise from that investment. The implementation of additional technology places an upward pressure on IT costs which we must mitigate by reducing expenditure on our legacy estate.

The challenges in modernising our data and technology are well known: legacy technology and supplier lock-in; our organisational structures; underinvestment in key areas; conservative risk appetite; and inconsistent understanding of our data. We must commission new work wisely, and avoid the development of new national systems where off-the-shelf products are already available. When we implement new technology our focus should be on re-use of designs and approaches across forces to maximise efficiency and learning across the whole policing system.

How do we harness the power of digital, data and technology to better protect the communities we serve?

Our expenditure is spread across three areas of investment and we must look critically at how efficiently money is spent in all three areas.

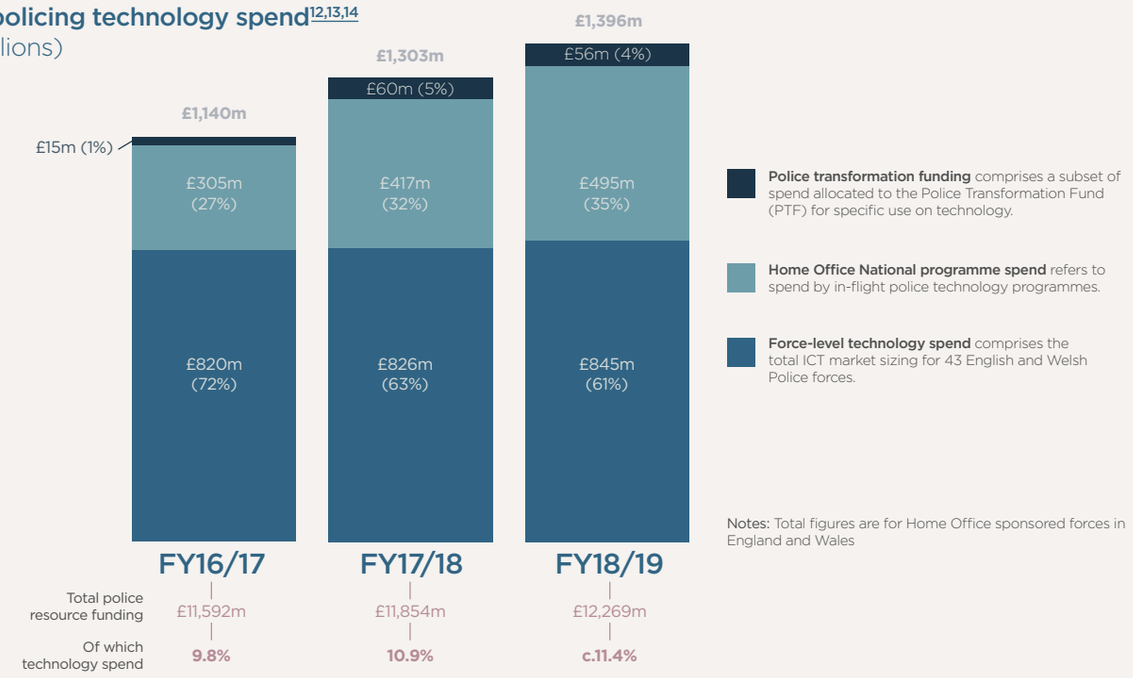
Together we can overcome the challenges

The strategy is written with the firm belief that the challenges associated with modernisation are surmountable, provided they are part of a concerted and coordinated movement across policing in England and Wales.

We need to move together across forces on this, realising economies of scale, sharing skills and generating insight; this could be in how we embed digital leadership and capabilities, how we get the most out of our legacy systems, how we ensure we achieve carbon neutral solutions, or how we innovate with emerging technologies. Mobilisation of this strategy is an opportunity to take stock of the specific changes required to better coordinate how we achieve this.

CLICK HERE FOR NOTE REFERENCES

National policing technology spend[12,13,14]
(GBP £millions)



IMAGINING 2030

From crowdsourcing evidence via thousands of pieces of digital media as part of an investigation, to building detailed simulations for complex responses to limit risk, using in-home sensors to assess a crime scene, or machine learning to detect patterns in an investigation — what seemed like science fiction a decade ago is now a reality.

None of us can foresee exactly how the next decade of policing will unfold. We can, however, assess how digital trends, behaviours around data, and new technologies will change the nature and volume of demand, and this will impact our ability to respond.

This strategy identifies key digital trends, and each raises some pressing questions for the direction of policing in England and Wales over the next 5-10 years:

Global, borderless, online crime

How will we clarify policing's role in order to address criminality which spans local and national boundaries?

Growing density of our digital lives

As people and devices become increasingly connected, how can we harness rich new sources of data and thus intelligence within appropriate ethical boundaries?

Vulnerability to digital distortion

As it becomes increasingly challenging to discern the true from the fake, how do we manage threats and risks to the public from media that is unreliable and that can rapidly spread?

The impact of bots, algorithms, automation and big data

How will we manage and harness the potential influence of digitisation on our everyday lives or across our workforce?

Complex convergence of our digital and physical realities

As digital becomes increasingly intertwined with our physical realities, how might policing evolve alongside this?

New crimes, and new victims, enabled by digital

How do we stay ahead of the curve and generate new methods to detect and respond?

The future of work

How will policing adapt our workforce model, leadership and culture to reflect changing future demands?

There are no definitive answers.

