techUK
FOR WHAT COMES NEXT

techUK Policing Solutions Book

A techUK member response to the NPCC Policing Problem Book

October 2026

Contents

Foreword 04

Introduction 05

techUK Policing Solutions Book 06

1. How can we best improve our capture and analysis of digital evidence? 07

2. How can policing enhance public contact delivery through Strategic Digital Transformation? 25

3. How can policing enable secure, efficient, and standardised data sharing across forces? 36

4. How can policing efficiently assess and monitor a growing population of community-based offenders, especially high-risk individuals? 62

5. How can policing transform the investigation and prevention of online sexual offences, particularly child exploitation? 69

6. How can policing build and maintain public trust through fair, transparent, and accountable practices? 77

7. How can policing responsibly deploy surveillance technologies by ensuring timely activation, ethical use, and public trust through robust legal and privacy frameworks? 87

8. How can policing design out the opportunities for criminal activity emerging from synthetic content, connected vehicles, and smart technologies? 93

9. How can police enhance its capability to investigate and prevent cybercrime by developing specialist skills, tools, and partnerships to address threats such as malicious communications, dark web activity, and digital stalking? 97

10. How can policing develop a digitally empowered, data literate and innovative workforce to meet the demands of modern, intelligence-led policing? 101

11. How can policing protect its workforce and keep them safe whilst delivering an effective service to the public, now and in the future? 110

12. How can policing modernise mobility capabilities to ensure safe, efficient and future-ready operations across air, road, and connected vehicle environments? 117

13. How can policing embed innovation, evaluation, and strategic foresight into its culture and operations? 123

Conclusion 137

techUK's Justice and Emergency Services Programme 138

Foreword

Julian David OBE
CEO, techUK

The model for British Policing is respected around the globe and advances over the ages in the fields of Fingerprinting and DNA amongst others has continually altered the way the public safety role of policing has evolved.

With an estimated 9 out of 10 offences having a digital element, the landscape continues to demand advances in the technology at the fingertips of investigators and front-line staff.

The NPCC's Policing Problem Book sets out, with real clarity, the scale of the challenge now facing policing, and the areas where industry can make the greatest difference.

techUK's membership represents the breadth of the UK tech sector, from established suppliers with a long history of working alongside policing, to emerging innovators bringing new capabilities to some of these long-standing challenges. The techUK Policing Solutions Book has been developed to bring that capability together in one place, mapped directly against the problems policing has identified as its priorities.

The use of technology within policing and the wider criminal justice system will always need to be governed and measured, but it must advance at pace and not be subject to hindrance of the legacy debt that holds back effective and efficient deployment.

I want to thank all techUK members who have contributed solutions to this piece, and the wider Justice and Emergency Services programme team for their work in bringing it together. This is only the beginning: as technology and policing's needs continue to evolve, so too will this piece, and I look forward to seeing the partnerships it helps to build.

Introduction

In October 2025, the National Police Chiefs' Council (NPCC), together with the Office of the Police Chief Scientific Adviser (OPCSA) for Policing, published the Policing Problem Book. Developed through extensive consultation and review across the service, it sets out 13 underlying problems that drive structural inefficiencies and growing pressures on policing today. These range from the capture and analysis of digital evidence to cross force data sharing, and the responsible use of surveillance technology. Together, they represent policing's collectively identified priorities for the near and long term, and a clear signal of where the service is most willing to invest in research, innovation, and partnership.

Solving these problems will require more than incremental change within policing alone. Many of the challenges set out in the Problem Book sit at the intersection of operational need and technical capability. Industry has a critical role to play in bringing forward the tools, platforms, and expertise that can address these problems at scale, and in helping policing test, evaluate, and adopt innovation with confidence. techUK's membership, spanning established suppliers and emerging technology companies, is uniquely positioned to respond to this call and to work in partnership with policing to turn identified problems into practical, deployable solutions.

Building on the established partnership between NPCC and techUK, and in direct response to the Problem Book, we have developed the techUK Policing Solutions Book: a curated collection of member-led solutions mapped against each of the 13 problems identified by the NPCC. It gives policing a single, accessible resource that demonstrates the breadth of industry capability available, and accelerates the partnerships needed to bring these solutions into practical use.

techUK is committed to supporting this process from problem to solution. Through its Justice and Emergency Services programme, techUK has convened members, coordinated submissions, and worked closely with the NPCC to ensure the techUK Policing Solutions Book reflects both the urgency of the problems identified and the maturity of the solutions on offer.

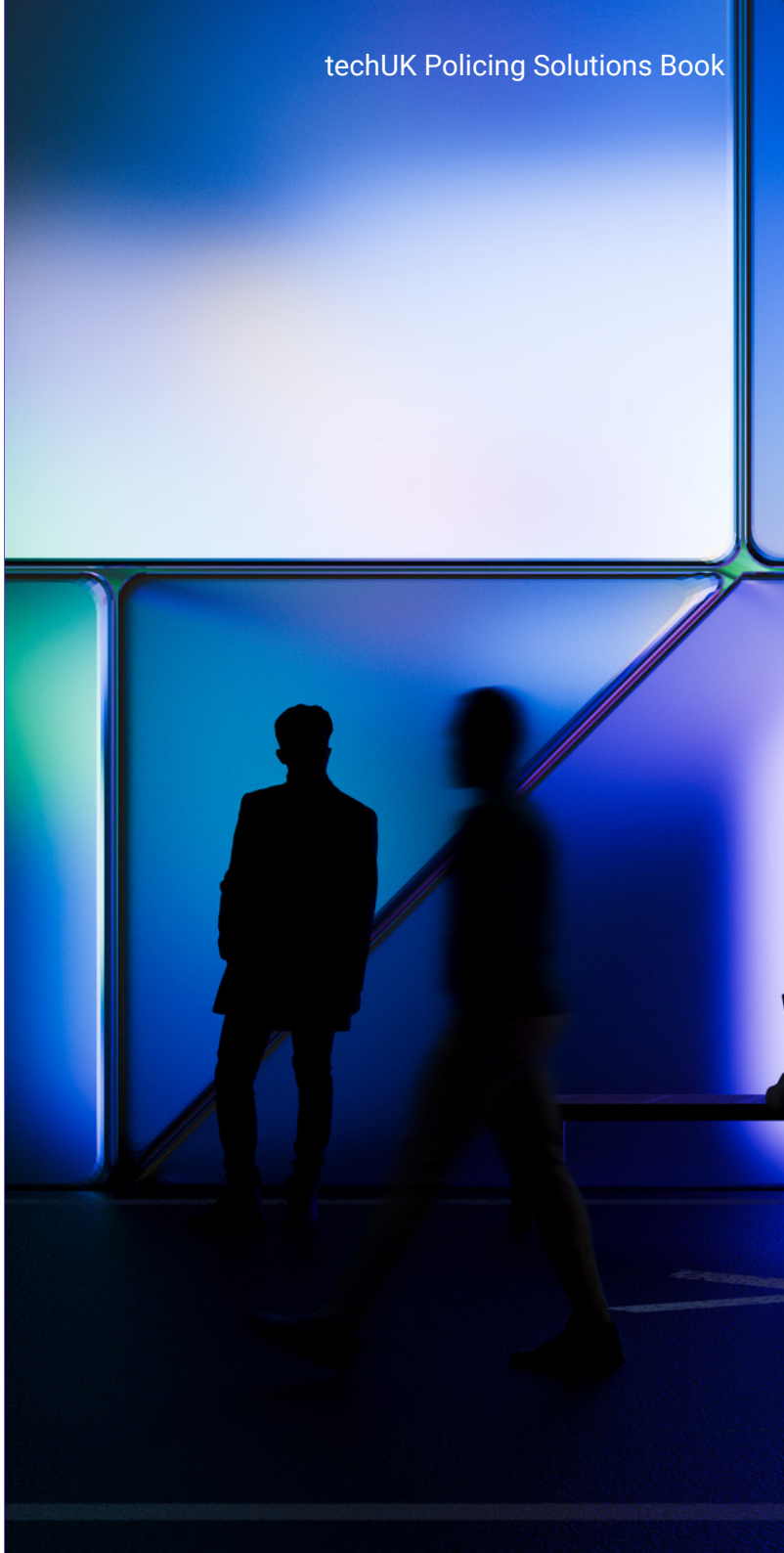
Launching at the NPCC Innovation and Digital Summit 2026, the techUK Policing Solutions Book marks a significant step in strengthening the relationship between industry and policing, and supporting the shared ambition of a more digitally enabled, data literate, and future ready service.

It should be noted that the inclusion of solutions within this resource does not constitute an endorsement, prioritisation, or recommendation by techUK of any specific product, service, or supplier. Rather, the resource is intended to showcase the breadth of capability that exists within techUK's membership, and to support informed conversations between policing and industry. Decisions on procurement, evaluation, and adoption remain entirely a matter for individual forces and policing bodies.

techUK Policing Solutions Book

The following pages set out each of the 13 problems identified in the NPCC Policing Problem Book. For every problem, we provide a short summary of the operational context, before showcasing the range of solutions put forward by techUK members in response. Solutions are presented in alphabetical order by organisation name.

It should be noted that the inclusion of solutions within this resource does not constitute an endorsement, prioritisation, or recommendation by techUK of any specific product, service, or supplier. Rather, the resource is intended to showcase the breadth of capability that exists within techUK's membership, and to support informed conversations between policing and industry. Decisions on procurement, evaluation, and adoption remain entirely a matter for individual forces and policing bodies.



1. How can we best improve our capture and analysis of digital evidence?

Digital evidence now underpins the vast majority of investigations, but manual handling of CCTV, mobile, and cloud data has been driving backlogs and leaving victims without their devices for extended periods. In response, techUK members have brought forward solutions that automate processing, standardise formats across all 48 forces, and enable secure, petabyte-scale cloud storage and analysis, while bridging legacy and modern forensic tools.

Primary Service Lines: *Identification & Tracing, Analytics*

Augur exists to protect people where they live, work, travel and gather.

The threat to public safety is growing faster than existing security services can respond. There is strong mission alignment between Augur and UK Policing; we have prioritised three Problem Book statements where Augur can have immediate, tangible impact:

Augur allows investigators to search vast volumes of footage in hours rather than weeks — reconstructing the movements, actions and interactions relevant to an incident, surfacing what matters. Augur also enables rapid packaging and export of footage from legacy VMS standard to evidentiary standards.

To find out more, visit our website or contact us.

BlackRainbow was founded by SMEs who recognised key challenges in the investigation industry and the limitations of supporting technology. We developed NIMBUS, a versatile and scalable platform built around three core pillars: Intelligence, Investigations and Forensics to streamline the entire case management lifecycle, improving efficiency, accuracy, auditability and compliance to standards and procedures. Designed for Law Enforcement, Government and Corporates, it delivers complete visibility and control through intelligence-led data, evidence tracking, automated workflows, decision making, tasking and reporting.

Already operational across UK policing, NIMBUS has unified case and quality management, reducing risk, improving interoperability, lowering manual workloads, and enhancing efficiency, cost effectiveness and staff wellbeing. Our solution addresses several problem questions, including how best to improve our capture and analysis of digital evidence.

You can find out more through our case study, or contact us.

As the Problem Book explains, digital evidence now plays a role in around 90% of investigations. Its growing volume and complexity—including body-worn video, CCTV, audio, mobile-device material—is creating backlogs, increasing manual workloads and delaying justice. Victims may also be traumatised by delays or by being separated from their devices.

A more effective approach would help forces capture, preserve, analyse and share evidence consistently, while improving outcomes for victims, officers and partner agencies. It should reduce duplication across fragmented systems, support evidential integrity and make relevant information available securely when needed.

With UK policing references, Box can support these outcomes through a secure, scalable content layer that works across existing policing applications and tools. It can help forces gather and organise evidence and case material, automate routine handling and improve collaboration between investigators, prosecutors, courts and partner agencies. AI-assisted summarisation extracts information and metadata, to help teams find and understand content more easily, while permissions, classification and audit trails support accountable handling.

The victim and witness experience can be improved through using the same Box foundation to submit statements and supporting evidence remotely, reducing officer travel and administration. This approach can be particularly valuable in sensitive cases such as domestic abuse, where a visit to a victim's home could create anxiety or reluctance to engage. Using Box, PSNI leverages a digital evidence submission portal and electronic statement experience, saving money, improving efficiency and optimising the victim journey.

Technology investment in policing has to deliver savings, and Box also offers proven line-of-business value, including, Communications, Legal, HR and Finance work. Rather than operating as a standalone DEMS, Box's broad integration and open API approach can help address interoperability challenges.

Crucially, Box's unlimited-storage model mean forces are not exposed to additional costs, even as the amount of digital evidence retained increases.

To find out more, visit our website or contact us.

Digital evidence now features in the vast majority of investigations, yet the challenge facing policing is no longer simply capturing information. The real issue is the volume of material that must be reviewed, assessed, shared and understood before it can contribute to an investigation. For victims, it can mean delays in justice and extended periods without access to personal devices while evidence is processed. BT believes this challenge is ultimately about helping investigators spend less time managing digital evidence and more time progressing investigations. Combined with specialist partners in digital evidence management and analytics, there is a significant opportunity to help policing move from evidence collection to evidence insight more quickly while maintaining trust in the evidence process.

To find out more, visit our website or contact us.

Over 90% of reported offences now feature a digital component, yet un-triaged hardware overloads Subject Matter Experts (SMEs) while disconnected systems silo intelligence. Butterfly Data delivers bespoke engineering and analytics to reduce forensic backlogs and connect isolated platforms. As a SAS Gold Partner, we pair tailored engineering with enterprise software—including SAS Law Enforcement Intelligence - to address NPCC Policing Problem Book Statements 1:

We build custom AI pipelines for automated text extraction and computer vision, flagging incriminating artifacts during intake. This reduces manual hours and eases SME pressure while maintaining human-in-the-loop oversight. We have applied similar generative AI for synthetic face data testing.

We implement automated ingestion scripts to categorise and route evidence without manual intervention, and deploy force-wide analytics to cross-reference identifiers and signatures across cases.
By combining bespoke integration with enterprise analytics, we turn raw data into actionable intelligence, closing the gap between disconnected systems.

To find out more, visit our website, or contact us.

Cellebrite

Digital evidence now features in around 90% of investigations, yet many investigative processes remain organised around devices, specialist units and disconnected systems. Critical evidence often moves through multiple teams, systems and queues before reaching investigators, creating delays, prolonging the retention of victims' devices and consuming valuable specialist resources on routine tasks. As digital evidence volumes continue to increase, simply adding more capacity is unlikely to solve the problem. Policing needs a more effective operating model that delivers relevant evidence faster while preserving evidential integrity and professional oversight.

A scalable approach should be built on three principles:
Automate the routine. High-volume, repetitive tasks such as evidence tracking, duplicate detection, known-hash matching, transcription, translation and initial screening should be automated where reliable and appropriate.

Escalate the complex. Activities requiring specialist expertise, including advanced forensic recovery, analysis of deleted or concealed data and technical interpretation, should be directed to qualified practitioners. This ensures scarce forensic resources remain focused on work where specialist knowledge and experience provide the greatest value.

Preserve human judgement. AI and automation can search, classify and prioritise information, but responsibility for decisions affecting safeguarding, disclosure, evidential value and justice must remain with investigators. Human review, accountability and transparent decision-making are essential.

Digital investigations are challenged not only by data volume but also by cognitive overload. Investigators and forensic practitioners often spend significant time moving between systems, reconstructing timelines and connecting disparate evidence sources. This increases workload and raises the risk of important insights being missed.

Cellebrite supports a connected approach by bringing evidence, review activity and case context together in a single environment. By reducing fragmentation and automating routine processes, investigators can focus on analysis, decision-making and victim outcomes. The result is a faster, more scalable investigative model that helps return victims' devices sooner and enables policing to keep pace with the growing role of digital evidence.

To find out more, visit our website or contact us.

CIS enables all evidence (CDR's); Handset Extractions; ANPR; CCTV; Financial and more related to a crime is loaded into an individual case for analysis. You can view our case study with North Wales Police here.

The Federated search capability of CIS, enrichment of data by searching through old cases and hundreds of social media platforms to get a comprehensive overview of an individual's activity. You can view our case study with Merseyside Police here.

Additional insight can be added to the case using the built-in Secure Open-Source Capture capability, capturing a whole webpage, snipped, image or video.

To find out more, visit our website or contact us.

Cloud Gateway operates the connectivity and security layer that modern policing runs on. Our secure connectivity platform brings network, security and observability into one operating model, delivered by one UK team on sovereign infrastructure built for the assurance standards specific to policing.

Urgent reform, tightening regulation and emergent technology are not arriving as separate problems that need solving one at a time. They are converging on the same policing infrastructure at once. Our platform is architected at that intersection: an experience plane for governed operations, a connectivity and security fabric that consolidates disparate tooling, an intelligence layer for unified observability, and an assurance foundation built on accreditation and evidence. It is the digital foundation policing needs to operate securely, modernise and stay compliant.

Interoperability, named as a design requirement in the NPCC Problem Book and the Hogan-Howe review, only becomes real when common patterns for data exchange, identity, access and audit sit underneath. Without that foundation, new capabilities, including those that are truly transformative, have to be rebuilt force by force. With it, what works in one force can travel to the next. This is what our platform provides.

Most forces start with one problem and extend from there:

- Evidencing compliance as a continuous, provable state rather than a pre-audit scramble
- A stronger security posture with consistent policy enforced across every user, site and connection
- Modernisation of legacy estates
- Connectivity to government networks, partners and sector peers
- AI-ready infrastructure to support increased data volumes and cloud workloads

For Avon and Somerset Police we migrated 64 WAN sites to direct cloud and PSN access, removing central backhaul and laying the foundation for cloud, AI tooling and data-sharing across forces. Read the case study.

To find out more, visit our website or contact us.

CLOUDFLARE

Digital evidence should be treated as a seamless national data flow, not a sequence of local hand-offs. Policing needs a trusted route from capture to judicial review, with common metadata, interfaces and assurance controls across all 48 forces.
At ingestion, every item should receive a unique identifier, source details, timestamps and a cryptographic fingerprint. Automated checks can verify integrity, identify duplicates and route material to the appropriate accredited tool. Cloudflare AI Search provides automated indexing, metadata filtering and combined semantic and keyword search, allowing investigators to ask natural language questions and retrieve relevant material without knowing an exact phrase. Sensitive applications can be unavailable by default and opened only when identity, device posture and other policy requirements are satisfied. Cloudflare's reference architecture for designing Zero Trust access policies explains how identity, device context, strong authentication and reusable policy groups can protect sensitive applications.

This platform would complement, not replace, accredited forensic tools and policing's evidential policies.

To find out more, visit our website or contact us.

CSL

Always-on in-field connectivity for frontline policing

Away from a fixed connection, body-worn video, mobile ANPR and covert cameras may depend on a cellular path to move evidence into force systems. If that path cannot carry data, a device may continue operating locally, but information intended for transmission cannot reach force systems over that path. In-field connectivity is therefore a dependency for the mobility capabilities in this chapter.

Where cellular data depends on one mobile network core, a core fault can interrupt the path even while the device remains registered and reports a usable radio signal. Signal-strength-only failover will not respond to that condition.

Exclusive to CSL, rSIM® is designed to support in-field connectivity by addressing that exposure. It holds two operator profiles on one SIM, each reaching multiple radio networks through a separate mobile network core. rSIM monitors whether data is passing from the device. If data stops for a sustained period, it can initiate a switch to the second profile without depending on the affected network to issue an instruction.

Conventional multi-network connectivity can reach alternative radio networks through one core. CSL's patented rSIM architecture adds SIM-resident failover between separate mobile network cores. Designed in the UK and launched in 2024, rSIM is used across telecare, fire and security, healthcare and payments.

CSL supports more than 3.5 million active connections and private VPN connectivity to more than 270 alarm receiving centres across Europe. This private APN and encrypted VPN architecture could support PNC queries, ANPR data and body-worn video, subject to each force's technical, security and assurance requirements.

To find out more, visit our website or contact us.

As the 2026 Police Reform White Paper states, police performance has declined in recent years, and criminals are outpacing the police in leveraging technology.

If UK policing wishes to improve in these areas, it must move beyond its current fragmented data foundations. This was evidenced in the Policing Insight and techUK Workforce Survey (2026), in which only 16% of 8,000 officers and staff reported that their force systems are well integrated. This was stated in the aforementioned White Paper:

...designing solutions separately several times over, leading to unnecessary spending. This locks away useful data and restricts our ability to make informed decisions at a national level. We are not getting the right information into the right hands at the right time. Compounding this landscape is the fact that digital evidence now features in approximately 90% of all investigations. The volume, variety, and complexity of such material place a burden on officers and analysts who still rely on manual processes to secure, transfer, and analyse evidence.

What is required is a Unified Intelligence Future. The Future is not one technology; it is an Open Standards Ecosystem that provides freedom from vendor lock-in. This future will unlock the full power of police data without rebuilding core systems or creating new data silos. The Databricks Platform provides such a future. Our unified data lakehouse architecture brings together structured records from crime and intelligence systems, as well as petabyte-scale digital evidence, enabling the police to adopt the AI and analytics capabilities they need to deliver real-time decision-making.

To find out more, visit our website or contact us.

Dell Technologies sets out how they believe law-enforcement organisations can manage, analyse and retain digital evidence. The paper recognises evidence is now coming from multiple sources including computers, phones, CCTV, body-worn cameras, drones, vehicles, social media and emergency call systems. The volume of data stored is increasing, and systems are often split across applications, teams and locations creating silos of storage.