Our digital ambition aims to provide guidance for how we start to address these key questions. As part of this we know that our ability to exploit data and harness new technologies will be fundamental to enable us to respond to these digital trends.

In seeking to answer some of these difficult questions and understand the complexities our service will encounter, emerging technologies, as illustrated in the diagram below, generate significant interest. The technologies have varying levels of significance, maturity, and adoption rates, from autonomous vehicles that are currently in working demos, to big data and analytics that are in mainstream development.

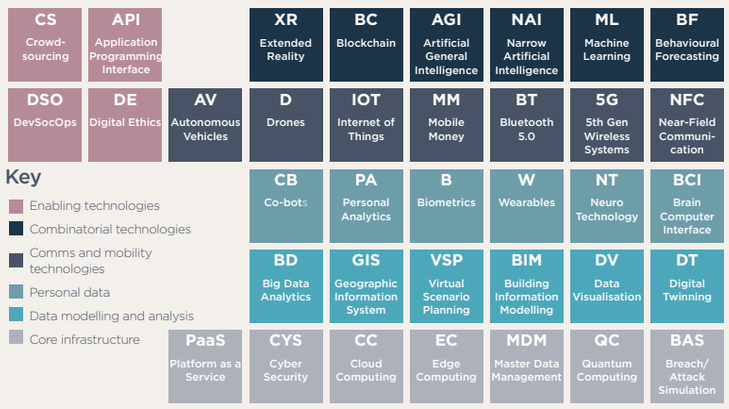
It is possible to imagine numerous solutions and threats through the likes of extended reality (XR), bots (through NAI and ML), and biometrics (B), which will have significant impact on the way policing operates in 2030 and beyond. Assessing combinations has helped us consider the possible disruptions and opportunities this strategy needs to address.

Rather than present an exhaustive list of potential threats and solutions in this strategy, we have considered the overall impact of emerging technologies for the transformation of policing. As part of this, we also considered how we enable the appropriate adoption of these technologies through modernisation of our technology estate in a consistent way.

Over time we will transition our computing and storage capability to the cloud, taking advantage of Software-as-a-Service to enable legacy rationalisation, increase the responsiveness of our technology estate and to deliver scaled efficiencies. These changes will begin to create a more modular and flexible technology estate that enables the secure transmission of data between connected applications and technologies, and ultimately creates the foundation for innovation to scale across the service.

Together with the critical questions prompted by digital trends, these disruptive technologies informed our digital ambition, priorities and enablers — providing a clear view of where we should focus our efforts and investments to modernise policing across England and Wales.

Policing Futures Framework



OUR DIGITAL AMBITION AND PRIORITIES

This strategy considers the internal and external pressures facing the service and presents five key digital ambitions, each with a set of digital priorities to guide focus and investment.

For each of these ambitions we envisaged the service we want to be in 2030, and how we can harness the opportunities of existing and disruptive digital technologies and capabilities.

1 Seamless citizen experience	We will deliver seamless, digitally enabled experiences. The public will have more choice in how they engage with us, using channels, media or devices most relevant to them. We will be able to connect citizen interactions, information and data across departments, and across forces to build a more credible and richer intelligence picture, all whilst maintaining public trust by ethically acquiring, exploiting and sharing their data.	
2 Addressing harm	We will harness the power of digital technologies and behaviours to identify the risk of harm and protect the vulnerable in the physical and digital world. We will deliver earlier, more precise and targeted proactive policing approaches and early interventions through the application of digital technology.	
3 Enabling officers & staff through digital	We will invest in our people, from leadership through to the front-line, to ensure they are equipped with the right capabilities (knowledge, skills and tools) to deal with increasingly complex crimes. We will establish digital leadership and ways of working to allow our workforce to focus on critical and value-adding activities.	
4 Embedding a whole public system approach	We will foster a philosophy of openness and deepen our collaboration with our public sector partners to jointly design and tackle complex public safety issues - sharing data insights and making use of digital tools to work more effectively across the public safety system, ensuring we do so in an ethical way to safeguard public trust.	
5 Empower the private sector	We will strengthen our relationships with the private sector to empower it to appropriately share in public safety responsibilities. The private sector, and the users of its services, have always shared responsibility for elements of public safety and, as technologies become easier and more accessible, there are new ways to safely empower those with an active desire to help.	

1 Seamless citizen experience

We will deliver seamless, digitally enabled experiences.

The public will have more choice in how they engage with us, using channels, media or devices most relevant to them.

We will be able to connect citizen interactions, information and data across departments, and across forces to build a more credible and richer intelligence picture, all whilst maintaining public trust by ethically acquiring, exploiting and sharing their data.

Priorities

1. We will make every digital interaction with us frictionless. The public will have the ability to contact us through relevant digital channels, submit multimedia evidence and self-serve for appropriate low-risk situations (if they choose) – all in a consistent and intuitive manner, irrespective of channel choice.
2. We will enhance physical experiences through digital means. This means we will use digital tools to improve the end-to-end citizen journey, and specifically the physical interactions within this, such as witness statements being enriched through body worn video footage collection.
3. We will harness shared data and connected devices ethically and securely. This means we will give the public the option to share data in near real-time where this is ethical and secure, allowing us to be more targeted in how we support public safety.
4. We will use digital technologies to enable the public to protect their communities. The public will be able to access policing platforms and channels to play a significant role in protecting themselves and their communities – in a way which is safe, appropriate and delivers positive policing outcomes and reduces the demand we face.