Dell Technologies' proposed approach is to consolidate processes together to a central platform. This covers data collection during an incident, data ingestion and analysis, reporting, sharing with others and secure archiving. The document makes it clear that chain of

custody, audit trails, access controls and compliance are essential. The original evidence must remain protected and traceable. The paper also discusses how to keep older evidence accessible as systems and devices become obsolete, which is becoming more common due to evidence retention policies. It is recognised the platform needs to scale as storage and processing requirements grow, and support on-premise, cloud, hybrid or air-gapped environments.

Dell Technologies' provides the underlying infrastructure and services, rather than a single application. This includes PowerEdge servers, PowerScale, PowerStore, ECS, networking, security, automation, analytics and partner software. AI and machine learning can help with tagging, searching, pattern recognition and prioritising useful information, but source files and provenance must be preserved. Overall, the message is straightforward: a unified and secure platform should reduce duplication, make investigations easier to manage, and support the journey from incident through to court and long-term archive.

To find out more, visit our website or contact us.

Real-Time Situational Awareness for Officer Safety helps protect officers and improve operational decision-making by giving command centres real-time visibility of frontline risks, welfare concerns, and emerging incidents. It replaces fragmented radio updates and delayed reporting with continuous, actionable intelligence.

Using approved wearables and mobile devices, the platform provides real-time officer safety and welfare monitoring, location awareness, and automatic detection of distress events. It can identify falls, panic activations, weapon deployment, and signs of escalating situations. Sensitive data is processed securely on the device, ensuring only relevant insights are shared with supervisors and control rooms. This enables faster intervention, intelligent deployment, and improved coordination of personnel and assets. SITREP AI maintains resilient communications when conventional networks fail through a mesh network operating across cellular, Wi-Fi, and satellite networks. This ensures a persistent operational picture during major incidents, public events, rural deployments, and in areas with poor signal coverage The platform also identifies patterns associated with escalating risk, helping supervisors prioritise alerts, allocate resources effectively, and make informed decisions in rapidly changing operational environments. As adoption matures, SITREP AI evolves from delivering situational awareness to providing operational insight and decision support, helping forces move from reacting to incidents to anticipating operational risk.

To find out more, visit our website or contact us.

AEGIS is Frazer-Nash Consultancy's Counter-Uncrewed Aerial Systems (C-UAS) intelligence and decision-support capability. Developed with operational stakeholders, AEGIS helps users identify, prioritise and investigate suspicious activity from large volumes of drone information using behavioural analytics, risk-ranking and geospatial analysis.

Whilst originally developed for C-UAS operations, AEGIS demonstrates a broader approach to helping analysts extract insight from large and complex datasets whilst reducing the burden of manual review. By applying configurable behavioural indicators and historical analysis techniques, the platform helps users identify activity that may warrant further investigation and focus attention where it is most needed. During pilot activity, AEGIS demonstrated the potential to reduce drone investigation effort by up to 90%, allowing analysts to spend more time interpreting information and developing intelligence.

AEGIS is designed to support human judgement rather than replace it. Its analytics are transparent and configurable, allowing behavioural indicators and risk criteria to be adapted to different operational contexts whilst maintaining user trust in the underlying assessment.

As a secure cloud-hosted application, AEGIS provides a standalone intelligence and decision-support capability. Equally, AEGIS can act as a service into larger enterprise environments, enabling information from multiple sources to be assessed through a consistent analytical lens without constraining future technology choices.

Developed through iterative engagement with operational users, AEGIS demonstrates how new capabilities can be matured through experimentation and evidence-led delivery.

To find out more, visit our website or contact us.

One area of IBM is focused on bringing data together from multiple sources whether its legacy hybrid or cloud so that insight can be captured without moving the data to another area .

This could be hugely successful in policing .

IBM's approach connects to data in place rather than requiring migration into a single central store, satisfying legal data protection boundaries while enforcing consistent governance.

Domestic abuse, vulnerability and safeguarding cases are complex because the picture of risk is scattered across command and control, records management, intelligence, safeguarding and partner-agency systems that were never designed to talk to each other.

Connecting these types of existing estates rather than replacing them - using federated query capability to pull a live, unified view of an individual, address or order across multiple sources without copying or migrating data. For example an officer preparing a Protective Order file, or a team checking compliance, can see the full evidential and offending history the moment it's needed, drawn directly from source-of-truth systems. Underpinning this is a trusted-data layer: automated quality, matching and enrichment so records relating to the same victim, offender or incident are reliably linked, reducing missed connections. Data lineage ensures every piece of information feeding a risk assessment or court-bound case file can be traced back to its origin, supporting evidential auditability. A shared data catalogue and semantic layer also let disparate force data models be reconciled consistently, so risk indicators mean the same thing wherever they're captured.

To find out more, visit our website or contact us.

MAGNET FORENSICS®

Many of the most pressing challenges facing law enforcement today are connected by a common reality: digital evidence now underpins most investigations.

Magnet Forensics helps police forces modernise the full digital investigation lifecycle. Its digital forensics solutions support the lawful acquisition, processing, analysis, review and sharing of evidence from mobile devices, computers, cloud services, vehicles, video and other digital sources.

Magnet Graykey allows investigators to gain lawful access to mobile devices, while Magnet Axiom enables the recovery and analysis of evidence from various digital sources. Magnet Automate reduces manual work and standardises evidence processing. Together, these solutions help agencies reduce investigative backlogs and accelerate access to critical information.

With digital evidence becoming increasingly prone to alteration, Magnet Verify can help confirm the authenticity of files by examining the digital structure to determine whether they have been changed.

Across these workflows, trusted AI and automation help teams surface relevant evidence, recognise connections and focus specialist time where it can have the greatest impact.

By connecting people, processes, and technology, Magnet Forensics helps address key policing challenges related to digital evidence, shortening the path from evidence to action, and delivering more efficient, transparent, and trusted outcomes for victims, communities, and the justice system.

To find out more, visit our website or contact us.

NiCE

Question 1 raises three pain points: manual processing driving backlogs, victims left without devices, and 43 forces needing one consistent approach without discarding legacy systems. NiCE Evidencentral answers all three from a single platform.

It automatically pulls evidence from BWC vendors, RMS, CAD and CCTV into one case environment, cutting manual work: Hampshire Constabulary credits it with letting them “automatically connect all our digital evidence,” saving a projected £846,000 in officer time annually.

NiCE Evidencentral's Community Portal also lets citizens submit photos, video and CCTV directly, removing the need to seize victims' devices, as Cheshire Constabulary confirms. Running on Microsoft Azure, Evidencentral integrates with forces' existing tools rather than replacing them, now managing over 240 million evidence items across 26 UK forces and organisations, with Lancashire Constabulary cutting CPS turnaround from days to under an hour.

To find out more, visit our website or contact us.

OPSWAT.

The Policing Problem Book identifies digital evidence capture and analysis (Problem 1), Digital Public Contact transformation (Problem 2), and secure data sharing across forces (Problem 3) as central challenges. Underlying all three is one question: as forces digitise contact, evidence and case management, who checks that every file entering the estate can be trusted?

MetaDefender is built on a zero trust principle. A firewall or VPN controls who can reach a system, but says nothing about whether the file they bring is safe. Encryption does not solve this either: an encrypted attachment or upload can still carry malware, since encryption protects a file in transit, not its content.

MetaDefender inspects, sanitises and rebuilds files at every point they cross into policing environments: crime reporting portals, email attachments, and USB, CCTV and bodycam footage collected in the field or moved between forces and to the CPS. Deep CDR and multiscanning remove hidden threats while preserving evidential integrity and chain of custody.

An "ingest once, share with many" approach means evidence is checked once, then moved across systems with a full audit trail, cutting manual triage and supporting the standardisation the Problem Book calls for.

UK police forces already run OPSWAT in live operation, on file upload portals, email gateways and frontline evidence handling.

To find out more, visit our website or contact us.

OXFORD DYNAMICS

At Oxford Dynamics, we've spent years building deep tech for environments where a wrong decision is a mission failure. That discipline is where the most credible progress in policing will be made in digital forensics, and increasingly resource allocation.
A concept worth borrowing is the "kill chain": the sequence defence uses to identify, track and act on a target. Law Enforcement has its own version: a "criminal justice chain" running from report, through investigation, to trial and successful prosecution. The Problem Book isn't thirteen isolated challenges, it's weak links in one chain.

Digital evidence plays a role in nine in ten investigations, and the NPCC's Problem Book names this Prob1. Triaging CSE imagery (Prob5), deepfake detection (Prob8), and dark web crime (Prob9) share the same constraint: too much data, too few resources and too little time.

AVIS™ and R71 help here. R71, used on the UK's Strategic Defence Review, retrieves and reports on petabyte-scale evidence at speed. AVIS is the reasoning layer above it: a multi-agent architecture where each stage is traceable, so an investigator sees why something was flagged.

Resource allocation is a different link, underneath several problems: prioritising high-risk offender visits (Prob4), call handling demand (Prob2), workforce deployment (Prob11), and coordinating air, road and surveillance assets (Prob12). The weakness here is orchestration, with ORION's role routing AVIS's prioritisation intelligence into deployable decisions.

Policing needs an intelligence layer that reasons transparently, and an orchestration layer so that Police Reform can ensure the integrity of the criminal justice chain.

To find out more, visit our website or contact us.

Peregrine

Peregrine is a data integration and intelligence platform used by more than 450 public safety organisations. It integrates any source of data a force holds or receives into a single, permission-controlled operational layer, without replacing existing systems. The premise is straightforward: most of the intelligence forces need already exists within their estates, but it is fragmented. The constraint is not data collection, it is integration and access.

Once integrated, all connected data becomes searchable through one interface designed for frontline use rather than specialist analysts. The evidence suggests adoption follows accessibility: Concord Police Department connected 19 data sources in 28 days.

To find out more, visit our website or contact us.

Digital evidence is fundamental to modern policing, but growing volumes create bottlenecks that can slow investigations.

Problem statement 1 of the Police Problem Book asks how policing can improve the capture and analysis of digital evidence. The challenge is increasingly what happens next. Growing volumes must be reviewed to find what matters, while manual processes create bottlenecks, backlogs and organisational risk. Pimloc uses AI-assisted investigative search to help investigators search across multiple media files and identify relevant people, objects and information in minutes, not hours.

To find out more, visit our website or contact us.

Synthetic data reproduces the structure, patterns and relationships found in real police data but includes no sensitive or personal information

Principle One brings synthetic data to life by applying it to real-world operational scenarios. Our outputs include communications data, ANPR, digital forensic material, financial data, crime reports or intelligence records

Why it's necessary | Police data is highly sensitive and often difficult to access for research, development and testing. Using live operational data creates privacy, access and governance risks.

Principle One's synthetic data creates a safe, controllable alternative. It allows realistic datasets to be generated without exposing victims, witnesses or officers, while still maintaining the complexity, links and imperfections of real operational information

What it enables | Synthetic data enables development and vigorous testing of new and emerging policing technologies. It can be used to expose knowledge gaps, software issues and improve functionality. It can also be used to gamify investigative scenarios to make training environments more immersive, and to build 'digital twins' of systems or organisations to develop AI
The benefits | Synthetic data makes innovation easier, safer and faster. It allows police forces and suppliers to develop, test and train using realistic data without exposing personal information. It can be generated at scale, reused consistently and tailored to include complex or rare scenarios that may be missing from live datasets. It also supports safer collaboration, better training and helps tools and approaches to be tested before they are introduced operationally.

To find out more, visit our website or contact us.

ROKE

Roke delivers digital evidence ecosystems combining automated capture, AI analysis and scalable cloud. Drawing on national security experience of managing petabyte-sized stores, our solutions reduce effort and accelerate investigations by using data fabrics, lakehouses and federated integration to enable operational impact across forces.

To find out more, visit our website or contact us.

---

trustmarque ultima

If public confidence remains a key measures of success, improving digital evidence capture and analysis must deliver a better service to the public and victims.

A mobile phone is someone's lifeline. When a victim's phone is taken, it adds further disruption at an already difficult time and potentially affects confidence in the investigation.

Policing should therefore explore greater use of remote, selective and targeted acquisition. The objective should not be to collect everything simply because the technology allows it, but to identify reasonable lines of enquiry and obtain relevant material in a way that is lawful, strictly necessary and proportionate. Wherever possible, this should reduce the time a victim is without their device. Investigators need greater digital confidence, clear submission criteria and the ability to identify relevant evidence quickly, allowing

specialists to concentrate on complex work. Progress should be measured through victim experience, turnaround times, backlog reduction, evidential quality and investigative outcomes - not simply the number of devices processed.

To find out more, visit our website or contact us.

---

whitespace

Policing is generating and handling ever-growing volumes of digital evidence. The challenge isn't simply capturing more information, but helping officers and investigators review, understand and use that evidence effectively while reducing manual effort and maintaining strong governance, assurance and evidential integrity.

Whitespace helps policing organisations turn operational challenges into trusted, governed AI capability. Rather than offering a one-size-fits-all product, we work alongside operational teams to understand where friction exists, define the outcome, and rapidly design, develop and test AI capabilities around that need.

We're already working with Microsoft and a large UK Police force to co-design an AI capability supporting the secure processing of taped and video interviews. The capability is designed to support translation, transcription, summarisation and structured outputs, helping reduce processing pressure while maintaining human oversight, accuracy and operational trust.

This work demonstrates our broader approach to digital evidence. Depending on the operational need, this could include capabilities that support evidence review, information access, workflow support and earlier operational assurance.

Our approach combines Solutions Engineering with Collective, our sovereign AI operating system, providing a secure and governed foundation for developing operational AI capabilities while retaining organisational control over data, deployment and AI.

The aim is not to replace investigators or automate policing. It's to help forces apply AI responsibly to validated operational problems, improve the speed and consistency of evidence handling, reduce unnecessary administrative burden and strengthen assurance.

To find out more, visit our website or contact us.

2. How can policing enhance public contact delivery through Strategic Digital Transformation?

The Single Online Home platform and related digital contact channels have transformed public interaction with police, but the underlying technology is ageing and costly as call and contact volumes rise.

The following solutions demonstrate how techUK members are unifying emergency and non-emergency channels, improving call-handling efficiency, and strengthening public trust through better digital contact experiences.

Primary Service Lines: *Interconnectivity, Analytics*

Public expectations of policing are increasingly shaped by experiences in the wider digital world. The challenge is not simply handling greater demand, but ensuring people receive the right support, through the right channel, at the right time. Strategic digital transformation should not be viewed as a destination in itself, nor as a means of replacing human interaction. From BT's perspective, effective public contact is about more than channel shift or service efficiency. It is about helping people access support at moments when they may be vulnerable, distressed or seeking reassurance. The opportunity for policing is to create simpler, more connected experiences that improve public confidence while allowing officers and staff to focus more of their time where it adds greatest value.

To find out more, visit our website or contact us

Contact with policing keeps rising across 999, 101, email and social media, yet the public still faces dozens of different routes into policing depending on where they live and what they need. Around 20% of calls to police are for non-police matters, and 40% of 101 traffic is people chasing an update on a report already made. Today, no single national entry point exists to resolve this demand, unify every contact channel, or give the public confidence that reporting is safe and reliable.

We answer this from direct experience. As the platform's delivery partner since inception, we have grown Single Online Home from one online form for Greater London into a national service reaching 94% of the population of England and Wales. We re-architected it for national multi-tenancy while it stayed live in production, migrated it to Azure, and deployed Cloudflare Zero Trust, delivering 100% uptime for three years against a 99.9% service level agreement.

That same platform already answers all three questions. AI-enabled triage and directive AI resolve and redirect the demand that does not need a person, freeing control room staff for the calls that do. iHub, the Citizen Portal and the National My Police Portal carry every report into force back-office systems once, whichever channel it came through. Every report is captured to a standard that is legally admissible from the moment it is submitted, with an audit log that can pass directly to the Crown Prosecution Service.

To find out more, visit our website, or contact us.

CIVICA

Six of the NPCC's 13 identified problems — spanning public contact, cross-force data sharing, offender monitoring, online child sexual exploitation, workforce protection, and innovation/strategic foresight — share a common structural cause: fragmented, unreconciled data about the same people, places, cases and equipment held across 48 independent systems.

The case made here is not that Master Data Management (MDM) solves policing's 13 problems. It is that six of them are, in part, the same problem — and that solving it once, doing it well, is worth significantly more than solving it 48 times separately.

A modern MDM platform does not solve every dimension of these problems on its own, however, MDM addresses the shared root cause running underneath most of them: the inability to reliably tell that a record in one system and a record in another refer to the same real-world person, case or thing.

For further descriptions of the value from MDM to Problem Statement 2, visit our dedicated page or contact us.

CLOUD GATEWAY

Cloud Gateway operates the connectivity and security layer that modern policing runs on. Our secure connectivity platform brings network, security and observability into one operating model, delivered by one UK team on sovereign infrastructure built for the assurance standards specific to policing.

Urgent reform, tightening regulation and emergent technology are not arriving as separate problems that need solving one at a time. They are converging on the same policing infrastructure at once. Our platform is architected at that intersection: an experience plane for governed operations, a connectivity and security fabric that consolidates disparate tooling, an intelligence layer for unified observability, and an assurance foundation built on accreditation and evidence. It is the digital foundation policing needs to operate securely, modernise and stay compliant.

Interoperability, named as a design requirement in the NPCC Problem Book and the Hogan-Howe review, only becomes real when common patterns for data exchange, identity, access and audit sit underneath. Without that foundation, new capabilities, including those that are truly transformative, have to be rebuilt force by force. With it, what works in one force can travel to the next. This is what our platform provides.

Most forces start with one problem and extend from there:

- Evidencing compliance as a continuous, provable state rather than a pre-audit scramble
- A stronger security posture with consistent policy enforced across every user, site and connection
- Modernisation of legacy estates
- Connectivity to government networks, partners and sector peers
- AI-ready infrastructure to support increased data volumes and cloud workloads

For Avon and Somerset Police we migrated 64 WAN sites to direct cloud and PSN access, removing central backhaul and laying the foundation for cloud, AI tooling and data-sharing across forces. Read the case study.

To find out more, visit our website or contact us.

Dataminr

Dataminr's AI platform continuously scans over 1 million public data sources in real time, using Multi-Modal Fusion AI, generative AI, and agentic AI to detect physical and cyber events, threats, and risks as they unfold. This real-time intelligence layer underpins both strategic digital transformation of public contact, adds stronger protection for the workforce delivering it and builds public trust. First Alert and Dataminr for Cyber Defence are cloud-based SaaS services delivered on a subscription model that integrates into clients' existing workflows rather than requiring new on-premise infrastructure. This means data is hosted, structured, and secured within established cloud architecture, with capacity and access managed centrally rather than left to fragmented local systems.

Strategic digital transformation for public contact: Dataminr replaces slow, manual monitoring of incoming information with an efficient 24/7/365 automated, AI-corroborated alerting. This capability provides control rooms, contact centres and intelligence teams with early context on public safety incidents and emergencies so forces can better respond before and after arriving on scene.

Building public trust through fair, transparent, accountable practices: Dataminr's public-data-only input limits exposure on data protection and privacy grounds; the system does not require access to classified or citizen personal data mitigating need for surveillance authorities. It validates every alert through a multi-layered approach that automatically corroborates patterns across multiple sources and modalities before an alert is issued, rather than relying on a single subjective source. The system surfaces alerts for human responders — it does not take autonomous action.

To find out more, visit our website or contact us

Frequentis can help policing enhance public contact delivery through Strategic Digital Transformation. Policing is under growing pressure to improve public contact while managing rising demand, increasing operational complexity and evolving citizen expectations. Modern communities expect seamless engagement through voice, webchat, messaging, video and other digital channels, yet many police control rooms still rely on disconnected systems for contact handling, dispatch, communications and incident management. This fragmentation increases cognitive load, slows decision-making and can impact service quality.

Frequentis supports strategic digital transformation by providing an integrated CR environment bringing together emergency and non-emergency contact, communications, dispatch, incident management, situational awareness and analytics within a single operational ecosystem. Rather than forcing forces into disruptive system replacements, Frequentis adopts an open, modular architecture that enables gradual modernisation while protecting existing investments and reducing delivery risk.

For policing, this means a unified public contact platform where information from voice calls, text, video, digital channels and operational systems is presented in context, supporting faster assessment, improved triage and more effective deployment decisions. Automated workflows, role-based interfaces and integrated data sources help reduce operator workload, eliminate duplicate data entry and provide a common operational picture across teams and partner agencies.

To find out more, visit our website or contact us.

One area of IBM is focused on bringing data together from multiple sources whether its legacy hybrid or cloud so that insight can be captured without moving the data to another area .

This could be hugely successful in policing .

IBM’s approach connects to data in place rather than requiring migration into a single central store, satisfying legal data protection boundaries while enforcing consistent governance.

Domestic abuse, vulnerability and safeguarding cases are complex because the picture of risk is scattered across command and control, records management, intelligence, safeguarding and partner-agency systems that were never designed to talk to each other.

Connecting these types of existing estates rather than replacing them - using federated query capability to pull a live, unified view of an individual, address or order across multiple sources without copying or migrating data. For example an officer preparing a Protective Order file, or a team checking compliance, can see the full evidential and offending history the moment it's needed, drawn directly from source-of-truth systems. Underpinning this is a trusted-data layer: automated quality, matching and enrichment so records relating to the same victim, offender or incident are reliably linked, reducing missed connections. Data lineage ensures every piece of information feeding a risk assessment or court-bound case file can be traced back to its origin, supporting evidential auditability. A shared data catalogue and semantic layer also let disparate force data models be reconciled consistently, so risk indicators mean the same thing wherever they're captured.

To find out more, visit our website or contact us.