2 Addressing harm

We will harness the power of digital technologies and behaviours to identify the risk of harm and protect the vulnerable in the physical and digital world.

We will deliver earlier, more precise and targeted proactive policing approaches and early interventions through the application of digital technology.

Priorities

1. We will translate evolving definitions of threat, harm and risk (THR) into digital formats that complement human judgement. This means we will have digital formats for THR definitions that enable us to significantly improve our use of intelligent technologies to more rapidly and precisely address risk of harm or of offending, including recognising when and where digital technologies and channels are part of the risk exposure.
2. We will use digital tools to rapidly identify harm related behaviours in order to target interventions. We will have the digital capabilities to more precisely identify, and appropriately intervene where citizens are at risk of harm, or of offending at key moments. This will also allow us to be more informed and effective in our approach to community and neighbourhood policing.
3. We will use digital tools to disrupt criminal activity.
   We will have the digital capability to identify the potential for harm to large groups of the public, and to disrupt this activity accordingly. Key to this will be our ability to disrupt large-scale threats online, and organised criminal groups which exploit technology.
4. We will design and deliver digitally-enabled interventions that work across boundaries. We will adopt digital technologies such as automated data-sharing mechanisms and data analysis tools to deliver more targeted and digitally supported interventions to prevent harm, across forces and with partners, in a streamlined and efficient manner which avoids duplication of efforts.

3 Enabling officers & staff through digital

We will invest in our people, from leadership through to the front-line, to ensure they are equipped with the right knowledge, skills and tools to deal with increasingly complex crimes.

We will establish digital leadership and ways of working to allow our workforce to focus on critical and value adding activities.

Priorities

1. We will digitise core policing processes — removing the need for manual, repetitive and duplicative business processes, increasing our officers' and staff's operational efficiency.
2. We will develop a digitally literate workforce and leadership. We will foster a culture of constant learning and evolution to equip our workforce, from leadership through to the front-line, with the knowledge, skills and support to fully harness digital technologies, intelligent insights and connected ways of working – helping us reduce our reliance on external expertise.
3. We will provide officers and staff with the digital tools they need. This means a workforce that is digitally enabled, by default, with technology that seeks to replicate the intuitiveness of consumer experiences - increasing their situational awareness and ability to make informed decisions.
4. We will establish specialist digital service hubs and cross-force networks. We will have the capability to tackle the most tech-dependent and enabled crimes, pooling expertise from all appropriate talent in a way that delivers desired outcomes for all forces.
5. We will establish new digitally-enabled, dynamic workforce models. This means we will have more flexible workforce models, allowing us to attract more talent, offer flexible career routes to retain talent, and even temporarily source individuals when surge capacity is needed. We will use digital technologies to have a more accurate and dynamic picture of 'demand and supply' to inform deployment decisions.

Getty Images/Monty Rakusen

4 Embedding a whole public system approach

We will foster a philosophy of openness and deepen our collaboration with our public sector partners and criminal justice partners to jointly design and tackle complex public safety issues.

This means sharing data insights and making use of digital tools to work more effectively across the public safety system, ensuring we do so in an ethical way to safeguard public trust.

Priorities

1. We will deepen our collaboration with public sector agencies to unlock effectiveness. Using digital technology and ways of working jointly designed with our partners means we will be able to collaborate effectively in a consistent manner, without having to re-build the foundations every time.
2. We will develop 'fluid' data and insight exchange between public sector agencies, within appropriate ethical and legal boundaries. This means we will be able to exchange information between public agencies, providing the whole system with richer public safety insights that cannot be created in isolation.
3. We will support the creation of integrated digital public services for public safety. The public will be able to address their public safety issues through a more consistent citizen journey, without constraints arising from public agency silos.

5 Empower the private sector

We will strengthen our relationships with the private sector to empower it to appropriately share in public safety responsibilities.

The private sector, and the users of its services, have always shared responsibility for elements of public safety and, as technologies become easier and more accessible, there are new ways to safely empower those with an active desire to help. But we must better define the nature of this responsibility to ensure this is effective, and to ensure that addressing the growing threat, harm and risk in digital spaces does not solely fall on the police.

Priorities

1. We will help define expectations through open dialogue with the private sector but also with input from citizens. We will be able to clarify expectations and responsibilities in public safety protection, to have a clearer ongoing delineation of roles and accountabilities. This includes the definition of the police's role in providing the national cyber security infrastructure to create a secure environment for business to operate within.
2. We will help build awareness of digital threat, harm and risk. This means we will work with partners to encourage more private companies, and their customers, to become more aware of these risks and understand how they can protect against it.
3. We will support the private sector role in digitally-enabled public safety. We will collaborate strategically with the private sector to help them ensure their products and services are secure by design — preventing them from being an unwilling enabler to harm.
4. We will foster a vibrant PoliceTech landscape. This means we will stimulate a competitive and innovative supplier landscape while working to actively remove commercial barriers. This will allow us to procure technology which suits policing needs while also aggregating our buying power to ensure we are increasing value for money.

TAKING STRIDES IN MAKING THIS HAPPEN

To deliver the ambition and priorities will require investment in our workforce, the re-engineering of established ways of working, and the modernisation of our current underpinning data and technology foundations.

The remainder of this strategy focusses on these foundations, proposes a set of activities that will enable their creation and assesses the key considerations in their delivery.

4 DATA AND TECHNOLOGY ENABLERS

We need to invest in these enablers in a collaborative way to achieve the priorities we aspire to achieve in the next 5 to 10 years. In setting out the data and technology enablers, we have also considered the impact on people, ethics and capabilities. Together, these illustrate how transformation can be delivered and sustained.

This strategy sets out seven data and technology enablers that underpin the modernisation of our service and allow us to improve our capabilities.

1. Data	We will unlock value from data while maintaining public trust. We will do this by improving national support and guidance on data management and drive convergence to a national data architecture model.
2. Strategic alignment and design	We will align around a national vision for police data and technology. This will be borne from the architectural principles we apply, and will guide our investments.
3. Modernised core technology	We will take every opportunity to reduce the complexity and cost of the legacy infrastructure as we modernise.
4. Connected technology	We will put the power of data and information in the hands of our officers and staff when and where they need it.
5. Risk and security	We will maintain public trust by securing our data and by applying a consistent, proportional approach to technology risk across policing.
6. Talent in data & technology	We will identify, develop, and position the next generation of data and technology talent required in our technology functions to help inform and enable our transformation.
7. Transforming the PoliceTech market	We will incentivise an open, vibrant PoliceTech market that drives value and innovation around real-world policing challenges in a responsible way.

1. Data

We will unlock more value from data while maintaining public trust. We will do this by improving national support and guidance on data management and drive convergence to a national data architecture and model.

Data is an essential asset to enable digital transformation. We need data that can be securely accessed by our workforce and our public sector partners to improve our services for citizens, the private sector and to enable positive community policing outcomes.

Data will help us shift from a reactive policing model, to designing proactive and preventative solutions to improve how we protect the public from harm.

Recommended actions:

1. Drive data quality and consistency by developing a reference data management guide nationally, to be deployed locally.
2. Develop, and converge towards, a common abstract data model, with supplier adherence, to facilitate system integration and data aggregation.
3. Improve secure access to data between police and partner organisations through in-force data sharing and access mechanisms, including federated identity management.
4. Define new relationships and responsibilities for data governance to drive a high-performing data culture, where data-sharing and quality are optimal.
5. Develop a national data ethics governance model to ensure data is acquired, used and shared in an ethical way to safeguard public trust.
6. Continue to build national automation, analytics, and AI capabilities to enhance data quality, facilitate data-sharing across systems and extract insights to deliver better service outcomes.

2. Strategic alignment and design

We will align ourselves around a national vision for police data and technology. This will be borne out in the architectural principles we apply, and guide our investments.

An agreed data and technology vision and roadmap will underpin policing digital transformation, delivering change in a consistent way across national programmes and forces.

Recommended actions:

1. Define a Policing Technology Blueprint or "enterprise architecture" capability to guide further transformation investments and drive alignment between national programmes and force transformation plans.
2. Enable forces to properly assess their as-is state, identify architectural gaps or duplications, and guide aligned local transformation activity by defining a logical force architecture and roadmap avoiding the creation of bespoke solutions in favour of Commercial off-the-Shelf (COTS) applications.
3. Define architectural principles for business, data, technology, and applications to drive consensus in developing and maintaining technology across policing.
4. Designate a technical design capability to support the uptake of architectural principles and standards to drive alignment across national and force level investments.
5. Create adoption guides that help forces simplify and speed up adoption of new functionality and minimise cumbersome centralised governance mechanisms.

3. Modernised core technology

We will take every opportunity to reduce the complexity and cost of the legacy infrastructure as we modernise.

It is essential that we invest in developing our infrastructures to meet existing and future demand. The recommended actions will provide the foundation for new digital services for our citizens and the private sector, as well as ensure we can work collaboratively and effectively with our partners. They will also be crucial in underpinning and enabling digital innovations.

Recommended actions:

1. Develop and execute a nationally coordinated transition to the cloud. Adopt a "cloud first" principle for applications and data, where economical. Consume Infrastructure-as-a-Service to enhance police storage and compute capabilities.
2. Update our network capacity by investing in more flexible and cost-effective ways of managing our networks to ensure our move to cloud is not barred by prohibitive costs or poor connectivity.
3. Consolidate applications and decommission non-essential infrastructure to deliver better value for money as well as the means to move towards more interoperable solutions such as Software-as-a-Service.
4. Apply a digital "loose coupling" strategy whereby legacy systems are not directly integrated into front-end applications or data layers. This will drive value from existing estate over a short delivery period.

Getty Images/Monty Rakusen

4. Connected technology

We will put the power of data and information in the hands of our officers and staff when and where they need it.

Operational effectiveness and the ability to protect and engage with citizens or our workforce can be significantly enhanced through connected technologies and by bringing insights and functionality directly to officers and staff wherever they are.

Recommended actions:

1. Define a roadmap charting the national policing connected technology standards to ensure our workforce is consistently enabled across the service.
2. Invest in common connected technology development to benefit from economies of scale and joint expertise.
3. Move towards open source code for policing mobile applications and formalise development standards to converge the policing application landscape towards the same high standards, as well as enabling interoperability with a larger range of partners and suppliers.
4. Converge to a mobile enterprise application environment at a national level to provide standardisation in the management of core requirements such as data security and device authentication.
5. Coordinate exploring the practical use cases, piloting and testing of emerging connected technology (e.g. drones, sensors, heads up displays) to maximise the potential of emerging technologies and to improve sharing of knowledge whilst also avoiding duplication of effort.