---

innov8law

Public-sector organisations already hold many of the warning signals of tomorrow's failures: complaints, incidents, claims, misconduct, workforce pressures, financial losses, poor outcomes and declining public trust. Too often, those signals are considered separately.

innov8law Haemostasis™ is a cross-government methodology designed to help leaders connect those signals, identify where organisational harm is developing, quantify its human, social and economic impact, diagnose root causes and intervene before harm and cost escalate.

The methodology follows six stages: Target → Structure → Quantify → Diagnose → Intervene → Make the Case.

Its configurable Haemostasis Scorecard™ provides an early-warning and decision-support architecture through which different public services can select relevant indicators while retaining a common framework based on Human Value, Social Value and Economic Value.

For policing, Haemostasis™ could bring together indicators including complaints, victim experience, misconduct, workforce information, operational data, legal and financial exposure and public-confidence measures. The objective is not another complaints system, but better organisational intelligence: identifying patterns, understanding the true cost of the bleed, prioritising intervention and measuring whether action has reduced harm.

The methodology is being developed through real-world public-sector problem solving. An initial University of Reading consultancy demonstrator has applied Haemostasis™ to NHS maternity services, exploring how fragmented evidence can become board-level risk intelligence, cost-of-failure analysis and strategic recommendations.

innov8law now proposes applying this cross-government architecture to policing, initially supporting Problem 6: building and maintaining public trust, with direct relevance to Problem 2.

Stop Harm. Repair Damage. Rehabilitate Systems.

To find out more about Haemostasis™, visit our website or contact us.

InterSystems
Creative data technology

Policing cannot afford to wait years for a single future system before improving how information moves between forces, counties and partner agencies. The 2026 Police Reform White Paper says nine in ten crimes have a digital component and argues for less fragmentation and clearer national standards. Better data sharing will be central to making that ambition practical.

It is to help policing and justice partners share structured, meaningful information securely, so they can build a fuller view of people, incidents, intelligence and risk, including when cases move across county lines.

Data still sits across 43 forces, national systems and local platforms. The Police Digital Service handbook positions interoperability as essential to sharing data across organisational boundaries, reducing duplication, and enabling analytics and AI at scale.
Healthcare has faced a similar challenge: how to connect sensitive information across complex organisations without disrupting frontline services.

Shared Care Records offer a useful example. They connect sensitive information across NHS, local authority and care settings, giving staff access to more complete and up-to-date information while frontline systems remain in place.
Forces can start by making the information they already hold easier to share securely across counties and partners, while local systems modernise over time.

Why data fabric deserves attention
A data fabric approach is well suited to this challenge because it connects existing data sources rather than requiring forces to replace systems that still support daily operations. By creating a secure, governed layer across multiple environments, it can give authorised users a more coherent view of operational information in real time

To find out more, visit our website or contact us.

NiCE

Question 2's pain points: an ageing, costly call-handling stack; rising 999, 101, email and social-media contact straining control rooms; and a need to unify emergency/non-emergency channels while building public trust. NiCE Evidencentral answers this by holding call handling and digital evidence on one platform.

This is already operational: Cheshire Constabulary uses NiCE Inform to record 999 and 101 calls alongside CCTV, body-worn video and interviews in one environment, and Humberside Police is extending this, planning to route roughly 23,500 monthly 999/101 calls straight into investigation files. The same platform eases control-room demand through self-service digital contact: Humberside's "golden hour" burglary response now lets officers hand residents a link rather than book a follow-up visit. Nottinghamshire Police and Northamptonshire Police use it to deliver more compassionate, trusted contact to vulnerable people, turning legacy technology, channel fragmentation and public trust into one platform-level answer.

To find out more, visit our website or contact us.

OPSWAT.

The Policing Problem Book identifies digital evidence capture and analysis (Problem 1), Digital Public Contact transformation (Problem 2), and secure data sharing across forces (Problem 3) as central challenges. Underlying all three is one question: as forces digitise contact, evidence and case management, who checks that every file entering the estate can be trusted?
MetaDefender is built on a zero trust principle. A firewall or VPN controls who can reach a system, but says nothing about whether the file they bring is safe. Encryption does not solve this either: an encrypted attachment or upload can still carry malware, since encryption protects a file in transit, not its content.

MetaDefender inspects, sanitises and rebuilds files at every point they cross into policing environments: crime reporting portals, email attachments, and USB, CCTV and bodycam footage collected in the field or moved between forces and to the CPS. Deep CDR and multiscanning remove hidden threats while preserving evidential integrity and chain of custody.

An “ingest once, share with many” approach means evidence is checked once, then moved across systems with a full audit trail, cutting manual triage and supporting the standardisation the Problem Book calls for.

UK police forces already run OPSWAT in live operation, on file upload portals, email gateways and frontline evidence handling.

To find out more, visit our website or contact us.

Simpson Associates

Public contact remains one of the most important interfaces between policing and the communities it serves. Whether through a 999 call, a 101 enquiry, an online report or another digital channel, every interaction shapes public confidence and provides valuable insight into community demand.

As demand continues to grow in both volume and complexity, many forces face a common challenge: information relating to public contact is often spread across multiple systems, teams and processes. This can make it difficult to establish a complete view of an individual’s interactions, ensure staff have the context they need and provide a consistent experience for the public.

Simpson Associates has more than three decades of data and analytics experience and has worked with over 65% of UK police forces. Through this experience, we have seen that forces often already hold the information needed to improve service delivery and support decision-making. The challenge is making that information accessible, connected and actionable at the point it is needed.

A more connected approach to public contact can help forces better understand demand, improve visibility across citizen interactions and support more informed operational decision-making. It also creates opportunities to reduce effort for both staff and the public while helping build confidence in policing services.

In this article, Simpson Associates explores why connected data is becoming increasingly important to modern policing and how forces can make better use of the information they already hold to deliver better outcomes for the communities they serve.

To find out more, visit our website or contact us.

---

sopra steria

Policing must move beyond fragmented local contact arrangements and create a consistent, citizen-centred contact-to-response model. Currently, public contact with police forces is delivered through 43 separate force operating models, with different processes, technologies and channels. This leads to inconsistent service experiences, duplicated effort, fragmented data, and varying approaches to identifying risk and vulnerability.

Strategic digital transformation presents an opportunity to redesign how policing engages with the public. Rather than simply digitising existing processes, policing can establish a nationally aligned model for public contact, supported by common standards, shared services and interoperable technology. This would enable citizens to access policing through a single, intuitive digital entry point while ensuring requests, reports and incidents are routed efficiently to the appropriate local or regional response capability.

Building on established command-and-control capabilities, public contact can become seamlessly connected to operational response. Information provided by the public would flow securely through a shared workflow from first contact to assessment, triage, tasking and resolution, reducing re-keying, improving visibility and enabling faster decision-making.

For citizens, this would mean simpler access to services, secure case tracking, personalised updates and a more transparent understanding of what happens next. For policing, it would provide better demand management, more consistent identification of vulnerability, improved resilience and greater insight across forces and partner organisations.

Underpinned by common data standards, open APIs, intelligent triage and cloud-based services, this approach would improve public service delivery, reduce duplication and create a resilient, scalable foundation for future policing needs.

To find out more, visit our website or contact us.

Untrite THRIVE is a Force Intelligence Platform that works inside the 999 and 101 control room. It listens to the live call, applies the force's own THRIVE risk methodology as the conversation happens, and drafts the structured record: incident log, risk assessment, vulnerability and repeat-victim flags, formatted for the force's systems. The operator stays focused on the caller, then reviews and signs off every output. THRIVE is real-time, human-in-the-loop and auditable by design, not a black box and not an autonomous decision-maker.

We lead with evidence, not promises. THRIVE has run live at Humberside Police since 2024, funded by the force, the Police Digital Service and the Office of the Police Chief Scientific Adviser, and aligned with the NPCC AI Strategy and the new PoliceAI centre. An independent University of Sussex evaluation of more than 1,252 calls found repeat victims identified far more often (up 19 percentage points, from 58% to 77%), 93% operator agreement with the AI's risk assessment, and around eight minutes saved on a typical domestic abuse call. The full evaluation report is available on request.

THRIVE addresses several of the thirteen problem statements at once, including Problem 2: better public contact at the point of first contact.

One proven system, addressing the challenges where policing needs it most.

To find out more, visit our website or contact us.

3. How can policing enable secure, efficient, and standardised data sharing across forces?

With 48 independent forces running separate IT systems, fragmented data landscapes have hampered investigations through duplicated entry, inconsistent formats, and poor interoperability. The solutions presented here enable secure, real-time data sharing across legacy systems, alongside mechanisms to ensure data integrity, auditability, and effective deduplication of records across agencies.

Primary Service Lines: *Interconnectivity, Analytics*

Augur exists to protect people where they live, work, travel and gather.

The threat to public safety is growing faster than existing security services can respond. There is strong mission alignment between Augur and UK Policing; we have prioritised three Problem Book statements where Augur can have immediate, tangible impact:

Augur ingests diverse data sources, from CCTV and body-worn video to metadata from radio calls and online reports, giving policing teams and key security partners (i.e. large public venues) a unified space to collaborate, prioritise and act — preventing critical information being siloed at the operational layer, with a clear evidentiary trail.

To find out more, visit our website or contact us.

BlackRainbow was founded by SMEs who recognised key challenges in the investigation industry and the limitations of supporting technology. We developed NIMBUS, a versatile and scalable platform built around three core pillars: Intelligence, Investigations and Forensics to streamline the entire case management lifecycle, improving efficiency, accuracy, auditability and compliance to standards and procedures. Designed for Law Enforcement, Government and Corporates, it delivers complete visibility and control through intelligence-led data, evidence tracking, automated workflows, decision making, tasking and reporting.

Already operational across UK policing, NIMBUS has unified case and quality management, reducing risk, improving interoperability, lowering manual workloads, and enhancing efficiency, cost effectiveness and staff wellbeing. Our solution addresses several problem questions, including how can policing enable secure, efficient, and standardised data sharing across forces.

You can find out more through our case study, or contact us.

Videris, from Blackdot Solutions, is a secure OSINT investigations platform originally built for the UK intelligence community and now used widely across UK policing, defence and financial crime teams. It pulls together over 200 data sources, including the surface, deep and dark web, social media, corporate records, and sanctions and PEP lists, plus any custom or internal data connected via API, into a single case. From there, automated link analysis charts networks and surfaces connections that would otherwise take hours to find manually.

As one UK policing user described it: "I'd describe Videris as an ever evolving powerful secure online investigative platform, enabling users to identify online accounts and commercial data with the capability to extensively map and visualise a network of people, companies, addresses, and identifiers. It also features a closed AI feature enabling complex network data returns to be queried to help explain how certain entities are linked in the data."

Problem 3 (secure, standardised data sharing across forces): Videris allows multiple investigators, including those working across force boundaries, to collaborate on the same case, share findings and generate consistent, audit-logged intelligence reports in seconds. This cuts down on duplicated effort and helps standardise how forces work together.

Videris is UKSV-cleared for trusted support, Cyber Essentials Plus and ISO 27001 accredited, and available via G-Cloud.

To find out more, visit our website or contact us.

The rapid growth of digital evidence, AI, and technology-enabled crime are creating significant challenges for UK policing. There is a common need for secure data sharing, interoperability and digital capability.

A range of internationally recognised standards provide a foundation for digital policing. ISO/IEC 27001 supports the secure management of information. ISO/IEC 27037 provides guidance on the identification, collection and preservation of digital evidence, while ISO/IEC 42001 supports the responsible governance of AI systems. ISO/IEC 27701 strengthens privacy and the secure handling of personal data.

Beyond existing standards, BSI is developing a Digital Product Safety Standard to help prevent online harms and technology-enabled crime. Emerging digital and AI literacy standards will help define skills for a modern police service.
To maximise impact, policing requires more than individual standards. A coordinated standards programme could provide a pathway from creation to implementation.

A national digital evidence standard could establish common data formats and workflows across all 48 police forces, enabling secure information sharing. Interoperability standards could create common interfaces between policing, forensic and criminal justice systems, accelerating investigations.

Together, existing standards and a development programme would ensure standards are adopted and deliver benefits. This programme will create a policing ecosystem capable of addressing multiple challenges across the Problem Book.

To find out more, visit our website, or contact us.

Butterfly Data Over 90% of reported offences now feature a digital component, yet un-triaged hardware overloads Subject Matter Experts (SMEs) while disconnected systems silo intelligence. Butterfly Data delivers bespoke engineering and analytics to reduce forensic backlogs and connect isolated platforms. As a SAS Gold Partner, we pair tailored engineering with enterprise software—including SAS Law Enforcement Intelligence—to address NPCC Policing Problem Book Statements 3:

We implement automated ingestion scripts to categorise and route evidence without manual intervention, and deploy force-wide analytics to cross-reference identifiers and signatures across cases.We layer secure API channels over existing infrastructure, streaming intelligence to frontline devices, as demonstrated with North Wales Fire and Rescue Service.

By combining bespoke integration with enterprise analytics, we turn raw data into actionable intelligence, closing the gap between disconnected systems.

To find out more, visit our website, or contact us.

Datalynx
A CACI Business

Effective policing depends on the ability to share trusted information securely and consistently across organisational boundaries. As forces tackle more complex, cross-border and digitally enabled crime, the need for high-quality, standardised data has never been greater.

The Police National Database (PND) is one of policing's most significant examples of national data sharing. When the platform was established, intelligence data was held across hundreds of operational systems in different formats, creating significant challenges for interoperability, consistency and access. Datalynx, a CACI company, addressed this challenge through data analysis, data quality assessment, interface development, testing and the implementation of integration capabilities from 300 systems across over 60 law enforcement data providers into a single dataset.

Today, Datalynx continues to support PND through a range of data management, integration and assurance services, helping ensure critical information remains accessible, reliable and actionable across policing.

The success of PND demonstrates that effective data sharing is about more than technology. It requires trusted data, common standards, robust governance and proven delivery experience. These same principles underpin today's policing transformation programmes, including LEDS and wider national data initiatives. With decades of experience supporting national policing data services, Datalynx is a trusted partner helping organisations overcome fragmentation, improve data quality and create the foundations for secure and efficient information sharing at scale.

Learn more about Datalynx's, a CACI company, policing and data integration expertise at our website, or contact us.

Capgemini

Policing can enable secure, efficient and standardised data sharing across forces by moving from data centralisation to trusted computation. Privacy-enhancing technologies provide a route to collaboration where sensitive information can remain under the control of the organisation that holds it, while authorised analytics, matching and decision-support processes are performed securely across distributed datasets. This approach allows organisations to unlock value from sensitive data without exposing the underlying information, supporting privacy by design and stronger governance. Further details are available here: Secure Data Analytics Without Moving Data | Capgemini UK.

This model offers an alternative to creating new central repositories or wholesale replacement of legacy systems. Secure execution layers, encrypted computation, federated analytics and trusted environments can sit across existing architectures, allowing forces and partner agencies to query, analyse and reconcile relevant information in near real time, while reducing the need to copy, pool or disclose sensitive records.

To ensure integrity and auditability, policing should combine these technical controls with common governance standards, clear authorisation rules and auditable workflows. Each organisation can retain ownership of its records while contributing to a shared analytical process.

The same approach can support reconciliation and deduplication across disparate systems.

Privacy-preserving matching techniques can compare identifiers without revealing full underlying records, helping agencies identify linked, duplicate or inconsistent information while maintaining appropriate safeguards.

To find out more, visit our website, or contact us.

Policing cannot investigate effectively while 48 forces hold data in 48 different ways. Officers duplicate work, evidence takes longer to piece together, and the risk of error grows every time a record is re-keyed by hand. Today, no shared layer exists to let one force reach another's data securely and in real time, without a national records rebuild that would take a decade to deliver.

We answer this from direct experience. Through ResilienceDirect, we have run the secure platform the UK's emergency services and armed forces use to share sensitive information since 2013, proving that identity-verified, fully logged access works across organisational boundaries under real pressure. We are applying the same connect-not-replace principle today inside West Mercia Police, using Appian's data fabric to link a new digital forensics case management platform to other force systems through API integration, keeping specialist teams working in the tools they already know.

That same evidence extends to integrity, reconciliation and emerging technology. Our proof of concept for the College of Policing, built on an open integration standard, shows structured data and unstructured policy guidance can be queried together in real time, cutting the wait for manual searches and overnight batch transfers. Zero Trust access, delivered with our partner Cloudflare, secures every one of these connections without requiring forces to rebuild what they already run.

To find out more, visit our website, or contact us.

Chorus
Discover • Link • Solve

CIS is by design a collaboration platform, enabling Frontline Officers, Investigators, Analysts & DFU's to work concurrently on a single case both within a single force or collaborating across multiple forces providing a single source of evidence for all connected users. Access to individual cases can be strictly controlled at the user level by assigning individuals Security levels and Security Groups.

You can view our County Lines case study here.

To find out more, visit our website or contact us.

CIVICA

Six of the NPCC's 13 identified problems — spanning public contact, cross-force data sharing, offender monitoring, online child sexual exploitation, workforce protection, and innovation/strategic foresight — share a common structural cause: fragmented, unreconciled data about the same people, places, cases and equipment held across 48 independent systems.

The case made here is not that Master Data Management (MDM) solves policing's 13 problems. It is that six of them are, in part, the same problem — and that solving it once, doing it well, is worth significantly more than solving it 48 times separately.

A modern MDM platform does not solve every dimension of these problems on its own, however, MDM addresses the shared root cause running underneath most of them: the inability to reliably tell that a record in one system and a record in another refer to the same real-world person, case or thing.

Problem 3 is a foundational problem that, when solved, would provide value to all other problems.

A pilot focused on Problem 3 would test the core matching and relationship-discovery capability in its most direct application and would generate the evidence base needed before extending the same underlying platform to the more sensitive problems.

For further descriptions of the value from MDM to Problem Statement 3, visit our dedicated page or contact us.

CLOUD GATEWAY

Cloud Gateway operates the connectivity and security layer that modern policing runs on. Our secure connectivity platform brings network, security and observability into one operating model, delivered by one UK team on sovereign infrastructure built for the assurance standards specific to policing.

Urgent reform, tightening regulation and emergent technology are not arriving as separate problems that need solving one at a time. They are converging on the same policing infrastructure at once. Our platform is architected at that intersection: an experience plane for governed operations, a connectivity and security fabric that consolidates disparate tooling, an intelligence layer for unified observability, and an assurance foundation built on accreditation and evidence. It is the digital foundation policing needs to operate securely, modernise and stay compliant.

Interoperability, named as a design requirement in the NPCC Problem Book and the Hogan-Howe review, only becomes real when common patterns for data exchange, identity, access and audit sit underneath. Without that foundation, new capabilities, including those that are truly transformative, have to be rebuilt force by force. With it, what works in one force can travel to the next. This is what our platform provides.

Most forces start with one problem and extend from there:

- Evidencing compliance as a continuous, provable state rather than a pre-audit scramble
- A stronger security posture with consistent policy enforced across every user, site and connection
- Modernisation of legacy estates
- Connectivity to government networks, partners and sector peers

- AI-ready infrastructure to support increased data volumes and cloud workloads

For Avon and Somerset Police we migrated 64 WAN sites to direct cloud and PSN access, removing central backhaul and laying the foundation for cloud, AI tooling and data-sharing across forces. Read the case study.

To find out more, visit our website or contact us.

COEUS software

PoliceBox is a nationally scalable, locally configurable Frontline Operational Platform designed to help policing modernise frontline work while making better use of existing systems.

It primarily addresses Problem Statements 3, 10 and 13: secure, efficient and standardised data sharing; a digitally empowered workforce; and embedding innovation and evaluation into policing.

PoliceBox provides a common operational layer between officers and systems such as CAD, RMS and national services. Its open, API-first architecture supports secure integration with existing and future systems without replacing systems of record.

For officers, PoliceBox brings tasks, operational information, workflows and guidance into one mobile-first experience. It works online and offline, reduces re-keying and system switching, and supports structured, auditable data capture at the point of activity.
Cecil, the PoliceBox AI-enabled operational assistant, provides procedural support using approved national and force-specific sources. It remains advisory: professional judgement stays with the officer, who authors the operational record.

This approach was evaluated with Humberside Police through the NPCC NSIB-funded Project Moriarty Test & Learn trial. Cecil achieved average scores of 4.6/5 for accuracy, 4.5/5 for relevance and 4.6/5 for usability, with responses in under 30 seconds.

To find out more, visit our website or contact us.

As the 2026 Police Reform White Paper states, police performance has declined in recent years, and criminals are outpacing the police in leveraging technology.

If UK policing wishes to improve in these areas, it must move beyond its current fragmented data foundations. This was evidenced in the Policing Insight and techUK Workforce Survey (2026), in which only 16% of 8,000 officers and staff reported that their force systems are well integrated. This was stated in the aforementioned White Paper:

...designing solutions separately several times over, leading to unnecessary spending. This locks away useful data and restricts our ability to make informed decisions at a national level. We are not getting the right information into the right hands at the right time. Compounding this landscape is the fact that digital evidence now features in approximately 90% of all investigations. The volume, variety, and complexity of such material place a burden on officers and analysts who still rely on manual processes to secure, transfer, and analyse evidence.

What is required is a Unified Intelligence Future. The Future is not one technology; it is an Open Standards Ecosystem that provides freedom from vendor lock-in. This future will unlock the full power of police data without rebuilding core systems or creating new data silos. The Databricks Platform provides such a future. Our unified data lakehouse architecture brings together structured records from crime and intelligence systems, as well as petabyte-scale digital evidence, enabling the police to adopt the AI and analytics capabilities they need to deliver real-time decision-making.