5. Risk and security

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

In the future we will exchange more data and information with partners, adopt new connected technologies and move to cloud-based infrastructures. But the move to a more open ecosystem will not be at the expense of security. We will investigate and invest in new security measures in light of evolving external threats to protect our systems from powerful next generation security threats such as quantum computers.

Recommended actions:

1. Define a holistic data and technology risk framework to enable more consistent risk decisions.
2. Define a “secure by design” model to align security standards across policing, which will be communicated to suppliers and partners to drive higher standards of cyber security across the service.
3. Provide standardised training and a formalised risk and security curriculum to ensure our service understands evolving risks we are exposing ourselves to.
4. Enhance existing risk and security communities to create a professionalised community of practice to equip policing resources with the right skills to assess risk.

6. Talent in data and technology

We will identify, develop, and position the next generation of data and technology talent required in our digital, data and technology functions to help inform and enable our transformation.

Digital transformation will alter the demands on policing digital, data and technology functions. To be able to deliver the Digital Strategy, we need to have defined the right roles and to have staffed these with the right people.

Recommended actions:

1. Implement a new data and technology talent model and sourcing strategies to help the digital, data and technology functions adapt to new demands from digital transformation.
2. Implement a new competency model to enable the change in core digital activities by delivering skill shifts in the digital, data and technology functions.
3. Redefine the role of the Chief Technology, Digital, or Information Officer to become a voice for digital and to support operational decision makers with the adoption of new digital capabilities to deliver improved services.

7. Transforming the PoliceTech market

We will incentivise an open and vibrant PoliceTech market that will drive value and innovation through the use of current and emerging technologies.

We need to improve our engagement with suppliers as we commence service wide digital transformation to drive greater efficiency and value for the policing family when we go to market. We need to create a vibrant market place where suppliers understand our expectations clearly and are incentivised to invest in policing technology.

Recommended actions:

1. Develop market and horizon-scanning capabilities to inform adoption of evolving disruptive technologies within public safety, and to provide guidance to citizens so that they can proactively protect themselves from disruptive threats.
2. Shift to a strategic partnership model with PoliceTech suppliers to work more collaboratively in designing policing solutions.
3. Set procurement frameworks for Commercial off-the-Shelf (COTs) products to ensure standardisation in procurement and adoption of products. This will minimise the burden of the procurement processes and enhance value for money.
4. Launch PoliceTech innovation challenges to bring emerging technology to address police challenges and incentivise suppliers to invest in the quality of their services and products.
5. Launch new funding mechanisms that support long term planning and PoliceTech innovation. This will help aggregate our buying power across forces whilst not blocking new disruptive market entrants.

Getty Images/Monty Rakusen

KEY CONSIDERATIONS IN DELIVERY

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 of the application of technologies 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.

Getty Images/Kypros

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 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.

The workforce transformation is already underway through national and local level initiatives. The College of Policing and NPCC are leading on the delivery of the Workforce Strategy to realise the ambition set by Policing Vision 2025. In support, 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.
3. We should foster a 'one-team' mentality – encouraging collaboration across forces and with public sector partners.

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 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 joint technical solutions that enable the transfer of learning and knowledge between forces and public sector partners.

Policing ethics

"The power of police to fulfil their functions and duties is dependent on public approval of their existence, actions and behaviour and on their ability to secure and maintain public respect."

This principle for 'policing by consent' is particularly relevant in today's environment, and will become even more so given the ethical challenges provided by continuous technological advancement.

The debate is already active, and public scrutiny is likely to increase over the next 5 to 10 years. Public concerns include the use and storage of data, privacy breaches, data accuracy and bias, and the quality of decision making informed by algorithms.

A number of the priorities set out in this strategy are underpinned by data; from sharing information across forces and partners, to collecting new data sources provided by digital channels and platforms, and applying data analytics, and AI to assist decision making. Appropriate and transparent consideration of ethics in pursuing these priorities is critical to maintaining the integrity of our policing service and the trust of the public.

We will be faced with decisions on what information we choose to acquire, the methods used to transfer and store it, and how we use it to inform actions. These decisions will need to be guided by collective debate, and made open to scrutiny to maintain public trust.

As initial steps, this strategy outlines a commitment to:

1. Develop a National Data Ethics Governance model, which will outline standards and guidelines to be adhered to and embedded in our decision making processes.
2. Establish a core principle that the public's views on data analytics are pro-actively built into an ethical assessment at the design stage of any digitally-enabled service improvement.
3. Provide clear lines of accountability on data and algorithm use at the top of all policing organisations, including accessible complaints and redress processes. This could be achieved by extending the Data Protection Officer role and updating Chief Officer responsibilities.
4. Safely test the operational deployment of new capabilities which approach ethical boundaries. To do this we will establish appropriate practises in 'lab' settings before we consider scaling solutions and approaches across forces.
5. Work with independent, non-policing bodies, such as the Centre for Data Ethics and Innovation (CDEI), to ensure data-driven technologies used by policing are used responsibly to support society and businesses.

Getty Images/James Baylis AMA

Capabilities

Capabilities are the 'things that forces need to do' in order 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. In recent years, with support from the NPCC, COP and National Programmes, Policing has become increasingly capability focused through the development of the Law Enforcement (LE) Capability Model. This model sets out the strategic, core and enabling capabilities for policing.

This strategy depends on changes to all of the data-centric capabilities outlined in the Law Enforcement (LE) 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 LE 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 unsettle 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.

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 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 the Law Enforcement Capability model.

TOWARDS DELIVERY — ILLUSTRATIVE ROADMAP

The digital enablers set out in this strategy seek to enhance and accelerate the service's capacity to adopt and implement critical digital capabilities – building on inflight activity. The journey will not be linear. The indicative transformation roadmap over the first five years comprises three phases as illustrated below.

	Phase 0 — mobilisation	Phase 1 — setting direction	Phase 2 — shifting experience	Phase 3 — redefining expectations
		Phase one focuses on laying the foundations for digital transformation. We see the first "moments of truth" as service-wide agreement to the delivery model, commitment to the technology blueprint, force-level roadmap planning, and a refined Law Enforcement capabilities model, to reflect improved understanding of cross-cutting digital capabilities.	Phase two will see concerted effort and results from modernising core technology to deliver digitally-enabled police services. This will enable the expansion of channels we offer to citizens, and support our ambition to scale ethical data sharing and interoperability across agency boundaries. Using the new delivery model, we will identify and drive scaled rationalisation of legacy applications to modernise the core. This will be challenging. Not all forces will be at the same level of maturity, and local constraints (e.g. contractual arrangements) will impact the pace of change. We will learn from, and align to, work that is already underway.	Phase three will be characterised by the new choices made possible by large benefits from modernisation. These will range from new and improved security measures to combat changing cyber-threats, through to new collaborative models for the provision and consumption of policing technology.
DIGITAL AMBITIONS				
Seamless citizen experiences		Definition of national citizen experience focussed on key user journeys and public empowerment. Definition of how existing infrastructure can be developed in support of this.	Significant expansion and integration of channels the public can choose to engage with us. Consistent citizen profiles available across forces.	Near real-time enrichment of the intelligence picture delivered to the font-line through ethical use of connected devices; leading to more proactive engagement.
Addressing harm		Development and refinement of digital format 'risk models' that support consistent triage and identify the Threat, Harm and Risk picture, including in digital spaces.	Proactive identification of Threat, Harm and Risk, to inform proactive neighbourhood (or community) policing approaches, and automated deployment of next best action interventions in offender management.	Multi-agency (private and public) delivery of interventions and scaled disruption of harm, across physical and digital realms, targeted and enabled digital technologies.
Enabling officers & staff through digital		Definition of digital skill requirement and expectations for the workforce through to 2030 (e.g. Digital Workforce Strategy and embedding digital in the Law Enforcement capability model).	Shift in learning and development delivery to reflect digital skill requirements; resulting in a more dynamic workforce that is enabled by targeted automation to reduce high volume, low risk, workloads.	Significant shift in data literacy and digital fluency at all levels. Scaled roll out of automation use cases. Shift towards preventative policing with optimum deployment support (situational awareness). AI to support complex decision making with enhanced intelligence packages.
Embedding a whole public system approach		Priority engagement with public sector partners to agree key areas for collaboration – defining responsibilities and dependencies. Define a roadmap to reduce system integration blockers and start addressing critical cross-agency data sharing issues in ethical ways.	Scaling of 'fluid' data exchange across agency boundaries in legal and ethical ways, supported by intelligent technologies to enable multi-agency working for high priority journeys.	Scaling of new platforms that support integrated service delivery across agency boundaries, and enhanced situational awareness with the near real-time transmission of data across for key journeys.
Empower the private sector		Define expectations through open dialogue with the private sector and citizens; clarifying the boundary between the role of the police to protect the public from harm, and the role of the private sector.	Incentivise innovation in the PoliceTech Market with new routes to innovation funding that enables long-term planning. This will be supported by greater clarity on architectural expectations for all suppliers.	Secure by design' becomes the norm for all private sector organisations that deliver products and services. This is supported by a clear offer of guidance from the police that promotes a secure operating environment.
DATA AND TECHNOLOGY ENABLERS		These core activities will include foundational digital milestones such as the definition of key national citizen experiences, and digital workforce skills requirements. This phase cannot be just design work. It must also include quick delivery of enhanced capability over the first year.	Convergence to the police data model, defined architectural principles, an increasingly rationalised application environment, and a coordinated design capability, will combine to create a more open and accessible technology estate. In turn, suppliers will have greater certainty over service-wide expectations on ensuring technologies are designed to be interoperable. There will also be new routes to innovation funding to encourage collaboration and development of new solutions.	We will scale the use of platforms for cross-agency collaboration and enhance situational awareness with ethical real-time data sharing. Focus will intensify on driving ever greater operational effectiveness with new advanced digital capabilities. Automated dispatch or "next best action" advice pushed to officers' connected devices will become possible by combining technologies such as mobility, IoT and AI. The service will continue to invest in innovation and work closely with the PoliceTech market to drive through the promise of digital transformation.
Data		— Establish data governance and organisation structures — Create ethical framework — Automation, Analytics & AI Pilots — Prioritised APIs exposed to key partners	— Large set of APIs exposed to key partners — Common data model convergence begins — Training roll out supporting data sharing and capability uplift of key roles — Scaling Automation, Analytics & AI solutions	— Comprehensive API set for partners/forces — High conformity to data model — Test more complex use cases of Analytics and AI solutions
Strategic alignment and design		— Enterprise and force logical architecture — Set up technical design authority — Develop local delivery roadmaps	— Roll out adoptions guides for standardised services — Support convergence to National Technology Blueprint	— Updates to target architecture in line with ongoing market scouting and horizon scanning
Modernised core technology		— As-is application review — "Quick win" automations — Commence digital decoupling for new front end services	— Application rationalisation and optimisation — First waves of network optimisation — First waves of cloud migrations	— c.80% of police technology hosted on public cloud — Common connectivity measures established to main cloud providers
Connected technology		— Set connected technology standards and roadmap (link to Enterprise architecture)	— Common connected technology development capability — Standardised deployment of connected technology across multiple regions	— Advanced means of data acquisition (IOT) — "Next best action" functionality to mobile devices — Policing mobility platform
Risk and security		— Develop technology risk framework — Develop security model (link into enterprise architecture) to embed secure by design approach	— First wave of training on new technology risk standards — Standardised risk and security roles in place	— Implementation of advanced security measures across enterprise technology estate (e.g. quantum computing defences)
Talent in data & technology		— New roles and expectations set — "Signature" appointments to key roles for the transformation	— Mature service orientated ways of working in place across policing technology functions	— Consideration of advanced shared service models for policing technology
Transforming the PoliceTech market		— Develop market and horizon scanning capability to PoliceTech use cases — Commence strategic supplier engagement	— Set procurement frameworks for COTs products — Launch new funding mechanisms that target PoliceTech Innovation	— Launch PoliceTech Innovation challenges to bring emerging technology to address police use cases