To find out more, visit our website or contact us.

Real-Time Situational Awareness for Officer Safety helps protect officers and improve operational decision-making by giving command centres real-time visibility of frontline risks, welfare concerns, and emerging incidents. It replaces fragmented radio updates and delayed reporting with continuous, actionable intelligence.

Using approved wearables and mobile devices, the platform provides real-time officer safety and welfare monitoring, location awareness, and automatic detection of distress events. It can identify falls, panic activations, weapon deployment, and signs of escalating situations. Sensitive data is processed securely on the device, ensuring only relevant insights are shared with supervisors

and control rooms. This enables faster intervention, intelligent deployment, and improved coordination of personnel and assets. SITREP AI maintains resilient communications when conventional networks fail through a mesh network operating across cellular, Wi-Fi, and satellite networks. This ensures a persistent operational picture during major incidents, public events, rural deployments, and in areas with poor signal coverage.

The platform also identifies patterns associated with escalating risk, helping supervisors prioritise alerts, allocate resources effectively, and make informed decisions in rapidly changing operational environments.

As adoption matures, SITREP AI evolves from delivering situational awareness to providing operational insight and decision support, helping forces move from reacting to incidents to anticipating operational risk.

To find out more, visit our website or contact us.

---

esri UK

ArcGIS uses location as the essential thread to connect policing data, people, systems and intelligence, with trusted information shared securely, understood consistently and acted upon in real time. A Location Data Fabric brings together fragmented policing data in a single, coherent operational view. Location is one of the most powerful references to join datasets together, adding geographic context that helps forces better understand patterns in data, identify risks and make informed decisions. ArcGIS creates a trusted operational picture that forces and partner organisations can work from across boundaries, ensuring shared understanding, clarity and consistency.

Trusted, consistent, verifiable location data provides a common operational picture across forces and partner agencies. The West Midlands Violence Reduction Partnership uses shared location intelligence to support coordinated, evidence-based action, allowing partners to easily track progress, target interventions and strengthen initiatives.

To find out more, visit our website or contact us.

One area of IBM is focused on bringing data together from multiple sources whether its legacy hybrid or cloud so that insight can be captured without moving the data to another area .

This could be hugely successful in policing .

IBM's approach connects to data in place rather than requiring migration into a single central store, satisfying legal data protection boundaries while enforcing consistent governance.

Domestic abuse, vulnerability and safeguarding cases are complex because the picture of risk is scattered across command and control, records management, intelligence, safeguarding and partner-agency systems that were never designed to talk to each other. Connecting these types of existing estates rather than replacing them - using federated query capability to pull a live, unified view of an individual, address or order across multiple sources without copying or migrating data. For example an officer preparing a Protective Order file, or a team checking compliance, can see the full evidential and offending history the moment it's needed, drawn directly from source-of-truth systems. Underpinning this is a trusted-data layer: automated quality, matching and enrichment so records relating to the same victim, offender or incident are reliably linked, reducing missed connections. Data lineage ensures every piece of information feeding a risk assessment or court-bound case file can be traced back to its origin, supporting evidential auditability. A shared data catalogue and semantic layer also let disparate force data models be reconciled consistently, so risk indicators mean the same thing wherever they're captured.

To find out more, visit our website or contact us.

Public-sector organisations already hold many of the warning signals of tomorrow's failures: complaints, incidents, claims, misconduct, workforce pressures, financial losses, poor outcomes and declining public trust. Too often, those signals are considered separately.

innov8law Haemostasis™ is a cross-government methodology designed to help leaders connect those signals, identify where organisational harm is developing, quantify its human, social and economic impact, diagnose root causes and intervene before harm and cost escalate.

The methodology follows six stages: Target → Structure → Quantify → Diagnose → Intervene → Make the Case.

Its configurable Haemostasis Scorecard™ provides an early-warning and decision-support architecture through which different public services can select relevant indicators while retaining a common framework based on Human Value, Social Value and Economic Value.

For policing, Haemostasis™ could bring together indicators including complaints, victim experience, misconduct, workforce information, operational data, legal and financial exposure and public-confidence measures. The objective is not another complaints system, but better organisational intelligence: identifying patterns, understanding the true cost of the bleed, prioritising intervention and measuring whether action has reduced harm.

The methodology is being developed through real-world public-sector problem solving. An initial University of Reading consultancy demonstrator has applied Haemostasis™ to NHS maternity services, exploring how fragmented evidence can become board-level risk intelligence, cost-of-failure analysis and strategic recommendations.

innov8law now proposes applying this cross-government architecture to policing, initially supporting Problem 6: building and maintaining public trust, with direct relevance to Problem 3.

Stop Harm. Repair Damage. Rehabilitate Systems.

To find out more about Haemostasis™, visit our website or contact us.

InterSystems
Creative data technology

Policing cannot afford to wait years for a single future system before improving how information moves between forces, counties and partner agencies. The 2026 Police Reform White Paper says nine in ten crimes have a digital component and argues for less fragmentation and clearer national standards. Better data sharing will be central to making that ambition practical.

It is to help policing and justice partners share structured, meaningful information securely, so they can build a fuller view of people, incidents, intelligence and risk, including when cases move across county lines.

Data still sits across 43 forces, national systems and local platforms. The Police Digital Service handbook positions interoperability as essential to sharing data across organisational boundaries, reducing duplication, and enabling analytics and AI at scale.
Healthcare has faced a similar challenge: how to connect sensitive information across complex organisations without disrupting frontline services.

Shared Care Records offer a useful example. They connect sensitive information across NHS, local authority and care settings, giving staff access to more complete and up-to-date information while frontline systems remain in place.
Forces can start by making the information they already hold easier to share securely across counties and partners, while local systems modernise over time.

Why data fabric deserves attention
A data fabric approach is well suited to this challenge because it connects existing data sources rather than requiring forces to replace systems that still support daily operations. By creating a secure, governed layer across multiple environments, it can give authorised users a more coherent view of operational information in real time

To find out more, visit our website or contact us.

Kahootz provides secure workspaces for sharing information and coordinating work across organisational boundaries. Authorised participants can access current documents, discuss issues, manage tasks, record decisions and maintain an auditable history of activity in one shared workspace.

This is relevant to policing because forces increasingly need to collaborate with other forces, national bodies, suppliers and community or specialist partners. Kahootz can provide a single source of truth for this work, reducing reliance on email attachments, disconnected shared drives and informal channels. Its features include configurable access permissions, document version control, review and approval workflows, task management and audit trails.

Kahootz is already used in sensitive public-sector collaboration across government, including through Defence Share, the Ministry of Defence's primary collaboration tool. Powered by Kahootz, Defence Share enables the MOD to share information classified up

to OFFICIAL-SENSITIVE with defence industry partners, other government departments, agencies and allied nations. It provides geographically distributed participants with secure workspaces for accessing information and collaborating on complex programmes.

The same principles could support policing collaboration while complementing, rather than replacing, core operational systems and information-governance processes.

To find out more, visit our website or contact us.

Lumilinks

January's white paper commits to integrating information across local and national systems through a National Data Integration and Exploitation Service and national data standards. Most forces already own digital evidence and records systems. What is missing is a governed layer where data can be joined, interpreted consistently and acted on without waiting for structural reform.

Sharing today means an extract, a transfer, a copy. Control is lost the moment it lands. It drifts out of date. No one can say who holds what. The NAO concluded in November 2025 that patchy digital adoption and weak standardisation have hampered productivity; 443,000 officer hours sit in crime recording duplicating information already held. Picture an officer working a suspect active across three force boundaries: requesting, waiting, then reconciling extracts that define the same offence differently.

There is an alternative. Stop moving data. Grant governed, revocable access instead. On Snowflake a force publishes a permissioned view (a defined slice, not a database) that a neighbouring force, regional unit or CPS queries live. Nothing is exported. Access is logged, scoped and withdrawn at will. Where organisations need only confirm whether an individual appears in both datasets, the match returns without either side exposing records. Standardisation remains the harder half. Offence codes, risk flags and vulnerability markers carry different meanings across systems. Lumilinks delivers the shared semantic layer that resolves this: agreed definitions, version-controlled and mapped onto whatever each force runs. Standardisation becomes a modelling exercise deliverable in a quarter rather than a programme measured in years.

The binding constraint is governance, not technology. Lumilinks starts small. One or two forces, one measurable outcome, this year.

To find out more, visit our website or contact us.

Made Tech worked with the Ministry of Justice on the Victim Pathfinder project to explore how data and digital services could improve victims' experiences in the criminal justice system.

The work exposed a fundamental challenge. Victim information is held across police forces, the Crown Prosecution Service, HMCTS, and other agencies, but it does not flow easily between them. Legacy systems are secure in isolation, creating silos that prevent staff from accessing a trusted, up-to-date view of a case and leave victims unsure of what is happening.

Rather than just documenting the problem, the Pathfinder used live delivery to test how boundaries could be overcome. The team developed a victim-facing Track My Case service, giving people clear information on where and when their case would be heard, alongside guidance and support. They also worked with HMCTS to create a lightweight API exposing court data in a reusable form, extending value beyond the Pathfinder itself.

The product strategy connected user-facing services and reusable platform components around accurate, shared data. The goal was to reduce duplicated administration, free staff to focus on those needing support, and provide victims with timely, transparent information. These principles address wider policing challenges, such as community-based offender management, drawing on our discovery work into VCMS and Victim Liaison Officers, where staff need secure access to cross-agency information.

The Pathfinder showed that solving local problems with isolated technology deepens national fragmentation. Reusable components, common data standards, and secure data-level access enable joined-up services without weakening controls. The research, learning, and code remain available to build on, offering a tested foundation for criminal justice services that are more efficient, transparent, and capable of strengthening public trust.

To find out more, visit our website or contact us.

Many of the most pressing challenges facing law enforcement today are connected by a common reality: digital evidence now underpins most investigations.

Magnet Forensics helps police forces modernise the full digital investigation lifecycle. Its digital forensics solutions support the lawful

acquisition, processing, analysis, review and sharing of evidence from mobile devices, computers, cloud services, vehicles, video and other digital sources.

Magnet One connects tools, data, and authorised stakeholders in a unified investigative platform. It enables secure sharing and collaboration and centralized evidence management, across forensic units, investigators, supervisors, and prosecutors, reducing delays and duplication while strengthening oversight, chain of custody, and auditability. With digital evidence becoming increasingly prone to alteration, Magnet Verify can help confirm the authenticity of files by examining the digital structure to determine whether they have been changed. Across these workflows, trusted AI and automation help teams surface relevant evidence, recognise connections and focus specialist time where it can have the greatest impact.

By connecting people, processes, and technology, Magnet Forensics helps address key policing challenges related to digital evidence, shortening the path from evidence to action, and delivering more efficient, transparent, and trusted outcomes for victims, communities, and the justice system.

To find out more, visit our website or contact us.

NiCE

Question 3 highlights the cost of fragmentation: 43 forces running incompatible systems, inconsistent formats, and duplicated entry that slows cases and raises error risk. NiCE Evidencentral acts as the shared, secure layer across those legacy systems rather than requiring a rebuild.

South Wales and Gwent Police already run it as one centralised platform, giving them, as Bryn Glennie puts it, “a single centralised DEMS.” British Transport Police proves the model works between organisations too: registering the Metropolitan Police through its Business Portal now delivers 999 recordings electronically, with “no discs, no tapes, no delays,” a model extending toward all 43 forces. Every deployment is ISO 27001-certified on Microsoft Azure with full audit trails, letting Cheshire Constabulary’s counter terrorism unit assess evidence remotely in minutes. Leicestershire Police shows duplicated entry eliminated entirely, completing an end-to-end process at their desk within half an hour.

To find out more, visit our website or contact us.

One of the greatest challenges in implementing meaningful change is knowing where to begin. Establishing a reliable framework for data sharing requires navigating complex regulatory requirements, adhering to ethical and legal obligations, and selecting secure, resilient systems to manage and protect sensitive information. The process can often be overwhelming, resource-intensive, and time-consuming.

How can Nine23 support you to achieve multi-agency data-sharing?
Nine23's FLEX Pathway offers a flexible managed service for connectivity across multiple assured networks, hybrid cloud and zero-trust internet services to provide the infrastructure layer that underpins interoperability. However, the challenge of sustaining successful interoperability requires foundational work, before technology solutions are considered.
PIRI has been developed to simplify that journey. Our roadmap provides a foundational assessment of a force's readiness for interoperable and connected data and outlines the practical steps agencies need to take to build the right foundations. It offers a structured approach to assessing, selecting, and investing in secure, scalable infrastructure that supports compliant and effective data sharing.

Designed specifically for policing authorities and law enforcement agencies, this roadmap provides a step-by-step framework to build confidence in the legal, ethical, and operational aspects of data sharing. Most importantly, it provides access to experienced subject matter experts who can advise, demonstrate, and support implementation, ensuring organisations have a trusted partner to guide transformation from strategy through to delivery.

To find out more, visit our website or contact us.

The Policing Problem Book identifies digital evidence capture and analysis (Problem 1), Digital Public Contact transformation (Problem 2), and secure data sharing across forces (Problem 3) as central challenges. Underlying all three is one question: as forces digitise contact, evidence and case management, who checks that every file entering the estate can be trusted?

MetaDefender is built on a zero trust principle. A firewall or VPN controls who can reach a system, but says nothing about whether the file they bring is safe. Encryption does not solve this either: an encrypted attachment or upload can still carry malware, since encryption protects a file in transit, not its content.

MetaDefender inspects, sanitises and rebuilds files at every point they cross into policing environments: crime reporting portals, email attachments, and USB, CCTV and bodycam footage collected in the field or moved between forces and to the CPS. Deep CDR and multiscanning remove hidden threats while preserving evidential integrity and chain of custody.

An “ingest once, share with many” approach means evidence is checked once, then moved across systems with a full audit trail, cutting manual triage and supporting the standardisation the Problem Book calls for.

UK police forces already run OPSWAT in live operation, on file upload portals, email gateways and frontline evidence handling.

To find out more, visit our website or contact us.

Peregrine

Peregrine is a data integration and intelligence platform used by more than 450 public safety organisations. It integrates any source of data a force holds or receives into a single, permission-controlled operational layer, without replacing existing systems. The premise is straightforward: most of the intelligence forces need already exists within their estates, but it is fragmented. The constraint is not data collection, it is integration and access.

Peregrine applies a dynamic ontology above source systems, mapping heterogeneous records to a common data model so that information can be searched, shared and governed consistently within and between forces. Role and attribute-based permissions provide row and field-level control, allowing sharing arrangements to reflect existing legal and policy frameworks. This offers a route to interoperability that does not depend on a single national platform. The results achieved in regional sharing networks across the United States’ highly fragmented law enforcement landscape have been powerful, please see this video as an example.

To find out more, visit our website or contact us.

Digital evidence is fundamental to modern policing, but growing volumes create bottlenecks that can slow investigations.

Problem Statement 3 considers secure, efficient data sharing. Pimloc automatically detects and redacts personal information—including faces, licence plates, screens—across video and documents. Following human review, this compliant media can then be securely shared, downloaded or returned to supported DEMS platforms, helping evidence move safely to the CPS, partner organisations, data subjects - and more commonly, the media in order to manage misinformation, inform the public and build public trust and confidence.

To find out more, visit our website or contact us.

Synthetic data reproduces the structure, patterns and relationships found in real police data but includes no sensitive or personal information

Principle One brings synthetic data to life by applying it to real-world operational scenarios. Our outputs include communications data, ANPR, digital forensic material, financial data, crime reports or intelligence records

Why it's necessary
Police data is highly sensitive and often difficult to access for research, development and testing. Using live operational data creates privacy, access and governance risks.

Principle One's synthetic data creates a safe, controllable alternative. It allows realistic datasets to be generated without exposing victims, witnesses or officers, while still maintaining the complexity, links and imperfections of real operational information

What it enables
Synthetic data enables development and vigorous testing of new and emerging policing technologies. It can be used to expose knowledge gaps, software issues and improve functionality. It can also be used to gamify investigative scenarios to make training environments more immersive, and to build 'digital twins' of systems or organisations to develop AI

The benefits

Synthetic data makes innovation easier, safer and faster. It allows police forces and suppliers to develop, test and train using realistic data without exposing personal information. It can be generated at scale, reused consistently and tailored to include complex or rare scenarios that may be missing from live datasets. It also supports safer collaboration, better training and helps tools and approaches to be tested before they are introduced operationally.

To find out more, visit our website or contact us.

Q-SOLUTION

Data sharing across forces remains a significant challenge and can feel so large and complex an issue that it can't be addressed. There is however, a relatively little-known example from which a lot can be learned and leveraged.

The Criminal Justice Secure Exchange (CJSE) is the asynchronous message broker which links every police force in England and Wales with CPS, HMCTS and the Home Office. It is an incredibly resilient and reliable piece of nationally critical interoperability infrastructure backed by the security, governance, and crucially, data sharing agreements required to make it an excellent template that can be easily built upon.

Contracted by MoJ on behalf of CJS, CJSE is thoroughly modern serverless, microservice-architecture SaaS that transfers 5TB of information a year at a rate of 5.5m messages a month 24/7 365. On a minute-by-minute basis it communicates case information between the many disparate systems in the criminal justice system quietly providing assurance that files sent this way get to where they are supposed to and providing elasticity in the system so whilst other systems are down, off for maintenance, being patched or otherwise unavailable CJSE waits for them to be back up and ready before delivering.

There are so many potential areas CJSE can assist policing at a detailed level including data quality within forces and the reduction of casefile errors at source being just a few examples. Essentially the CJSE is an example of using an integration layer to provide efficient, extensible, configurable, scalable many-to-many connectivity. It is an extensible template for how Policing should think about data sharing capability when there is almost no end to the ways in which a force may want and need to share data of all types in future.

To find out more, visit our website or contact us.

Roke delivers secure, scalable information-sharing solutions that drive collaboration across complex national security environments. These are underpinned by synthetic data generation to enable experimentation amidst policy constraints. By applying common data standards (POLE/IES), we deliver interoperable solutions to enable confident action at pace.

To find out more, visit our website or contact us.

The NPCC Policing Problem Book outlines 13 critical challenges, emphasizing the need for data integration, digital trust, and operational efficiency. The Splunk Metropolitan Police (Met) case study serves as a direct response to these hurdles, demonstrating how a unified data platform transforms policing from reactive to proactive.

A core NPCC challenge is the burden of legacy systems and a lack of interoperability. The Met addressed this by using Splunk to monitor its “Connect” programme, which was designed to unify fragmented legacy data. Splunk provides the “single pane of glass” visibility required to ingest and analyze vast volumes of operational data in near real-time. This effectively bridges the gap between old and new systems, ensuring that critical tools for frontline officers remain operational and performant.

In summary, the Met’s use of Splunk provides a blueprint for the NPCC’s vision. It proves that by treating data as a strategic asset, police forces can strengthen public trust, eliminate technical silos, and achieve the operational agility necessary for modern law enforcement.

To find out more, visit our website or contact us.

Telefónica Tech’s Predictive Policing Accelerator, built on Databricks, helps police forces move from reactive reporting towards more proactive, intelligence-led policing. The solution brings together data from multiple policing systems into a single governed platform, providing a real-time view of crime, emerging trends, demand and harm-based priorities. Geospatial analytics helps identify hotspots and patterns, while AI-generated insights support earlier identification of emerging risks and more targeted operational responses.

Integrated with Databricks Genie, the accelerator also enables officers, analysts and operational leaders to explore governed policing

data using natural language, without relying on specialist technical skills or predefined reports. Users can investigate trends, drill into patterns and answer operational questions more quickly, helping translate data into actionable intelligence at the point of need. This supports better resource allocation, more targeted prevention activity and more informed decision making.

The approach is designed around responsible AI, with governance, transparency and human oversight embedded into the platform. This enables predictive insight to support professional judgement rather than replace it, helping forces adopt AI in a way that is accountable and aligned with policing principles.

To find out more, visit our website or contact us.

---

telicent

Secure, efficient, and standardised data sharing across the UK's 48 independent forces is essential to provide the interoperability needed to ensure the credibility of evidence, improve the timeliness of investigations, reduce the risk of intelligence failure, and free up Officer time by reducing repetitive tasks. Currently there are 48 IT estates, and even if there is consolidation, there will always remain a diversity of systems, not one overarching monolith. So, data must flow out of the existing systems, and once it leaves the estate, systems-based access control won't provide the security needed – data must carry its own security labels with it.

Telicent CORE is a secure open source, open standards data integration platform. We designed it to give fast-moving innovators the capability to adapt to changing mission needs and the demands for better data sharing, while giving the enterprise the assurance needed that their data is secured and standardised appropriately. It's capability directly addresses questions in Problem 3, sharing labelled data across legacy systems in real-time and ensuring only those cleared to access the data do through attribute-based access control. It's also being used by part of the Met and GMP police, and is currently part of the Home Office ACE's National Data Integration and Exploitation Service (NDIES) initiative.

Implementing CORE, and adopting a suitable data standard (e.g. POLE or the UK Government Information Exchange Standard (IES)) will enable data sharing, reconciliation of duplicate records across disparate systems, and auditability across multiple agencies.

To find out more, visit our website or contact us.

TENACIUM DC

There are 43 territorial police forces in England and Wales—and 48 UK-wide when non-territorial forces are included. Each is an independent data controller with different systems, suppliers and recording practices.

A police data exchange succeeds only when the recipient can establish where information came from, how safely it can be used and whether it is relevant to the task.

This matters when determining whether information held elsewhere concerns the same person, location, vehicle or event. The national audit of group-based child sexual exploitation and abuse found that some forces use around 100 systems, alongside uneven Police National Database access and uploads. More records alone cannot resolve differences in meaning, identifiers, currency, confidence or handling.