THE CRITICAL PATH

We will need to invest significantly in digital leadership and capabilities to deliver our transformation.

Based on current levels, over the next five years it is estimated that policing in England and Wales will spend between £7bn - £9bn on technology alone.

It is incumbent upon us all to deliver maximum value for money in how and where we direct these funds to achieve transformation.

It is recognised that policing's current national decision-making mechanisms must improve if the collaboration required to drive economies of scale across policing and national programmes is to be realised. The benefits will be tangible, from de-duplication of activity at the local level, greater consistency in the way that innovation is funded, through to increased realised benefit from some national programmes.

The improvement must be focussed on capability rather than structure; in how we distribute digital transformation capabilities across policing to serve the needs of the whole network, and of localities.

The diagram on page 19 illustrates the transformation capabilities we need to build and harness if we are to deliver this strategy. Some are specialist capabilities that will sit centrally, others will be more distributed, and force led. The definition of this model is key, and needs to be completed in consultation during the proposed Mobilisation phase.

The question is whether we need a more streamlined, effective version of the governance structures that already exists, or whether something bolder is required.

For some enablers, the answer will be clear: developing a Policing Technology Blueprint to guide national programmes and force level convergence will be done centrally, whereas the assessment of existing system applications will be owned at force level. Other enablers will require further discussion and alignment, such as the development and enhancement of automation, analytics and AI capabilities. Innovation is another such capability. It is likely a hybrid model will be required that incentivises innovation from the centre, to reduce duplication and ensure scalability of innovative solutions, and supports new routes to experimentation at the local level.

The new model for service wide, digital transformation delivery must be ultimately accountable to PCCs and Chief Constables but it has to carry enough delegated authority to succeed.

It will be characterised by a pooling of sovereignty that is driven by a very clear intent; the unlocking of local transformational outcomes in the most efficient and effective way possible.

Mobilising for delivery

There are number of actions that will be completed as part of a short mobilisation phase for the Strategy, these include:

- The definition of a Digital Charter that reflects leadership commitment to a set of agreed design and delivery principles.
- The definition of a detailed 12-18 month implementation plan for the strategy, aligned with planned activity at a national level.
- The development of an investment case for the implementation plan, aligned with SR19 and SR20 timelines.
- Lower level design of the Digital Transformation Capabilities and Governance model.
- Communication and engagement plan for the Strategy across the 43 forces, including a clear process for how it evolves over time.

Digital transformation capabilities and governance spectrum

Example transformation capabilities:

Principles and Standards: Supporting consistency across digital ways of working, solution development and procurement.

Strategy and Architecture: Coordinating alignment between business, data and technology direction and approaches.

Risk Assessment and Security: Defining scalable practices to secure data, applications and digital ways of working.

Investment Prioritisation and Roadmap: Prioritising investment to deliver coordinated national and local outcomes, and projected next steps.

Solution and Service Development: Implementing and building solutions that meet citizen, user and service needs.

Procurement and Strategic Supplier Management: Managing supplier relationships and stimulating industry engagement.

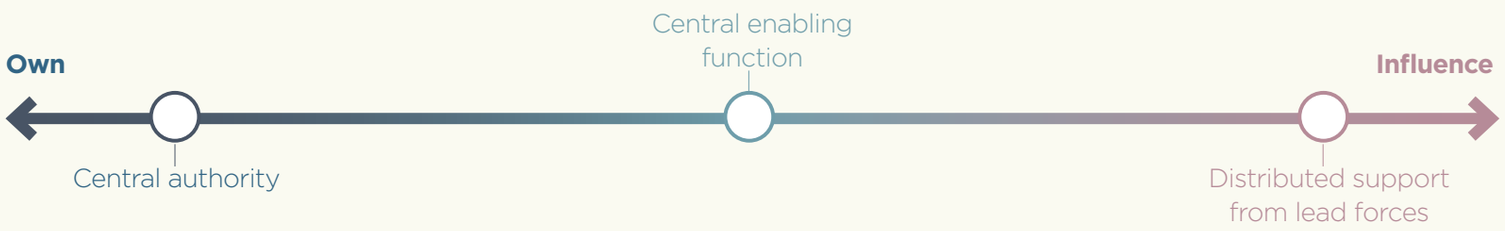
Delivery and Service Management: Supporting and/or managing provision of live services to ensure quality.

Business Change: Supporting integrated delivery of new technology, ways of working and culture change.

Impact Assessment and Compliance: Assessing the impact of digital change and ensuring compliance with laws, standards and ethical guidelines.

Innovation and R&D: Empowering industry and academia to develop and scale new approaches and solutions to support policing.

The level of influence and ownership that 'national governance' has on the how these capabilities are delivered:



Shutterstock/Flyby Photography

Call to action

We are rightly proud of our Policing Model, providing local responsiveness and strong accountability.

But in every sphere of policing a balance must be struck which respects local control whilst realising efficiency and effectiveness through appropriate national intervention. While the balance varies between policing functions, the need for smart investment in digital, data technology is strong and growing.

If we believe in a National Digital Strategy and recognise it as something that will continue to evolve, we must create the capability that will allow it to happen. If we do not change our approach our current risks and problems will be exacerbated by the evolving pressures and accelerating pace of change.

This is not, primarily, a debate about structure. Few are supportive of a national monolithic structure owning a fixed plan. But if we are open to coming together, and pooling our sovereignty in certain key areas, we will successfully achieve our digital ambitions.

As with so much in policing, navigating this compromise will require balance and judgement. The requirement is to adhere to standards, sign-up to a common plan, and in doing so accept that we will need to make choices on the ownership of decision-making across our service. The prize is the ability to deliver common solutions that transform the working practices of our workforce, and improve service outcomes for citizens. After all, the impact of getting this right will be in the hands of 123,000 officers and 65,000 staff who are committed to serving the public and protecting the vulnerable from harm.

END NOTES REFERENCES

1. 13 to 34 year olds spend an average of four and half hours a day online. “Online Nation 2019 Report – Ofcom” *(https://www.ofcom.org.uk/__data/assets/pdf_file/0025/149146/online-nation-report.pdf)*
2. 62% of citizens think increased use of technology by police, border agencies and government as a whole will make them more secure. ”What do Citizens want – Accenture Research, 2018”
3. 55%“of citizens agreed with the following statement: “[Police] will need to keep up and be able to stay one step ahead of the online criminals.” in response to the question “Over the next 10 years, technology trends will influence the types of crimes being committed (e.g. hacking of personal data, online financial fraud, online bullying etc.), as well as our communities and how we live. How do you think your expectations of the Police might change as a result?”. “Crowdsourced Citizen Research – Deloitte 2019”
4. “Big Data, for better or worse: 90% of world’s data generated over last two years – SINTEF” *(https://www.sciencedaily.com/releases/2013/05/130522085217.htm)*
5. “Data storage goes from $1M to 2 cents per gigabyte”, Computer World, 2017 (*https://www.computerworld.com/article/3182207/cw50-data-storage-goes-from-1m-to-2-cents-per-gigabyte.html*)
6. More than 90% of reported crime now has a digital element. Often this involves the police investigator retrieving evidence from digital devices and this includes social media, mobile phone applications and the Internet. “Internet Intelligence and Investigation (III Project) Full Business Case – Mayor’s Office for Policing and Crime” *(https://www.london.gov.uk/sites/default/files/pcd_525_part_1_internet_intelligence_and_investigation.pdf)*
7. For almost all types of organised crime, criminals are deploying and adapting technology with ever greater skill and to ever greater effect. The number of organised crime groups that are involved in more than one criminal activity (poly-criminal) has increased sharply over the last years (45% in 2017 compared to 33% in 2013). “Crime in the age of technology – Europol’s serious and organised crime threat assessment 2017”, *(https://www.europol.europa.eu/newsroom/news/crime-in-age-of-technology-%E2%80%93-europol%E2%80%99s-serious-and-organised-crime-threat-assessment-2017)*
8. The Home Office invested £600,000 in Project Arachnid, software that can be deployed across websites, forums, chat services and newsgroups to instantaneously detect illegal content. “Serious Violence Strategy – HM Government” *(https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/698009/serious-violence-strategy.pdf)*
9. “2017 Norton Cyber Security Insights Report – Symantec” *(https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-comparison-united-kingdom-en.pdf)*
10. “The Cost of Cyber Crime – Deltica & Cabinet Office” *(https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf)*
11. According to Jack Clark, Policy Director for OpenAI, much of the worries [OpenAI] have about the future of media relate to the increasing ease with which we’ll be able to cheaply create ‘fake’ rich media and use this to mount public opinion campaigns which could accentuate societal divisions, or cause political destabilization . “Written testimony of Jack Clark, OpenAI, for The National Security Challenges of Artificial Intelligence, Manipulated Media, and ‘Deep Fakes’ Hearing – House Permanent Select Committee on Intelligence ”, *(https://intelligence.house.gov/uploadedfiles/clark_deepfakes_sfr.pdf)*
12. “Police Funding for England and Wales 2015 to 2019”, July 2018, Home Office Statistical Bulletin
13. “ICT Market Sizing: Criminal Justice”, 2016-2019, GlobalData
14. PTF Investments Documentation, February 2019, Gov.uk

CLICK HERE TO RETURN TO ‘THE BIG PICTURE’