The National Data Integration and Exploitation Service and National Policing Digital Strategy are strengthening APIs, standards, identity and governance.

AI raises the stakes. Applied to fragmented or poorly contextualised information, it can accelerate retrieval while amplifying weak matches, stale assumptions and opaque reasoning. Forces need foundations that preserve meaning, evidence, permissions, human review and correction.

A “context contract” would help authorised recipients answer five questions:

1. What does this information mean?
2. Where did it come from?
3. When was it observed or verified?
4. How confidently does it relate to the current person, object or event?
5. What may the recipient do with it?

Tenacium has demonstrated multi-source refinement, semantic cataloguing, graph-based context and evidence-linked investigation in prototypes. We propose testing these patterns using synthetic or de-identified policing data, without replacing authoritative sources or national services.

This is not another platform. It tests whether information remains understandable, contestable and evidence-linked.

To find out more, visit our website or contact us.

TJA Associates offers a practical, outcome-led solution to Problem 3. Its core proposition is that policing should not treat data, innovation, emerging technology and mobility as separate issues, but as connected operating-model challenges that require governance, collaboration, evaluation and business change as much as technical capability.

TJA helps forces move from fragmented data and local workarounds to secure, standardised and auditable information sharing, focused on the operational decisions that need better intelligence.

TJA's product/case-study offer is not a single technology platform; it is a structured consultancy and delivery approach that helps NPCC and partner organisations define the problem, convene the right stakeholders, shape operating models, translate complex data into actionable intelligence requirements, manage delivery and measure benefits. This means TJA can address many Problem Book challenges where the barriers are interoperability, trust, evidence quality, public confidence, supplier engagement, governance and adoption. Find out more at TJA Associates.

To find out more, visit our website or contact us.

We all know the challenge of secure, efficient and standardised data sharing across policing is not a new one.

Policing already demonstrates that data can be successfully shared when common standards, governance and operating models are in place. The greater challenge is creating consistent approaches to data ownership, interoperability, security and adoption across a federated policing landscape.

At Trustmarque, we help public sector organisations solve complex business and technology challenges by aligning strategy, governance, data and platforms. We believe the opportunity for policing lies in establishing nationally mandated data standards, supported by secure-by-design architectures, modern integration capabilities and clear accountability for implementation.

Our expertise in secure cloud, data and AI, cyber security, integration and digital transformation enables organisations to unlock information from legacy systems, improve interoperability and build trusted data-sharing environments. By combining technology with governance and change management, policing can move beyond isolated systems and create a more connected ecosystem that improves operational decision-making, safeguarding outcomes and public confidence.

To find out more, visit our website or contact us.

4. How can policing efficiently assess and monitor a growing population of community-based offenders, especially high-risk individuals?

The population of offenders managed in the community, notably Registered Sex Offenders, now over 70,000, has grown 44% since 2014, increasing the burden of home visits and risk assessments. The solutions showcased below support earlier identification of high-risk individuals, enhance risk assessment tools, and improve the efficiency of in-person monitoring.

Primary Service Lines: *Personal Safety, Surveillance & Sensing*

BAE SYSTEMS

ILAS is an intelligence automation application that continuously ingests sub-threshold data points to monitor individuals for change and alerts officers when an intervention may be needed. The core policing problem it addresses is one of scale meeting scarcity. The community offender population is growing steadily while proactive capacity to visit, monitor and disrupt is finite. A static assessment made at the point of release rapidly ages as offenders' circumstances change, potentially missing the escalation signals that matter most. ILAS addresses this through a continuous, automated monitoring function that tracks change across a population and alerts at the inflection point where scrutiny is needed. This allows officers to prioritise their face-to-face capacity, rather than applying equal intensity across a caseload irrespective of current risk.

The capability maps directly onto two problem statements in the NPCC Policing Problem Book: Problem 4, regarding how to identify high-risk offenders earlier and enhance offender risk assessments; and Problem 5, in terms of identifying the need to automate evidence analysis to address the current scale of offending. The NPCC AI Strategy adds further strategic alignment, identifying the use of algorithmic tools combining datasets to identify risk more effectively and support better-informed decision-making.

The cross-cutting theme on data and interoperability identifies that relevant intelligence about an individual often does not reach the responsible officer in time to act, and that automated threat detection is now necessary. ILAS is designed to solve that problem. It empowers offender managers to function, in effect, at expert level across an entire caseload rather than paying close attention to a handful of cases. A two-force STAR-funded trial, led by Kent Police and Essex Police, tested ILAS in VAWG, with academic validation built into the trial design.

To find out more, visit our website or contact us.The CIS platform is currently being enhanced to include proactive social media monitoring, this functionality is being developed based on feedback from existing customers and is scheduled to be GA by the end of 2026.

To find out more, visit our website or contact us.

CIVICA

Six of the NPCC's 13 identified problems — spanning public contact, cross-force data sharing, offender monitoring, online child sexual exploitation, workforce protection, and innovation/strategic foresight — share a common structural cause: fragmented, unreconciled data about the same people, places, cases and equipment held across 48 independent systems.

The case made here is not that Master Data Management (MDM) solves policing's 13 problems. It is that six of them are, in part, the same problem — and that solving it once, doing it well, is worth significantly more than solving it 48 times separately.

A modern MDM platform does not solve every dimension of these problems on its own, however, MDM addresses the shared root cause running underneath most of them: the inability to reliably tell that a record in one system and a record in another refer to the same real-world person, case or thing.

Given the scale and sensitivity of the data involved — particularly for Problem 4 — we would suggest that any move to trial this approach begin as a bounded pilot, evaluated through the kind of national testing sandbox described in the Problem 13 section above, rather than a single national rollout.

For further descriptions of the value from MDM to Problem Statement 4, visit our dedicated page or contact us.

---

esri UK

ArcGIS uses location as the essential thread to connect policing data, people, systems and intelligence, with trusted information shared securely, understood consistently and acted upon in real time. A Location Data Fabric brings together fragmented policing data in a single, coherent operational view. Location is one of the most powerful references to join datasets together, adding geographic context that helps forces better understand patterns in data, identify risks and make informed decisions. ArcGIS creates a trusted operational picture that forces and partner organisations can work from across boundaries, ensuring shared understanding, clarity and consistency.

Using real-time, location-based intelligence of offenders, incidents, ankle tags and other sensors, to focus resources. In Canada, Durham Regional Police Service increased their bail checks from 1000 to 7000 per year, using our location-based dashboard.

To find out more, visit our website or contact us.

---

iizuka

Case Manager by IIZUKA is used by police, local authorities, charities and other organisations including Victim Support, Cranstoun, the Drive Project and Lancashire Constabulary to support victims of crime or work with perpetrators to reduce re-offending rates. We believe that its mobile working capability, offline synchronisation, proven security and reliability, integrations with police data systems, comprehensive and flexible assessment capabilities and quick to operate information access and case management functions make it ideally suited to address problem 4.

Any number of types of assessments can be set up, each with their own unique structure, which can follow sector defined best practice models, local or force specific working practices and legislative requirements as needed. When an assessment is required, the relevant structures are presented automatically, driven by rules based on a wide range of factors, including location, type of offence, situation and more. New assessments are automatically pre-populated from the last known status, making them quick to update and complete in both mobile and office-based situations.

In combination with identification technologies, such as Live Facial Recognition and the forthcoming Justice ID programme, Case Manager can automatically present the most recently completed assessment and other details, giving officers an immediate view of known risks, alerts and quick access to an individual's history enabling quick, on the spot decisions to be made. The outcomes of assessments feed directly into Case Manager and can drive further processes, alerts and business rules.

To find out more, visit our website or contact us.

ModularData

Community offender monitoring needs explainable risk signals.

Challenge 4 asks how forces can efficiently assess and monitor a growing population of community-based offenders, especially those at high risk. Most monitoring decisions are based on one or two facts, such as a recent risk classification change or a licence exclusion zone covering the officer's current address. These signals can move between probation and policing without the full case file, avoiding the governance and civil liberties problems of bulk record sharing.

Officers should only act on checked signals. Each signal should arrive with an evidenced assessment, the approver's name, and a decision audit trail. Part 3 of the Data Protection Act 2018 already requires safeguards around significant automated decisions, and

the same discipline should apply wherever an automated risk signal may lead to intrusive police action. Every AI recommendation should record the model and version, human review, and the final decision.

Forces should ask for explainability first. Officers can act quickly on signals they can trust, and spend far less time defending unexplained decisions in reviews and in court.

To find out more, read the full article or contact us.

Peregrine

Peregrine is a data integration and intelligence platform used by more than 450 public safety organisations. It integrates any source of data a force holds or receives into a single, permission-controlled operational layer, without replacing existing systems. The premise is straightforward: most of the intelligence forces need already exists within their estates, but it is fragmented. The constraint is not data collection, it is integration and access.

The same integrated layer supports configurable alerting when monitored individuals appear in new records, and network analysis that surfaces associations siloed systems obscure. The operational effect is measurable: Fairfax County Police Department identified a child abduction suspect within 13 minutes of the 911 call. The decisive search took 60 seconds, a result attributable to data already being connected and a platform usable at operational tempo.

To find out more, visit our website or contact us.

ROKE

Roke's Crucible Veil analyses social media to spot offensive online activity. Our Bickershaw product complements this by assessing linguistics and behaviour to flag risks of offending. Used alongside Vigil AI to monitor CSAM activity, we offer a comprehensive suite to manage community-based offenders.

To find out more, visit our website or contact us.

TENACIUM DC

There are 43 territorial police forces in England and Wales—and 48 UK-wide when non-territorial forces are included. Each is an independent data controller with different systems, suppliers and recording practices.

A police data exchange succeeds only when the recipient can establish where information came from, how safely it can be used and whether it is relevant to the task.

This matters when determining whether information held elsewhere concerns the same person, location, vehicle or event. The national audit of group-based child sexual exploitation and abuse found that some forces use around 100 systems, alongside uneven Police National Database access and uploads. More records alone cannot resolve differences in meaning, identifiers, currency, confidence or handling.

The National Data Integration and Exploitation Service and National Policing Digital Strategy are strengthening APIs, standards, identity and governance.

AI raises the stakes. Applied to fragmented or poorly contextualised information, it can accelerate retrieval while amplifying weak matches, stale assumptions and opaque reasoning. Forces need foundations that preserve meaning, evidence, permissions, human review and correction.

A “context contract” would help authorised recipients answer five questions:

1. What does this information mean?
2. Where did it come from?
3. When was it observed or verified?
4. How confidently does it relate to the current person, object or event?
5. What may the recipient do with it?

Tenacium has demonstrated multi-source refinement, semantic cataloguing, graph-based context and evidence-linked investigation in prototypes. We propose testing these patterns using synthetic or de-identified policing data, without replacing authoritative sources or national services.

This is not another platform. It tests whether information remains understandable, contestable and evidence-linked.

To find out more, visit our website or contact us.

University of Exeter

Through the Knowledge Transfer Partnership (KTP) programme, we are working in close collaboration with Devon and Cornwall Police (DCP) to embed innovation, evaluation, and strategic foresight into its culture and operations through the use of computer and data science. The headline aim of the KTP is to improve strategic management decision making through the use of digital tools such as artificial intelligence (AI) and digital twins, and to build confidence and a culture change within DCP.

An initial output is the development of a risk assessment tool for victims of domestic abuse. The tool is based on fast, lightweight, AI models that are transparent and explainable, with each victim's risk of harm being assessed on a percentage scale, which is then clustered into red-amber-green for visualisation. There has been very positive feedback from HMICFRS and early interest from other police forces.

The position is jointly funded by DCP and Innovate UK, whose aim is to translate cutting edge research into real-world impact. But the police are no longer able to participate in KTPs and so this route to funding projects long enough to establish close collaborations and knowledge exchange is now closed.

To find out more, visit our website or contact us.

---

5. How can policing transform the investigation and prevention of online sexual offences, particularly child exploitation?

Online child sexual exploitation and related offences are rising rapidly alongside offenders' use of emerging technology, generating large volumes of sensitive, unstructured data that overwhelm manual investigative methods. The solutions below support ways to automate the triage and categorisation of indecent imagery, enable secure cross-force collaboration, and provide adaptive training for evolving digital threats.

Primary Service Lines: *Personal Safety, Identification & Tracing*

BAE SYSTEMS

BAE Systems ILAS is an intelligence automation application that continuously ingests sub-threshold data points to monitor individuals for change and alerts officers when an intervention may be needed. The core policing problem it addresses is one of scale meeting scarcity. The community offender population is growing steadily while proactive capacity to visit, monitor and disrupt is finite. A static assessment made at the point of release rapidly ages as offenders' circumstances change, potentially missing the escalation signals that matter most. ILAS addresses this through a continuous, automated monitoring function that tracks change across a population and alerts at the inflection point where scrutiny is needed. This allows officers to prioritise their face-to-face capacity, rather than applying equal intensity across a caseload irrespective of current risk.

The capability maps directly onto two problem statements in the NPCC Policing Problem Book: Problem 4, regarding how to identify high-risk offenders earlier and enhance offender risk assessments; and Problem 5, in terms of identifying the need to automate evidence analysis to address the current scale of offending. The NPCC AI Strategy adds further strategic alignment, identifying the use of algorithmic tools combining datasets to identify risk more effectively and support better-informed decision-making.

The cross-cutting theme on data and interoperability identifies that relevant intelligence about an individual often does not reach the responsible officer in time to act, and that automated threat detection is now necessary. ILAS is designed to solve that problem. A two-force STAR-funded trial, led by Kent Police and Essex Police, tested ILAS in VAWG, with academic validation built into the trial design.

To find out more, visit our website or contact us.

BLACK RAINBOW

BlackRainbow was founded by SMEs who recognised key challenges in the investigation industry and the limitations of supporting technology. We developed NIMBUS, a versatile and scalable platform built around three core pillars: Intelligence, Investigations and Forensics to streamline the entire case management lifecycle, improving efficiency, accuracy, auditability and compliance to standards and procedures. Designed for Law Enforcement, Government and Corporates, it delivers complete visibility and control through intelligence-led data, evidence tracking, automated workflows, decision making, tasking and reporting.

Already operational across UK policing, NIMBUS has unified case and quality management, reducing risk, improving interoperability, lowering manual workloads, and enhancing efficiency, cost effectiveness and staff wellbeing. Our solution addresses several

problem questions, including how can policing transform the investigation and prevention of online sexual offences, particularly child exploitation.

You can find out more through our case study, or contact us.

Videris, from Blackdot Solutions, is a secure OSINT investigations platform originally built for the UK intelligence community and now used widely across UK policing, defence and financial crime teams. It pulls together over 200 data sources, including the surface, deep and dark web, social media, corporate records, and sanctions and PEP lists, plus any custom or internal data connected via API, into a single case. From there, automated link analysis charts networks and surfaces connections that would otherwise take hours to find manually.

As one UK policing user described it: "I'd describe Videris as an ever evolving powerful secure online investigative platform, enabling users to identify online accounts and commercial data with the capability to extensively map and visualise a network of people, companies, addresses, and identifiers. It also features a closed AI feature enabling complex network data returns to be queried to help explain how certain entities are linked in the data."

Problem 5 (online sexual offences, particularly child exploitation): These investigations rely on deep exploitation of social media, wider online presence and the dark web. Videris lets analysts map a suspect's network of friends, followers and associates anonymously and without leaving a digital footprint, helping identify further suspects and potential victims, all while staying compliant with RIPA and other legal frameworks.

Videris is UKSV-cleared for trusted support, Cyber Essentials Plus and ISO 27001 accredited, and available via G-Cloud.

To find out more, visit our website or contact us.

The rapid growth of digital evidence, AI, and technology-enabled crime are creating significant challenges for UK policing. There is a common need for secure data sharing, interoperability and digital capability.

A range of internationally recognised standards provide a foundation for digital policing. ISO/IEC 27001 supports the secure management of information. ISO/IEC 27037 provides guidance on the identification, collection and preservation of digital evidence, while ISO/IEC 42001 supports the responsible governance of AI systems. ISO/IEC 27701 strengthens privacy and the secure handling of personal data.

Beyond existing standards, BSI is developing a Digital Product Safety Standard to help prevent online harms and technology-enabled crime. Emerging digital and AI literacy standards will help define skills for a modern police service.
To maximise impact, policing requires more than individual standards. A coordinated standards programme could provide a pathway from creation to implementation.

A national digital evidence standard could establish common data formats and workflows across all 48 police forces, enabling secure information sharing. Interoperability standards could create common interfaces between policing, forensic and criminal justice systems, accelerating investigations.

Together, existing standards and a development programme would ensure standards are adopted and deliver benefits. This programme will create a policing ecosystem capable of addressing multiple challenges across the Problem Book.

To find out more, visit our website, or contact us.

The CIS platform is currently being enhanced to include proactive social media monitoring, this functionality is being developed based on feedback from existing customers and is scheduled to be GA by the end of 2026.

To find out more, visit our website or contact us.

CIVICA

Six of the NPCC's 13 identified problems — spanning public contact, cross-force data sharing, offender monitoring, online child sexual exploitation, workforce protection, and innovation/strategic foresight — share a common structural cause: fragmented, unreconciled data about the same people, places, cases and equipment held across 48 independent systems.

The case made here is not that Master Data Management (MDM) solves policing's 13 problems. It is that six of them are, in part, the same problem — and that solving it once, doing it well, is worth significantly more than solving it 48 times separately.

A modern MDM platform does not solve every dimension of these problems on its own, however, MDM addresses the shared root cause running underneath most of them: the inability to reliably tell that a record in one system and a record in another refer to the same real-world person, case or thing.

Given the scale and sensitivity of the data involved — particularly for Problem 5 — we would suggest that any move to trial this approach begin as a bounded pilot, evaluated through the kind of national testing sandbox described in the Problem 13 section above, rather than a single national rollout.

For further descriptions of the value from MDM to Problem Statement 5, visit our dedicated page or contact us.

MAGNET FORENSICS®

Many of the most pressing challenges facing law enforcement today are connected by a common reality: digital evidence now underpins most investigations.

Magnet Forensics helps police forces modernise the full digital investigation lifecycle. Its digital forensics solutions support the lawful acquisition, processing, analysis, review and sharing of evidence from mobile devices, computers, cloud services, vehicles, video and other digital sources.

For investigations involving large volumes of images and video, including online child sexual exploitation and terrorism, Magnet Griffeye helps teams identify, categorise and prioritise relevant material. This accelerates the search for victims and offenders while reducing investigators' repeated exposure to harmful content.

With digital evidence becoming increasingly prone to alteration, Magnet Verify can help confirm the authenticity of files by examining the digital structure to determine whether they have been changed.

Across these workflows, trusted AI and automation help teams surface relevant evidence, recognise connections and focus specialist time where it can have the greatest impact.

By connecting people, processes, and technology, Magnet Forensics helps address key policing challenges related to digital evidence, shortening the path from evidence to action, and delivering more efficient, transparent, and trusted outcomes for victims, communities, and the justice system.

To find out more, visit our website or contact us.

ROKE

Roke's Vigil AI helps protect vulnerable children by rapidly detecting and categorising illegal imagery. Already trusted across most UK forces, it integrates easily and surpasses hash-matching to triage at machine-speed and automatically detect unknown material. Free licences available for UK forces.

To find out more, visit our website or contact us.

SHORENET

Shorenet is a UK evidence technology company. Our desktop application captures web-based evidence in a form that can be verified by anyone, without trusting the officer's machine or Shorenet.

Screenshots, screen recordings and saved pages record what an officer's screen displayed. They do not prove what the server actually served, which places the officer's own device inside the chain of proof. Our capture engine instead records the encrypted network session at OS level and preserves the server's own TLS authentication tags. A relay operated separately from the investigating party then witnesses the ciphertext in transit, holding no decryption keys and seeing no plaintext, so the record is witnessed off the collecting device before that device could have authored it. We call this the Unwitting Witness®. The sealed bundle is timestamped by an independent RFC 3161 authority and signed with both post-quantum (ML-DSA-87) and classical (Ed25519) algorithms.

Against statement 5, this answers synthetic content evidentially rather than by detection: section 66B of the Sexual Offences Act 2003, as amended by the Online Safety Act 2023, asks whether an image appears to show the person, not whether it is real, so the gap is provenance of capture, not detection of content. There is also a wider need to evidence material published on platforms.

Shorenet is pre-deployment. We are seeking a law enforcement unit to host an evaluation.

To find out more, visit our website or contact us.

TENACIUM DC

There are 43 territorial police forces in England and Wales—and 48 UK-wide when non-territorial forces are included. Each is an independent data controller with different systems, suppliers and recording practices.

A police data exchange succeeds only when the recipient can establish where information came from, how safely it can be used and whether it is relevant to the task.

This matters when determining whether information held elsewhere concerns the same person, location, vehicle or event. The national audit of group-based child sexual exploitation and abuse found that some forces use around 100 systems, alongside uneven

Police National Database access and uploads. More records alone cannot resolve differences in meaning, identifiers, currency, confidence or handling.

The National Data Integration and Exploitation Service and National Policing Digital Strategy are strengthening APIs, standards, identity and governance.

AI raises the stakes. Applied to fragmented or poorly contextualised information, it can accelerate retrieval while amplifying weak matches, stale assumptions and opaque reasoning. Forces need foundations that preserve meaning, evidence, permissions, human review and correction.

A “context contract” would help authorised recipients answer five questions:

1. What does this information mean?
2. Where did it come from?
3. When was it observed or verified?
4. How confidently does it relate to the current person, object or event?
5. What may the recipient do with it?

Tenacium has demonstrated multi-source refinement, semantic cataloguing, graph-based context and evidence-linked investigation in prototypes. We propose testing these patterns using synthetic or de-identified policing data, without replacing authoritative sources or national services.

This is not another platform. It tests whether information remains understandable, contestable and evidence-linked.

To find out more, visit our website or contact us.

6. How can policing build and maintain public trust through fair, transparent, and accountable practices?

Inconsistent approaches to disproportionality, victim support, and the needs of vulnerable groups, have undermined public confidence in policing and the justice system. The following solutions seek to standardise and visualise disproportionality data and help track victim and witness support against the Victims' Code of Practice.

Primary Service Lines: *Personal Safety, Analytics*

The rapid growth of digital evidence, AI, and technology-enabled crime are creating significant challenges for UK policing. There is a common need for secure data sharing, interoperability and digital capability.

A range of internationally recognised standards provide a foundation for digital policing. ISO/IEC 27001 supports the secure management of information. ISO/IEC 27037 provides guidance on the identification, collection and preservation of digital evidence, while ISO/IEC 42001 supports the responsible governance of AI systems. ISO/IEC 27701 strengthens privacy and the secure handling of personal data.

Beyond existing standards, BSI is developing a Digital Product Safety Standard to help prevent online harms and technology-enabled crime. Emerging digital and AI literacy standards will help define skills for a modern police service.
To maximise impact, policing requires more than individual standards. A coordinated standards programme could provide a pathway from creation to implementation.

A national digital evidence standard could establish common data formats and workflows across all 48 police forces, enabling secure information sharing. Interoperability standards could create common interfaces between policing, forensic and criminal justice systems, accelerating investigations.

Together, existing standards and a development programme would ensure standards are adopted and deliver benefits. This programme will create a policing ecosystem capable of addressing multiple challenges across the Problem Book.

To find out more, visit our website, or contact us.

Dataminr's AI platform continuously scans over 1 million public data sources in real time, using Multi-Modal Fusion AI, generative AI, and agentic AI to detect physical and cyber events, threats, and risks as they unfold. This real-time intelligence layer underpins both strategic digital transformation of public contact, adds stronger protection for the workforce delivering it and builds public trust. First Alert and Dataminr for Cyber Defence are cloud-based SaaS services delivered on a subscription model that integrates into clients' existing workflows rather than requiring new on-premise infrastructure. This means data is hosted, structured, and secured within established cloud architecture, with capacity and access managed centrally rather than left to fragmented local systems.

Strategic digital transformation for public contact: Dataminr replaces slow, manual monitoring of incoming information with an efficient 24/7/365 automated, AI-corroborated alerting. This capability provides control rooms, contact centres and intelligence teams with early context on public safety incidents and emergencies so forces can better respond before and after arriving on scene. Building public trust through fair, transparent, accountable practices: Dataminr's public-data-only input limits exposure on data protection and privacy grounds; the system does not require access to classified or citizen personal data mitigating need for surveillance authorities. It validates every alert through a multi-layered approach that automatically corroborates patterns across multiple sources and modalities before an alert is issued, rather than relying on a single subjective source. The system surfaces alerts for human responders — it does not take autonomous action.

To find out more, visit our website or contact us.

Davidhorn

Advancing Investigative Interview Excellence Through Digital Innovation

With over 40 years of experience, Davidhorn is the UK's leading provider of evidential interview recording and productivity solutions, directly supporting the National Policing Digital Strategy 2025-2030's mission to enable officers and staff through modern digital tools.

Our interview recording solution addresses critical strategic priorities: modernising core investigative technology, automating administrative processes to free officers for frontline duties and investigative work, and ensuring high-quality data capture for analytics-driven policing. By replacing legacy recording systems with interoperable, cloud-ready solutions, we help forces reduce complexity and costs while maintaining the highest evidential standards.

Davidhorn's technology streamlines the entire interview process, from secure digital recording to efficient case file preparation, enabling investigators to focus on outcomes rather than administration. With integrations to major UK Records Management Systems (RMS) and Digital Evidence Management Systems (DEMS), we deliver the connected technology vision central to the strategy, ensuring seamless data sharing across forces and criminal justice partners.

As committed partners to UK law enforcement, we deliver scalable, sustainable solutions that protect the public through more efficient, effective investigations.

To find out more, visit our website or contact us.

---

innov8law

Public-sector organisations already hold many of the warning signals of tomorrow's failures: complaints, incidents, claims, misconduct, workforce pressures, financial losses, poor outcomes and declining public trust. Too often, those signals are considered separately.

innov8law Haemostasis™ is a cross-government methodology designed to help leaders connect those signals, identify where organisational harm is developing, quantify its human, social and economic impact, diagnose root causes and intervene before harm and cost escalate.

The methodology follows six stages: Target → Structure → Quantify → Diagnose → Intervene → Make the Case.

Its configurable Haemostasis Scorecard™ provides an early-warning and decision-support architecture through which different public services can select relevant indicators while retaining a common framework based on Human Value, Social Value and Economic Value.

For policing, Haemostasis™ could bring together indicators including complaints, victim experience, misconduct, workforce information, operational data, legal and financial exposure and public-confidence measures. The objective is not another complaints system, but better organisational intelligence: identifying patterns, understanding the true cost of the bleed, prioritising intervention and measuring whether action has reduced harm.

The methodology is being developed through real-world public-sector problem solving. An initial University of Reading consultancy demonstrator has applied Haemostasis™ to NHS maternity services, exploring how fragmented evidence can become board-level risk intelligence, cost-of-failure analysis and strategic recommendations.

innov8law now proposes applying this cross-government architecture to policing, supporting Problem 6.

Stop Harm. Repair Damage. Rehabilitate Systems.

To find out more about Haemostasis™, visit our website or contact us.

Kahootz provides secure workspaces for sharing information and coordinating work across organisational boundaries. Authorised participants can access current documents, discuss issues, manage tasks, record decisions and maintain an auditable history of activity in one shared workspace.

This is relevant to policing because forces increasingly need to collaborate with other forces, national bodies, suppliers and community or specialist partners. Kahootz can provide a single source of truth for this work, reducing reliance on email attachments, disconnected shared drives and informal channels. Its features include configurable access permissions, document version control, review and approval workflows, task management and audit trails.

Kahootz is already used in sensitive public-sector collaboration across government, including through Defence Share, the Ministry of Defence's primary collaboration tool. Powered by Kahootz, Defence Share enables the MOD to share information classified up to OFFICIAL-SENSITIVE with defence industry partners, other government departments, agencies and allied nations. It provides geographically distributed participants with secure workspaces for accessing information and collaborating on complex programmes.

The same principles could support policing collaboration while complementing, rather than replacing, core operational systems and information-governance processes. Kahootz can support problem statement 6 through recorded activity, document history and decision records.

To find out more, visit our website or contact us.

Made Tech worked with the Ministry of Justice on the Victim Pathfinder project to explore how data and digital services could improve victims' experiences in the criminal justice system.

The work exposed a fundamental challenge. Victim information is held across police forces, the Crown Prosecution Service, HMCTS, and other agencies, but it does not flow easily between them. Legacy systems are secure in isolation, creating silos that prevent staff from accessing a trusted, up-to-date view of a case and leave victims unsure of what is happening.

Rather than just documenting the problem, the Pathfinder used live delivery to test how boundaries could be overcome. The team developed a victim-facing Track My Case service, giving people clear information on where and when their case would be heard, alongside guidance and support. They also worked with HMCTS to create a lightweight API exposing court data in a reusable form, extending value beyond the Pathfinder itself.

The product strategy connected user-facing services and reusable platform components around accurate, shared data. The goal was to reduce duplicated administration, free staff to focus on those needing support, and provide victims with timely, transparent information. These principles address wider policing challenges, such as community-based offender management, drawing on our discovery work into VCMS and Victim Liaison Officers, where staff need secure access to cross-agency information.

The Pathfinder showed that solving local problems with isolated technology deepens national fragmentation. Reusable components, common data standards, and secure data-level access enable joined-up services without weakening controls. The research, learning, and code remain available to build on, offering a tested foundation for criminal justice services that are more efficient, transparent, and capable of strengthening public trust.

To find out more, visit our website or contact us.

principleone

Synthetic data reproduces the structure, patterns and relationships found in real police data but includes no sensitive or personal information

Principle One brings synthetic data to life by applying it to real-world operational scenarios. Our outputs include communications data, ANPR, digital forensic material, financial data, crime reports or intelligence records

Why it's necessary
Police data is highly sensitive and often difficult to access for research, development and testing. Using live operational data creates privacy, access and governance risks.

Principle One's synthetic data creates a safe, controllable alternative. It allows realistic datasets to be generated without exposing victims, witnesses or officers, while still maintaining the complexity, links and imperfections of real operational information

What it enables
Synthetic data enables development and vigorous testing of new and emerging policing technologies. It can be used to expose knowledge gaps, software issues and improve functionality. It can also be used to gamify investigative scenarios to make training environments more immersive, and to build 'digital twins' of systems or organisations to develop AI

The benefits
Synthetic data makes innovation easier, safer and faster. It allows police forces and suppliers to develop, test and train using realistic data without exposing personal information. It can be generated at scale, reused consistently and tailored to include complex or rare scenarios that may be missing from live datasets. It also supports safer collaboration, better training and helps tools and approaches to be tested before they are introduced operationally.

To find out more, visit our website or contact us.

Telefónica Tech

Telefónica Tech's Predictive Policing Accelerator, built on Databricks, helps police forces move from reactive reporting towards more proactive, intelligence-led policing. The solution brings together data from multiple policing systems into a single governed platform, providing a real-time view of crime, emerging trends, demand and harm-based priorities. Geospatial analytics helps identify hotspots and patterns, while AI-generated insights support earlier identification of emerging risks and more targeted operational responses.

Integrated with Databricks Genie, the accelerator also enables officers, analysts and operational leaders to explore governed policing data using natural language, without relying on specialist technical skills or predefined reports. Users can investigate trends, drill into patterns and answer operational questions more quickly, helping translate data into actionable intelligence at the point of need. This supports better resource allocation, more targeted prevention activity and more informed decision making.

The approach is designed around responsible AI, with governance, transparency and human oversight embedded into the platform. This enables predictive insight to support professional judgement rather than replace it, helping forces adopt AI in a way that is accountable and aligned with policing principles.

To find out more, visit our website or contact us.

UMNAI

Public trust depends on policing being able to provide a clear, reliable account of decisions that affect people: what informed them, why an action was chosen, whether and why it was permitted, and who held authority.

UMNAI provides governed Decision Intelligence: an AI system built on Hybrid Intelligence, its purpose-built neuro-symbolic architecture for forming, controlling and improving decisions. It is designed for decisions such as identifying and stratifying risk, prioritising cases, escalating safeguarding concerns, increasing monitoring or deciding what, if any, further action is proportionate. For each decision, the practitioner sees the source records and signals supporting the recommendation, which information is established or inferred, why one action is preferred, any missing or conflicting evidence and what changes would alter the result. The force's operational policies, legal requirements, evidence thresholds and human-defined authority limits determine which actions are permitted, what evidence is required and who must approve them.

The practitioner retains control: approving, changing or rejecting the recommendation and recording the reason. UMNAI's Evidence Vault preserves all evidence available at the time, the reasoning applied, policy versions, system recommendations, practitioner judgement and action taken.

The result is a deterministic, replayable decision record answering five essential questions: What did we know? Why did we act or decide not to? Were we permitted to act? Who made the decision? What happened next?

Decision Intelligence operates within the police-controlled environment, without reliance on LLMs or external foundation-model services. Operational data, policies, models, accumulated knowledge and decision records remain under the force's sovereign control.

To find out more, visit our website or contact us.

Yoono is a Channel Islands Headquartered AI intelligence platform. It helps organisations make better, faster and more defensible decisions about people, entities and networks. The platform is particularly relevant where decisions are high consequence, who to do business with, who to onboard, who to investigate further, who is connected to whom, where risk may sit, and whether the available information supports a decision.

Yoono brings together identity, risk, reputation, relationships and public-source intelligence into one structured view. The aim is not just to give users more information, but to help them understand what matters, why it matters, and how a decision can be explained and defended later.
That is particularly important in regulated and high accountability environments. In financial services, law enforcement, defence and government, it is no longer enough simply to say that checks have been completed. Organisations increasingly need to show that they have understood the evidence, considered the risk, and reached a decision in a consistent and auditable way.

The platform has clear relevance to law enforcement, investigations, defence, government, intelligence workflows, public sector risk assessment and national security relevant use cases. Public sector organisations face many of the same issues as financial institutions, but often with greater

sensitivity and consequence; fragmented information, complex networks, reputational risk, operational urgency, and decisions that may need to be explained long after the event.

Potential Police Use Cases include Recruitment & Vetting, investigative intelligence, serious and organised crime support, subject and associate assessment, network analysis, ownership and corporate structure analysis, public-source (OSINT) intelligence reporting, supplier and third-party risk, asset recovery intelligence, operational briefing support, and governance or assurance work. The platform can be used to compliment various aspects of the 'Police Problem book', where keeping the public safe is concerned. Yoono will decrease the intelligence gap for Policing regarding subjects of investigations and vetting concerns, by expediting and improving their effectiveness.

To find out more, visit our website or contact us.

7. How can policing responsibly deploy surveillance technologies by ensuring timely activation, ethical use, and public trust through robust legal and privacy frameworks?

Body-worn video, facial recognition, and CCTV offer significant investigative and safety benefits, but manual activation, legal constraints on automation, and public concern over bias and privacy have limited their effective and trusted use. Below, techUK members present solutions that enable context or voice-triggered activation, embed ethical frameworks for facial recognition, and introduce safe automation into CCTV handling.

Primary Service Lines: *Surveillance & Sensing, Analytics*

Augur exists to protect people where they live, work, travel and gather.

The threat to public safety is growing faster than existing security services can respond. There is strong mission alignment between Augur and UK Policing; we have prioritised three Problem Book statements where Augur can have immediate, tangible impact:

Augur is a software layer that integrates with existing CCTV and sensor infrastructure, transforming passive surveillance into real-time intelligence. Using advanced AI and ML, the system builds a three-dimensional understanding of space and how people move and interact within it.

Human operators remain the decision-makers; Augur surfaces insights at a scale and speed no human team could, enabling faster intervention. All processing operates within UK GDPR. Access is strictly role-based, with every action logged and auditable. Facial recognition, where necessary and legally proportionate, can be applied in use cases relevant to the PPB challenges.

To find out more, visit our website or contact us

Real-Time Situational Awareness for Officer Safety helps protect officers and improve operational decision-making by giving command centres real-time visibility of frontline risks, welfare concerns, and emerging incidents. It replaces fragmented radio updates and delayed reporting with continuous, actionable intelligence.

Using approved wearables and mobile devices, the platform provides real-time officer safety and welfare monitoring, location awareness, and automatic detection of distress events. It can identify falls, panic activations, weapon deployment, and signs of escalating situations. Sensitive data is processed securely on the device, ensuring only relevant insights are shared with supervisors and control rooms. This enables faster intervention, intelligent deployment, and improved coordination of personnel and assets. SITREP AI maintains resilient communications when conventional networks fail through a mesh network operating across cellular, Wi-Fi, and satellite networks. This ensures a persistent operational picture during major incidents, public events, rural deployments, and in areas with poor signal coverage.

The platform also identifies patterns associated with escalating risk, helping supervisors prioritise alerts, allocate resources effectively, and make informed decisions in rapidly changing operational environments.

As adoption matures, SITREP AI evolves from delivering situational awareness to providing operational insight and decision support, helping forces move from reacting to incidents to anticipating operational risk.

To find out more, visit our website or contact us.

OPSWAT.

The Policing Problem Book identifies digital evidence capture and analysis (Problem 1), Digital Public Contact transformation (Problem 2), and secure data sharing across forces (Problem 3) as central challenges. Underlying all three is one question: as forces digitise contact, evidence and case management, who checks that every file entering the estate can be trusted?

MetaDefender is built on a zero trust principle. A firewall or VPN controls who can reach a system, but says nothing about whether the file they bring is safe. Encryption does not solve this either: an encrypted attachment or upload can still carry malware, since encryption protects a file in transit, not its content.

MetaDefender inspects, sanitises and rebuilds files at every point they cross into policing environments: crime reporting portals, email attachments, and USB, CCTV and bodycam footage collected in the field or moved between forces and to the CPS. Deep CDR and multiscanning remove hidden threats while preserving evidential integrity and chain of custody.

An “ingest once, share with many” approach means evidence is checked once, then moved across systems with a full audit trail, cutting manual triage and supporting the standardisation the Problem Book calls for.

UK police forces already run OPSWAT in live operation, on file upload portals, email gateways and frontline evidence handling.

To find out more, visit our website or contact us.

Digital evidence is fundamental to modern policing, but growing volumes create bottlenecks that can slow investigations.

Problem Statement 7 asks about responsible surveillance technologies - but responsible use doesn't end when the camera stops recording. The resulting footage must remain protected, auditable and capable of being used lawfully, ethically and transparently. Working with police forces, national policing stakeholders and the Home Office, Pimloc develops privacy-first technology with policing, not simply for policing—reducing manual workload while helping evidence reach the people who can unlock its value. Because digital evidence only creates value when it moves—from capture, to intelligence, to investigation, to disclosure and, ultimately, to justice.

To find out more, visit our website or contact us.

Roke's LUCID enables video analysis at the edge (without upload), thus aiding privacy and rapid response. By applying obfuscated watchlists to facial recognition, it detects threats while minimising privacy impact. LUCID is deployed on devices from CCTV to smartphones, suiting many policing requirements.

To find out more, visit our website or contact us.

The NPCC Policing Problem Book outlines 13 critical challenges, emphasizing the need for data integration, digital trust, and operational efficiency. The Splunk Metropolitan Police (Met) case study serves as a direct response to these hurdles, demonstrating how a unified data platform transforms policing from reactive to proactive.

The Problem Book also emphasizes "Digital Trust" and ethical data use. The Met case study highlights a significant shift in internal governance; by using Splunk, the Met identified 298 Connect ICT breaches and 149 technical breaches in just one year. This capability allows the force to proactively detect unauthorized access and system misuse, directly answering the NPCC's call for enhanced accountability and the protection of sensitive public data.

In summary, the Met's use of Splunk provides a blueprint for the NPCC's vision. It proves that by treating data as a strategic asset, police forces can strengthen public trust, eliminate technical silos, and achieve the operational agility necessary for modern law enforcement.

To find out more, visit our website or contact us.

Vizgard is a UK sovereign visual AI company. Our software turns cameras and drones that forces already operate into autonomous teammates, cutting operator workload and speeding up threat detection while keeping a human on the loop. Our flagship product, FortifAI, is a TRL 9 platform that adds real-time visual intelligence and automated camera control to existing infrastructure.

FortifAI automates steerable long-range visible and thermal cameras, running intelligent guard tours, slewing to radar or RF cues, and geolocating people and vehicles at distance. Detection runs on-device, so sensitive footage stays local and GDPR-aligned, and every alert is put to an operator for review rather than acted on automatically. One operator can supervise a wide camera estate without adding staff.

Vizgard has delivered for the UK MOD, Home Office and defence primes, including safeguarding the perimeter of a major international airport. The platform is open architecture, so forces can run their own models and keep full control of their data.

To find out more, visit our website or contact us.

Yoono is a Channel Islands Headquartered AI intelligence platform. It helps organisations make better, faster and more defensible decisions about people, entities and networks. The platform is particularly relevant where decisions are high consequence, who to do business with, who to onboard, who to investigate further, who is connected to whom, where risk may sit, and whether the available information supports a decision.

Yoono brings together identity, risk, reputation, relationships and public-source intelligence into one structured view. The aim is not just to give users more information, but to help them understand what matters, why it matters, and how a decision can be explained and defended later.

That is particularly important in regulated and high accountability environments. In financial services, law enforcement, defence and government, it is no longer enough simply to say that checks have been completed. Organisations increasingly need to show that they have understood the evidence, considered the risk, and reached a decision in a consistent and auditable way.

The platform has clear relevance to law enforcement, investigations, defence, government, intelligence workflows, public sector risk assessment and national security relevant use cases. Public sector organisations face many of the same issues as financial institutions, but often with greater sensitivity and consequence; fragmented information, complex networks, reputational risk, operational urgency, and decisions that may need to be explained long after the event.

Potential Police Use Cases include Recruitment & Vetting, investigative intelligence, serious and organised crime support, subject and associate assessment, network analysis, ownership and corporate structure analysis, public-source (OSINT) intelligence reporting, supplier and third-party risk, asset recovery intelligence, operational briefing support, and governance or assurance work. The platform can be used to compliment various aspects of the 'Police Problem book', where keeping the public safe is concerned. Yoono will decrease the intelligence gap for Policing regarding subjects of investigations and vetting concerns, by expediting and improving their effectiveness.

To find out more, visit our website or contact us.

8. How can policing design out the opportunities for criminal activity emerging from synthetic content, connected vehicles, and smart technologies?

Emerging technologies, from deepfakes (which have seen a sixfold rise in non-consensual synthetic imagery) to e-bikes, connected vehicles, and smart home devices, are creating new and fast-moving criminal opportunities. The solutions presented here identify tech-enabled crime hotspots, and detect synthetic content in real time.

Primary Service Lines: *Crime Prevention, Analytics*

ROKE

Roke conducts hands-on research on tech-enabled crime. We have developed automated covert identification of IoT devices; produced solutions to forensically analyse synthetic content; and perform cyber security analysis on our connected vehicle. We help policing understand and address criminal exploitation of emerging technologies.

To find out more, visit our website or contact us.

SHORENET

Shorenet is a UK evidence technology company. Our desktop application captures web-based evidence in a form that can be verified by anyone, without trusting the officer's machine or Shorenet.

Screenshots, screen recordings and saved pages record what an officer's screen displayed. They do not prove what the server actually served, which places the officer's own device inside the chain of proof. Our capture engine instead records the encrypted network session at OS level and preserves the server's own TLS authentication tags. A relay operated separately from the investigating party then witnesses the ciphertext in transit, holding no decryption keys and seeing no plaintext, so the record is witnessed off the collecting device before that device could have authored it. We call this the Unwitting Witness®. The sealed bundle is timestamped by an independent RFC 3161 authority and signed with both post-quantum (ML-DSA-87) and classical (Ed25519) algorithms.

Against statement 8, this answers synthetic content evidentially rather than by detection: section 66B of the Sexual Offences Act 2003, as amended by the Online Safety Act 2023, asks whether an image appears to show the person, not whether it is real, so the gap is provenance of capture, not detection of content.

Shorenet is pre-deployment. We are seeking a law enforcement unit to host an evaluation.

To find out more, visit our website or contact us.

Telefónica Tech's Predictive Policing Accelerator, built on Databricks, helps police forces move from reactive reporting towards more proactive, intelligence-led policing. The solution brings together data from multiple policing systems into a single governed platform, providing a real-time view of crime, emerging trends, demand and harm-based priorities. Geospatial analytics helps identify hotspots and patterns, while AI-generated insights support earlier identification of emerging risks and more targeted operational responses.

Integrated with Databricks Genie, the accelerator also enables officers, analysts and operational leaders to explore governed policing data using natural language, without relying on specialist technical skills or predefined reports. Users can investigate trends, drill into patterns and answer operational questions more quickly, helping translate data into actionable intelligence at the point of need. This supports better resource allocation, more targeted prevention activity and more informed decision making.

The approach is designed around responsible AI, with governance, transparency and human oversight embedded into the platform. This enables predictive insight to support professional judgement rather than replace it, helping forces adopt AI in a way that is accountable and aligned with policing principles.

To find out more, visit our website or contact us.

TJA Associates offers a practical, outcome-led solution to Problem 8. Its core proposition is that policing should not treat data, innovation, emerging technology and mobility as separate issues, but as connected operating-model challenges that require governance, collaboration, evaluation and business change as much as technical capability.

TJA brings a prevention-by-design approach to synthetic content, connected vehicles and smart technologies, helping policing anticipate criminal exploitation, map threat scenarios, clarify requirements and build proportionate governance before risks scale.

TJA's product/case-study offer is not a single technology platform; it is a structured consultancy and delivery approach that helps NPCC and partner organisations define the problem, convene the right stakeholders, shape operating models, translate complex data

into actionable intelligence requirements, manage delivery and measure benefits. This means TJA can address many Problem Book challenges where the barriers are interoperability, trust, evidence quality, public confidence, supplier engagement, governance and adoption. Find out more at TJA Associates.

To find out more, visit our website or contact us.

Vizgard

Vizgard is a UK sovereign visual AI company. Our software turns cameras and drones that forces already operate into autonomous teammates, cutting operator workload and speeding up threat detection while keeping a human on the loop. Our flagship product, FortifAI, is a TRL 9 platform that adds real-time visual intelligence and automated camera control to existing infrastructure.

The same person, vehicle, weapon and behaviour analysis supports proactive perimeter and event security, flagging risk at large public gatherings and critical sites before incidents escalate.

Vizgard has delivered for the UK MOD, Home Office and defence primes, including safeguarding the perimeter of a major international airport. The platform is open architecture, so forces can run their own models and keep full control of their data.

To find out more, visit our website or contact us.

---

9. How can police enhance its capability to investigate and prevent cybercrime by developing specialist skills, tools, and partnerships to address threats such as malicious communications, dark web activity, and digital stalking?

Cybercrime is rising sharply, with most domestic abuse cases now involving a digital or cyber element such as spyware or GPS trackers, alongside growing dark web and cryptocurrency-related offending. The solutions below seek to propose ways to detect and block malicious communications before they reach victims, support safe dark web and crypto investigation, and rapidly upskill officers.

Primary Service Lines: *Crime Prevention, Surveillance & Sensing*

Videris, from Blackdot Solutions, is a secure OSINT investigations platform originally built for the UK intelligence community and now used widely across UK policing, defence and financial crime teams. It pulls together over 200 data sources, including the surface, deep and dark web, social media, corporate records, and sanctions and PEP lists, plus any custom or internal data connected via API, into a single case. From there, automated link analysis charts networks and surfaces connections that would otherwise take hours to find manually.

As one UK policing user described it: "I'd describe Videris as an ever evolving powerful secure online investigative platform, enabling users to identify online accounts and commercial data with the capability to extensively map and visualise a network of people, companies, addresses, and identifiers. It also features a closed AI feature enabling complex network data returns to be queried to help explain how certain entities are linked in the data."

Problem 9 (cybercrime investigation capability): Videris gives investigators safe, secure access to the open, deep and dark web, including high-risk forums and Telegram, alongside sources already familiar to policing such as Companies House, the electoral roll and sanctions data. Bringing these together in one place supports investigations into malicious communications, dark web marketplaces and digital stalking by mapping criminal networks end to end. Videris is UKSV-cleared for trusted support, Cyber Essentials Plus and ISO 27001 accredited, and available via G-Cloud.

To find out more, visit our website or contact us.

Cybercrime is no longer a specialist issue operating at the edge of policing. It now underpins a growing proportion of criminality, from fraud, exploitation and harassment through to organised crime and threats against critical national infrastructure. The challenge is compounded by the pace of change. Equally important is the ability to collaborate effectively across forces and with government, industry and academia. No single organisation can maintain a complete picture of an increasingly complex and fast-moving threat landscape. For BT, this challenge reflects a reality we see every day. As policing considers the adoption of emerging technologies such as AI, ensuring sensitive data remains appropriately protected, governed and, where necessary, processed within trusted UK sovereign environments will become an increasingly important consideration.

To find out more, visit our website or contact us.

Dataminr's AI platform continuously scans over 1 million public data sources in real time, using Multi-Modal Fusion AI, generative AI, and agentic AI to detect physical and cyber events, threats, and risks as they unfold. This real-time intelligence layer underpins both strategic digital transformation of public contact, adds stronger protection for the workforce delivering it and builds public trust. First Alert and Dataminr for Cyber Defence are cloud-based SaaS services delivered on a subscription model that integrates into clients' existing workflows rather than requiring new on-premise infrastructure. This means data is hosted, structured, and secured within established cloud architecture, with capacity and access managed centrally rather than left to fragmented local systems. Strategic digital transformation for public contact: Dataminr replaces slow, manual monitoring of incoming information with an efficient 24/7/365 automated, AI-corroborated alerting. This capability provides control rooms, contact centres and intelligence teams with early context on public safety incidents and emergencies so forces can better respond before and after arriving on scene. Building public trust through fair, transparent, accountable practices: Dataminr's public-data-only input limits exposure on data protection and privacy grounds; the system does not require access to classified or citizen personal data mitigating need for surveillance authorities. It validates every alert through a multi-layered approach that automatically corroborates patterns across multiple sources and modalities before an alert is issued, rather than relying on a single subjective source. The system surfaces alerts for human responders — it does not take autonomous action.

To find out more, visit our website or contact us.

Roke delivers data science and intelligence capabilities that help law enforcement identify, investigate and prevent cybercrime. Working directly with mission teams, we develop and operationalise ML, analytics and OSINT solutions. We combine specialist expertise, trusted partnerships and operational delivery to enhance mission outcomes.

To find out more, visit our website or contact us.

Shorenet is a UK evidence technology company. Our desktop application captures web-based evidence in a form that can be verified by anyone, without trusting the officer's machine or Shorenet.

Screenshots, screen recordings and saved pages record what an officer's screen displayed. They do not prove what the server actually served, which places the officer's own device inside the chain of proof. Our capture engine instead records the encrypted network session at OS level and preserves the server's own TLS authentication tags. A relay operated separately from the investigating party then witnesses the ciphertext in transit, holding no decryption keys and seeing no plaintext, so the record is witnessed off the collecting device before that device could have authored it. We call this the Unwitting Witness®. The sealed bundle is timestamped by an independent RFC 3161 authority and signed with both post-quantum (ML-DSA-87) and classical (Ed25519) algorithms.

Against 9, it applies directly to malicious communications, digital stalking and dark web activity, where the material sits on a platform rather than a seized device.

Shorenet is pre-deployment. We are seeking a law enforcement unit to host an evaluation.

To find out more, visit our website or contact us.

10. How can policing develop a digitally empowered, data literate and innovative workforce to meet the demands of modern, intelligence-led policing?

Intelligence-led, data-driven policing demands a workforce with strong digital and data science skills at every level, including leadership, but policing has lacked a structured, scalable national CPD framework to close this gap. The solutions showcased here offer tools to assess and visualise digital skills gaps, and leadership programmes that build strategic digital fluency.

Primary Service Lines: *Identification & Tracing, Analytics*

Actr-AI uses AI simulation to assess how policing professionals perform in realistic, complex situations, generating evidence of competency and actionable insight into organisational capability. Our technology is currently being implemented within North Wales Police, and we are also working within the Prison Service.

Rather than testing what people know, Actr-AI captures what they do. Professionals interact with realistic AI role players and are assessed against established best practice, practitioner expertise and, where appropriate, victim-survivor perspectives. This provides evidence of how effectively they communicate, gather information, identify risk, apply policy and exercise professional judgement, while giving individuals a safe environment in which to develop their capability and confidence.

Every interaction generates structured data. At an individual level, this identifies strengths and areas for development. At an organisational level, aggregated data reveals patterns of practice, capability gaps and emerging areas of risk that may otherwise remain invisible. This gives leaders an evidence base for understanding workforce capability and how their organisation responds to complex problems.

This is particularly valuable in areas such as domestic abuse and technology-assisted child sexual abuse, where situations are complex and prone to risk being missed. Actr-AI combines AI, data, specialist practitioner expertise and victim-survivor insight to build a deeper understanding of both the problem and how the workforce responds to it.

The result is a continuous evidence loop: simulate, assess, measure, understand and improve.

Our vision is to extend this capability beyond assessment into SME-informed decision support and case review, using the knowledge and evidence generated through the platform to support better-informed professional decisions while retaining human judgement and accountability.

To find out more, visit our website or contact us.

Policing is digital. 90% of reported crime has a digital component, rising as AI reshapes both criminal activity and intelligence-led policing. Whilst PoliceAI, the Police STAR Fund and other recent investments are critical, the National Policing Digital Strategy 2025-2030 is clear - technology alone will not close capability gaps. Limited role clarity, low digital literacy and fragmented change management constrain digital transformation and the development of in-house expertise.

The real challenge, then, is people, not platforms. Five priorities emerge when building a digitally-empowered police force: Assess digital and data capability alongside potential, defining clear digital expectations. At the same time, test and recruit for enduring strengths that are resilient to digital advances, such as communication and critical thinking.

Embed learning into the flow of operational delivery and digital investigation, blending modular content, immersive experiences, and personalisation to build digital confidence and data literacy as technology evolves.

Make AI, data and digital leadership everyone's responsibility - top-level learning is about cultivating a common language around data and AI, unlocking organisational value, and role-modelling ethical judgement.

Create safe spaces for innovation, encouraging participation, intelligent failure, and inclusivity to shift culture and ways of working. Improve interoperability through people, building vision, standards, and implementation experience across academia, agencies and industry partners.

Read here how Capgemini supports the UK public safety sector to become more digital, or contact us.

Policing cannot deliver intelligence-led services without a workforce that is digitally confident at every level, from the officer analysing evidence to the chief officer setting strategy. Today, no national framework exists to build or measure that capability. The result is a patchwork of local training efforts, uneven digital fluency, and leaders asked to champion technology they have never seen work. We answer this from direct experience. We developed the single national platform used by Social Work England's 96,000 social workers, and our proof of concept for the College of Policing lets one integration layer serve every tool that needs it, blending

structured performance data with unstructured policy guidance in plain English. We are applying the same modular thinking today inside West Mercia Police's digital forensics case management system, where training guidance is version-controlled and built into the tools investigators already use.

That same evidence base extends to assessment, leadership and access. Our CSTTX platform uses AI to mark cyber security skills in real time, a model directly transferable to digital and data literacy.

To find out more, visit our website, or contact us.

COEUS software

PoliceBox is a nationally scalable, locally configurable Frontline Operational Platform designed to help policing modernise frontline work while making better use of existing systems.

It primarily addresses Problem Statements 3, 10 and 13: secure, efficient and standardised data sharing; a digitally empowered workforce; and embedding innovation and evaluation into policing.

PoliceBox provides a common operational layer between officers and systems such as CAD, RMS and national services. Its open, API-first architecture supports secure integration with existing and future systems without replacing systems of record.
For officers, PoliceBox brings tasks, operational information, workflows and guidance into one mobile-first experience. It works online and offline, reduces re-keying and system switching, and supports structured, auditable data capture at the point of activity.
Cecil, the PoliceBox AI-enabled operational assistant, provides procedural support using approved national and force-specific sources. It remains advisory: professional judgement stays with the officer, who authors the operational record.

This approach was evaluated with Humberside Police through the NPCC NSIB-funded Project Moriarty Test & Learn trial. Cecil achieved average scores of 4.6/5 for accuracy, 4.5/5 for relevance and 4.6/5 for usability, with responses in under 30 seconds.

To find out more, visit our website or contact us.

---

principleone

Synthetic data reproduces the structure, patterns and relationships found in real police data but includes no sensitive or personal information

Principle One brings synthetic data to life by applying it to real-world operational scenarios. Our outputs include communications data, ANPR, digital forensic material, financial data, crime reports or intelligence records

Why it's necessary
Police data is highly sensitive and often difficult to access for research, development and testing. Using live operational data creates privacy, access and governance risks.

Principle One's synthetic data creates a safe, controllable alternative. It allows realistic datasets to be generated without exposing victims, witnesses or officers, while still maintaining the complexity, links and imperfections of real operational information

What it enables
Synthetic data enables development and vigorous testing of new and emerging policing technologies. It can be used to expose knowledge gaps, software issues and improve functionality. It can also be used to gamify investigative scenarios to make training environments more immersive, and to build 'digital twins' of systems or organisations to develop AI

The benefits
Synthetic data makes innovation easier, safer and faster. It allows police forces and suppliers to develop, test and train using realistic data without exposing personal information. It can be generated at scale, reused consistently and tailored to include complex or rare scenarios that may be missing from live datasets. It also supports safer collaboration, better training and helps tools and approaches to be tested before they are introduced operationally.

To find out more, visit our website or contact us.

Public contact remains one of the most important interfaces between policing and the communities it serves. Whether through a 999 call, a 101 enquiry, an online report or another digital channel, every interaction shapes public confidence and provides valuable insight into community demand.

As demand continues to grow in both volume and complexity, many forces face a common challenge: information relating to public contact is often spread across multiple systems, teams and processes. This can make it difficult to establish a complete view of an individual's interactions, ensure staff have the context they need and provide a consistent experience for the public.

Simpson Associates has more than three decades of data and analytics experience and has worked with over 65% of UK police forces. Through this experience, we have seen that forces often already hold the information needed to improve service delivery and support decision-making. The challenge is making that information accessible, connected and actionable at the point it is needed.

A more connected approach to public contact can help forces better understand demand, improve visibility across citizen interactions and support more informed operational decision-making. It also creates opportunities to reduce effort for both staff and the public while helping build confidence in policing services.

In this article, Simpson Associates explores why connected data is becoming increasingly important to modern policing and how forces can make better use of the information they already hold to deliver better outcomes for the communities they serve.

To find out more, visit our website or contact us.

The NPCC Policing Problem Book outlines 13 critical challenges, emphasizing the need for data integration, digital trust, and operational efficiency. The Splunk Metropolitan Police (Met) case study serves as a direct response to these hurdles, demonstrating how a unified data platform transforms policing from reactive to proactive.

The NPCC highlights the need for a data-literate workforce and improved productivity. The Met implementation empowered 150 trained users to generate insights, moving away from manual audits that previously took a week. By reducing these tasks to just 10 minutes, the Met saved approximately 4,800 hours of staff time. This efficiency gain allows officers to focus on high-value frontline duties rather than administrative troubleshooting.

In summary, the Met's use of Splunk provides a blueprint for the NPCC's vision. It proves that by treating data as a strategic asset, police forces can strengthen public trust, eliminate technical silos, and achieve the operational agility necessary for modern law enforcement.

To find out more, visit our website or contact us.

Telefónica Tech

Telefónica Tech's Predictive Policing Accelerator, built on Databricks, helps police forces move from reactive reporting towards more proactive, intelligence-led policing. The solution brings together data from multiple policing systems into a single governed platform, providing a real-time view of crime, emerging trends, demand and harm-based priorities. Geospatial analytics helps identify hotspots and patterns, while AI-generated insights support earlier identification of emerging risks and more targeted operational responses.

Integrated with Databricks Genie, the accelerator also enables officers, analysts and operational leaders to explore governed policing data using natural language, without relying on specialist technical skills or predefined reports. Users can investigate trends, drill into patterns and answer operational questions more quickly, helping translate data into actionable intelligence at the point of need. This supports better resource allocation, more targeted prevention activity and more informed decision making.

The approach is designed around responsible AI, with governance, transparency and human oversight embedded into the platform. This enables predictive insight to support professional judgement rather than replace it, helping forces adopt AI in a way that is accountable and aligned with policing principles.

To find out more, visit our website or contact us.

Through the Knowledge Transfer Partnership (KTP) programme, we are working in close collaboration with Devon and Cornwall Police (DCP) to embed innovation, evaluation, and strategic foresight into its culture and operations through the use of computer and data science. The headline aim of the KTP is to improve strategic management decision making through the use of digital tools such as artificial intelligence (AI) and digital twins, and to build confidence and a culture change within DCP.

The full-time KTP Associate sits within DCP, but is employed by the University of Exeter and maintains strong links to it through close academic supervision. That embedding of a protected resource allows them to step back from immediate front-line troubleshooting and concentrate on innovation and knowledge transfer.

The position is jointly funded by DCP and Innovate UK, whose aim is to translate cutting edge research into real-world impact. But the police are no longer able to participate in KTPs and so this route to funding projects long enough to establish close collaborations and knowledge exchange is now closed.

To find out more, visit our website or contact us.

To meet the demands of modern intelligence-led policing, police forces need to overcome legacy limitations and set up strong digital foundations.

Digital empowerment is as much a tech issue as an educational one; systems don't talk to each other, there's too much manual entry, officers can't securely access/share information they need…

Not every officer needs to be a data expert. They need intuitive, user-centred tools that capture accurate data while governance/compliance is managed behind the scenes.

Empower them by redesigning services, automating workflows and removing friction. Like other public sector organisations, police deal with legacy that can't be replaced overnight. But there are ways forward.

Watch how The National Archives tackled that particular problem via this link.

And via this link you can watch how the Home Office turned around a stalled legacy project.

The biggest barrier to innovation is often culture. Adopting AI can mean navigating structural complexities – that's what our research of national security civil servants found in our recent whitepaper.

With our public sector clients, we use co-design workshops (Transformation Days) to start that culture change and de-risk innovation. These sessions bring officers and leaders together to reach alignment, rapidly prototype in safe environments, and turn ideas into a clear business case and plan.

To find out more, read our whitepaper or contact us.

11. How can policing protect its workforce and keep them safe whilst delivering an effective service to the public, now and in the future?

Rising demand, complex threats, and inconsistent systems, including a lack of national standards for uniform design and procurement, have placed growing pressure on officer safety, comfort, and wellbeing. The following solutions from techUK members aim to introduce national standards to reduce manual workload and operational risk through technology, and support improved retention and resilience.

Primary Service Lines: *Personal Safety, Mobility, Interconnectivity, Analytics*

BlackRainbow was founded by SMEs who recognised key challenges in the investigation industry and the limitations of supporting technology. We developed NIMBUS, a versatile and scalable platform built around three core pillars: Intelligence, Investigations and Forensics to streamline the entire case management lifecycle, improving efficiency, accuracy, auditability and compliance to standards and procedures. Designed for Law Enforcement, Government and Corporates, it delivers complete visibility and control through intelligence-led data, evidence tracking, automated workflows, decision making, tasking and reporting.

Already operational across UK policing, NIMBUS has unified case and quality management, reducing risk, improving interoperability, lowering manual workloads, and enhancing efficiency, cost effectiveness and staff wellbeing. Our solution addresses several problem questions, including how can policing protect its workforce and keep them safe whilst delivering an effective service to the public, now and in the future.

You can find out more through our case study, or contact us.

Six of the NPCC's 13 identified problems — spanning public contact, cross-force data sharing, offender monitoring, online child sexual exploitation, workforce protection, and innovation/strategic foresight — share a common structural cause: fragmented, unreconciled data about the same people, places, cases and equipment held across 48 independent systems.

The case made here is not that Master Data Management (MDM) solves policing's 13 problems. It is that six of them are, in part, the same problem — and that solving it once, doing it well, is worth significantly more than solving it 48 times separately.

A modern MDM platform does not solve every dimension of these problems on its own, however, MDM addresses the shared root cause running underneath most of them: the inability to reliably tell that a record in one system and a record in another refer to the same real-world person, case or thing.

For further descriptions of the value from MDM to Problem Statement 11, visit our dedicated page or contact us.

Protecting the policing workforce requires a broader definition of safety. Beyond uniform and equipment, officers need secure, reliable access to information, without fragmented systems adding delay, cognitive load, or avoidable risk. Real-time natural language access to systems, from case data to operational guidance, streamlines workflows ensuring officers have reliable information while built-in governance prevents the use of non-sanctioned tools.

A national approach provides every authorised user a consistent digital front door to applications, whether in a station, vehicle, or remote location. Cloudflare's secure workforce architecture explains how identity-led access, web protection, and application connectivity are delivered through a unified service.

The same layer protects officers from phishing and data leakage while maintaining an auditable record of every action. Resilient connectivity ensures services remain available during cyber incidents. When forces introduce AI assistants, Cloudflare's Agent Access Model enforces human oversight. Every action is authorised against the task state.

To find out more, visit our website or contact us.

Always-on in-field connectivity for frontline policing

Away from a fixed connection, an officer working alone may depend on a cellular path for intelligence checks, live video and location reporting. If that path cannot carry data, a device may continue operating locally, but information intended for transmission cannot reach force systems over that path. In-field connectivity is therefore a dependency for the mobility capabilities in this chapter. Where cellular data depends on one mobile network core, a core fault can interrupt the path even while the device remains registered and reports a usable radio signal. Signal-strength-only failover will not respond to that condition.

Exclusive to CSL, rSIM® is designed to support in-field connectivity by addressing that exposure. It holds two operator profiles on one SIM, each reaching multiple radio networks through a separate mobile network core. rSIM monitors whether data is passing from the device. If data stops for a sustained period, it can initiate a switch to the second profile without depending on the affected network to issue an instruction.

Conventional multi-network connectivity can reach alternative radio networks through one core. CSL's patented rSIM architecture adds SIM-resident failover between separate mobile network cores. Designed in the UK and launched in 2024, rSIM is used across telecare, fire and security, healthcare and payments.

CSL supports more than 3.5 million active connections and private VPN connectivity to more than 270 alarm receiving centres across Europe. This private APN and encrypted VPN architecture could support PNC queries, ANPR data and body-worn video, subject to each force's technical, security and assurance requirements.

To find out more, visit our website or contact us.

Dataminr

Dataminr's AI platform continuously scans over 1 million public data sources in real time, using Multi-Modal Fusion AI, generative AI, and agentic AI to detect physical and cyber events, threats, and risks as they unfold. This real-time intelligence layer underpins both strategic digital transformation of public contact, adds stronger protection for the workforce delivering it and builds public trust. First Alert and Dataminr for Cyber Defence are cloud-based SaaS services delivered on a subscription model that integrates into clients' existing workflows rather than requiring new on-premise infrastructure. This means data is hosted, structured, and secured within established cloud architecture, with capacity and access managed centrally rather than left to fragmented local systems. Strategic digital transformation for public contact: Dataminr replaces slow, manual monitoring of incoming information with an efficient 24/7/365 automated, AI-corroborated alerting. This capability provides control rooms, contact centres and intelligence teams with early context on public safety incidents and emergencies so forces can better respond before and after arriving on scene. Building public trust through fair, transparent, accountable practices: Dataminr's public-data-only input limits exposure on data protection and privacy grounds; the system does not require access to classified or citizen personal data mitigating need for surveillance authorities. It validates every alert through a multi-layered approach that automatically corroborates patterns across multiple sources and modalities before an alert is issued, rather than relying on a single subjective source. The system surfaces alerts for human responders — it does not take autonomous action.

To find out more, visit our website or contact us.

Real-Time Situational Awareness for Officer Safety helps protect officers and improve operational decision-making by giving command centres real-time visibility of frontline risks, welfare concerns, and emerging incidents. It replaces fragmented radio updates and delayed reporting with continuous, actionable intelligence.

Using approved wearables and mobile devices, the platform provides real-time officer safety and welfare monitoring, location awareness, and automatic detection of distress events. It can identify falls, panic activations, weapon deployment, and signs of escalating situations. Sensitive data is processed securely on the device, ensuring only relevant insights are shared with supervisors and control rooms. This enables faster intervention, intelligent deployment, and improved coordination of personnel and assets. SITREP AI maintains resilient communications when conventional networks fail through a mesh network operating across cellular, Wi-Fi, and satellite networks. This ensures a persistent operational picture during major incidents, public events, rural deployments, and in areas with poor signal coverage.

The platform also identifies patterns associated with escalating risk, helping supervisors prioritise alerts, allocate resources effectively, and make informed decisions in rapidly changing operational environments.

As adoption matures, SITREP AI evolves from delivering situational awareness to providing operational insight and decision support, helping forces move from reacting to incidents to anticipating operational risk.

To find out more, visit our website or contact us.

Policing has to protect its workforce whilst delivering an effective service to the public.

This is important in digital investigations involving child sexual abuse material. Investigators can be exposed to distressing material and may have to deal with thousands of images and videos within a single case. Asking officers to manually review everything is neither efficient nor sustainable, so technology can help reduce exposure whilst delivering effective investigations.

MSAB's collaboration with organisations such as the Child Rescue Coalition allows for the offenders to still get caught whilst tools within XRY Pro, such as the Hash Tree Builder can aid investigators directly. This is through identifying known material using established hash values & lists, and reducing the need to manually examine material that has already been identified.

XAMN Pro also provides grading tools that integrate Project VIC classifications, allowing relevant material to be categorized. Importantly, this approach also considers investigator welfare. XAMN Pro includes functionality that can cover over images once they have been graded, helping to prevent unnecessary exposure to potentially distressing content. Investigators can therefore work with the evidential information and classification without automatically having to repeatedly view the underlying imagery.

We need technology that reduces cognitive workload, prioritises relevant evidence and allows investigators to concentrate their time where it has the greatest impact.

Ultimately, protecting officers and protecting the public are not competing objectives. Technology should help in seeing less of what they do not need to see, understand more of what they need to understand, and spend their time where they can make the greatest difference.

To find out more, visit our website or contact us.

---

untrite

Untrite THRIVE is a Force Intelligence Platform that works inside the 999 and 101 control room. It listens to the live call, applies the force's own THRIVE risk methodology as the conversation happens, and drafts the structured record: incident log, risk assessment, vulnerability and repeat-victim flags, formatted for the force's systems. The operator stays focused on the caller, then reviews and signs off every output. THRIVE is real-time, human-in-the-loop and auditable by design, not a black box and not an autonomous decision-maker.

We lead with evidence, not promises. THRIVE has run live at Humberside Police since 2024, funded by the force, the Police Digital Service and the Office of the Police Chief Scientific Adviser, and aligned with the NPCC AI Strategy and the new PoliceAI centre.

An independent University of Sussex evaluation of more than 1,252 calls found repeat victims identified far more often (up 19 percentage points, from 58% to 77%), 93% operator agreement with the AI's risk assessment, and around eight minutes saved on a typical domestic abuse call. The full evaluation report is available on request.

THRIVE addresses several of the thirteen problem statements at once, including Problem 11: protecting the workforce by removing cognitive and administrative load during an acute control-room retention crisis.

One proven system, addressing the challenges where policing needs it most.

To find out more, visit our website or contact us

12. How can policing modernise mobility capabilities to ensure safe, efficient and future-ready operations across air, road, and connected vehicle environments?

Ageing air and vehicle fleets, rising drone traffic, and the growing complexity of connected and surveillance-enabled vehicles have constrained safe and effective policing operations. The solutions presented here seek to optimise in-vehicle systems to cut officer distraction and enable secure evidence extraction from connected vehicles.

Primary Service Lines: *Mobility, Surveillance & Sensing, Interconnectivity*

As policing evolves to support connected vehicles, increased mobility, autonomous capabilities and digitally enabled operations, the challenge is not simply adopting new technology. It is ensuring that the underlying systems, processes and governance can support innovation safely, securely and at scale.

Many policing organisations continue to operate complex technology estates, often comprising legacy applications, siloed data, and manual processes that were not designed for today's connected environments. Modernising mobility therefore starts with building a resilient digital foundation that enables new capabilities to be introduced with confidence.

At Acutest, we help organisations prepare for the future by reducing technical debt, modernising legacy systems and creating the assurance frameworks required to support critical digital services. Through application modernisation, cloud migration, test automation, quality engineering and digital assurance services, we enable organisations to introduce change faster while maintaining operational stability and security.

To learn more about Acutest's digital assurance, testing and modernisation services, visit our website or contact us.

Always-on in-field connectivity for frontline policing

Away from a fixed connection, patrol vehicles, mobile ANPR, body-worn video and drone ground stations exchange data with force systems over a cellular path. If that path cannot carry data, a device may continue operating locally, but information intended for transmission cannot reach force systems over that path. In-field connectivity is therefore a dependency for the mobility capabilities in this chapter.

Where cellular data depends on one mobile network core, a core fault can interrupt the path even while the device remains registered and reports a usable radio signal. Signal-strength-only failover will not respond to that condition.

Exclusive to CSL, rSIM® is designed to support in-field connectivity by addressing that exposure. It holds two operator profiles on one SIM, each reaching multiple radio networks through a separate mobile network core. rSIM monitors whether data is passing from the

device. If data stops for a sustained period, it can initiate a switch to the second profile without depending on the affected network to issue an instruction.

Conventional multi-network connectivity can reach alternative radio networks through one core. CSL's patented rSIM architecture adds SIM-resident failover between separate mobile network cores. Designed in the UK and launched in 2024, rSIM is used across telecare, fire and security, healthcare and payments.

CSL supports more than 3.5 million active connections and private VPN connectivity to more than 270 alarm receiving centres across Europe. This private APN and encrypted VPN architecture could support PNC queries, ANPR data and body-worn video, subject to each force's technical, security and assurance requirements.

To find out more, visit our website or contact us.

Real-Time Situational Awareness for Officer Safety helps protect officers and improve operational decision-making by giving command centres real-time visibility of frontline risks, welfare concerns, and emerging incidents. It replaces fragmented radio updates and delayed reporting with continuous, actionable intelligence.

Using approved wearables and mobile devices, the platform provides real-time officer safety and welfare monitoring, location awareness, and automatic detection of distress events. It can identify falls, panic activations, weapon deployment, and signs of escalating situations. Sensitive data is processed securely on the device, ensuring only relevant insights are shared with supervisors and control rooms. This enables faster intervention, intelligent deployment, and improved coordination of personnel and assets.

SITREP AI maintains resilient communications when conventional networks fail through a mesh network operating across cellular, Wi-Fi, and satellite networks. This ensures a persistent operational picture during major incidents, public events, rural deployments, and in areas with poor signal coverage.

The platform also identifies patterns associated with escalating risk, helping supervisors prioritise alerts, allocate resources effectively, and make informed decisions in rapidly changing operational environments.

As adoption matures, SITREP AI evolves from delivering situational awareness to providing operational insight and decision support, helping forces move from reacting to incidents to anticipating operational risk.

To find out more, visit our website or contact us.

Esri UK ArcGIS uses location as the essential thread to connect policing data, people, systems and intelligence, with trusted information shared securely, understood consistently and acted upon in real time. A Location Data Fabric brings together fragmented policing data in a single, coherent operational view. Location is one of the most powerful references to join datasets together, adding geographic context that helps forces better understand patterns in data, identify risks and make informed decisions. ArcGIS creates a trusted operational picture that forces and partner organisations can work from across boundaries, ensuring shared understanding, clarity and consistency.

Delivering live location intelligence to officers wherever they are deployed, helping teams coordinate responses. Police Scotland used a GIS-based app for vital search-and-seal operations to replace paper processes and improve missing person searches, Royal visit security and major events.

To find out more, visit our website or contact us.

Securing UK Police Vehicle Connectivity with FortiGate Firewalls, IPSec VPNs and SD-WAN

UK police forces increasingly rely on secure mobile connectivity to provide officers with access to command-and-control systems, intelligence databases, ANPR, body-worn video, and other operational applications while on patrol. Deploying FortiGate next-generation firewalls within police vehicles provides a secure gateway between onboard devices and police force networks.

FortiGate protects all vehicle communications by establishing encrypted IPSec VPN tunnels over public 4G and 5G mobile networks. This ensures that sensitive policing data remains confidential, authenticated and protected from interception while enabling secure access to force applications and services from any location.

In addition to VPN encryption, FortiGate provides advanced security capabilities including intrusion prevention, application control, web filtering and malware protection.

Integrated SD-WAN further enhances operational resilience by intelligently selecting the optimal network path for critical applications. Using multiple mobile connections, SD-WAN continuously monitors link performance and automatically prioritises mission-critical services such as Computer Aided Dispatch (CAD), intelligence systems and emergency communications over less critical traffic. Together, FortiGate, IPSec VPNs and SD-WAN provide UK police forces with a secure, resilient and centrally managed mobile networking solution. This architecture enables officers to securely access operational systems wherever they are deployed while ensuring consistent security and uninterrupted connectivity for frontline policing.

To find out more, visit our website or contact us.

TJA Associates offers a practical, outcome-led solution to Problem 12. Its core proposition is that policing should not treat data, innovation, emerging technology and mobility as separate issues, but as connected operating-model challenges that require governance, collaboration, evaluation and business change as much as technical capability.

TJA supports a future-ready mobility capability by connecting roads policing, transport innovation, ANPR, connected-vehicle data, and autonomous operations, safety, enforcement and cross-sector governance into a coherent national capability model.

TJA's product/case-study offer is not a single technology platform; it is a structured consultancy and delivery approach that helps NPCC and partner organisations define the problem, convene the right stakeholders, shape operating models, translate complex data

into actionable intelligence requirements, manage delivery and measure benefits. This means TJA can address many Problem Book challenges where the barriers are interoperability, trust, evidence quality, public confidence, supplier engagement, governance and adoption. Find out more at TJA Associates.

To find out more, visit our website or contact us.

Vizgard

Vizgard is a UK sovereign visual AI company. Our software turns cameras and drones that forces already operate into autonomous teammates, cutting operator workload and speeding up threat detection while keeping a human on the loop. Our flagship product, FortifAI, is a TRL 9 platform that adds real-time visual intelligence and automated camera control to existing infrastructure.

FortifAI steers distributed cameras to visually confirm and tell apart birds, drones, planes and helicopters, giving forces airspace situational awareness and counter-drone capability without buying new sensors. Our V-GroundControl software lets one operator run up to 12 air or ground platforms, and VizEdge puts the same analytics on a rugged wearable for officers working offline in the field.

Vizgard has delivered for the UK MOD, Home Office and defence primes, including safeguarding the perimeter of a major international airport. The platform is open architecture, so forces can run their own models and keep full control of their data.

To find out more, visit our website or contact us.

---

13. How can policing embed innovation, evaluation, and strategic foresight into its culture and operations?

Restrictive funding models and a lack of shared evaluation standards have limited policing's ability to adopt, scale, and legally validate new technologies. The solutions below seek to establish a national testing "sandbox" for policing technologies, automate legal admissibility evaluation, and embed future crime and tech trends into strategic planning.

Primary Service Lines: *Interconnectivity, Analytics*

Embedding innovation, evaluation and strategic foresight into policing requires more than adopting new technology; it requires creating a culture where officers and staff are empowered to challenge the status quo, test new ideas, and learn systematically from outcomes. Innovation must become everyone's responsibility, supported by leadership, governance and processes that encourage experimentation while maintaining operational integrity.

Through the Flashlight Innovation Project, Accenture worked alongside the Police Superintendents' Association (PSA), Amazon Web Services (AWS), the Society of Evidence Based Policing (SEBP) and the Open University to provide a national platform for officers and staff to propose technology enabled solutions to challenges identified within the NPCC Problem Book. The programme invited ideas directly from the policing workforce, shortlisted the strongest concepts, and provided mentoring, technical support and prototype development to help turn innovative thinking into practical solutions.

This model demonstrates how policing can embed innovation into everyday operations by giving frontline personnel a voice, creating safe spaces to challenge existing ways of working, and providing clear pathways from idea to implementation. Equally important is the emphasis on evaluation. By partnering with organisations such as SEBP and academic institutions, innovation can be assessed against measurable outcomes and evidence-based practices, ensuring that investment is focused on initiatives that deliver genuine operational benefit.

Strategic foresight can be strengthened by combining these innovation mechanisms with horizon scanning, technology partnerships and challenge led competitions. By supporting experimentation, innovation challenges, and rigorously evaluating results, policing can build a sustainable culture of continuous improvement that is better prepared for the complex public safety challenges of the future.

To find out more, visit our website or contact us.

Policing has always adapted to new challenges, but the pace of change is accelerating. Just as important is the ability to evaluate what works. Strategic foresight also has a key role to play. Realising the benefits of innovation depends on establishing the right foundations. No single organisation can achieve this alone. Stronger collaboration between policing, industry, academia and

government will be critical in bringing together different perspectives, expertise and evidence. BT believes the most valuable innovation is driven by real operational problems rather than technology for its own sake. As technological and societal change accelerates, creating stronger connections between practitioners, innovators and industry will be essential to help policing anticipate future challenges rather than simply react to them.

To find out more, visit our website or contact us.

CIVICA

Six of the NPCC's 13 identified problems — spanning public contact, cross-force data sharing, offender monitoring, online child sexual exploitation, workforce protection, and innovation/strategic foresight — share a common structural cause: fragmented, unreconciled data about the same people, places, cases and equipment held across 48 independent systems.

The case made here is not that Master Data Management (MDM) solves policing's 13 problems. It is that six of them are, in part, the same problem — and that solving it once, doing it well, is worth significantly more than solving it 48 times separately.

A modern MDM platform does not solve every dimension of these problems on its own, however, MDM addresses the shared root cause running underneath most of them: the inability to reliably tell that a record in one system and a record in another refer to the same real-world person, case or thing.

For further descriptions of the value from MDM to Problem Statement 13, visit our dedicated page or contact us.

CLOUDFLARE

Policing requires a national innovation system to transform ideas into evidence-based decisions, share learning, and avoid repeating unsuccessful experiments.

The foundation should be a secure, programmable evaluation environment where forces and partners test services using synthetic or de-identified data. Projects must define clear problems and measurable success criteria. Standard templates should assess accuracy, security, and operational impact, with results feeding a shared evidence library that manages discovery through national scaling.

Cloudflare OS provides this capability: workspaces grounded in approved knowledge and reusable skills. Cloudflare OS runs in isolated runtimes where agents create code or workflows with no default access; resources are granted through governed connections, and outbound access is restricted. This creates a sandbox for experimentation, recording agent activity and applying policy to all outputs. Private-by-default deployment controls add identity verification and visibility.

Governance should be proportionate. Low-risk experiments move quickly within guardrails, while higher-risk projects require rigorous human oversight and ethical review.

To find out more, visit our website or contact us.

COEUS software

PoliceBox is a nationally scalable, locally configurable Frontline Operational Platform designed to help policing modernise frontline work while making better use of existing systems. It primarily addresses Problem Statements 3, 10 and 13: secure, efficient and standardised data sharing; a digitally empowered workforce; and embedding innovation and evaluation into policing. PoliceBox provides a common operational layer between officers and systems such as CAD, RMS and national services. Its open, API-first architecture supports secure integration with existing and future systems without replacing systems of record.

For officers, PoliceBox brings tasks, operational information, workflows and guidance into one mobile-first experience. It works online and offline, reduces re-keying and system switching, and supports structured, auditable data capture at the point of activity. Cecil, the PoliceBox AI-enabled operational assistant, provides procedural support using approved national and force-specific sources. It remains advisory: professional judgement stays with the officer, who authors the operational record.

This approach was evaluated with Humberside Police through the NPCC NSIB-funded Project Moriarty Test & Learn trial. Cecil achieved average scores of 4.6/5 for accuracy, 4.5/5 for relevance and 4.6/5 for usability, with responses in under 30 seconds.

To find out more, visit our website or contact us.

Davidhorn

Advancing Investigative Interview Excellence Through Digital Innovation

With over 40 years of experience, Davidhorn is the UK's leading provider of evidential interview recording and productivity solutions, directly supporting the National Policing Digital Strategy 2025-2030's mission to enable officers and staff through modern digital tools.

Our interview recording solution addresses critical strategic priorities: modernising core investigative technology, automating administrative processes to free officers for frontline duties and investigative work, and ensuring high-quality data capture for analytics-driven policing. By replacing legacy recording systems with interoperable, cloud-ready solutions, we help forces reduce complexity and costs while maintaining the highest evidential standards.

Davidhorn's technology streamlines the entire interview process, from secure digital recording to efficient case file preparation, enabling investigators to focus on outcomes rather than administration. With integrations to major UK Records Management Systems (RMS) and Digital Evidence Management Systems (DEMS), we deliver the connected technology vision central to the strategy, ensuring seamless data sharing across forces and criminal justice partners.

As committed partners to UK law enforcement, we deliver scalable, sustainable solutions that protect the public through more efficient, effective investigations.

To find out more, visit our website or contact us.

FRAZER-NASH CONSULTANCY A KBR COMPANY

AEGIS is Frazer-Nash Consultancy's Counter-Uncrewed Aerial Systems (C-UAS) intelligence and decision-support capability. Developed with operational stakeholders, AEGIS helps users identify, prioritise and investigate suspicious activity from large volumes of drone information using behavioural analytics, risk-ranking and geospatial analysis.

Whilst originally developed for C-UAS operations, AEGIS demonstrates a broader approach to helping analysts extract insight from large and complex datasets whilst reducing the burden of manual review. By applying configurable behavioural indicators and

historical analysis techniques, the platform helps users identify activity that may warrant further investigation and focus attention where it is most needed. During pilot activity, AEGIS demonstrated the potential to reduce drone investigation effort by up to 90%, allowing analysts to spend more time interpreting information and developing intelligence.

AEGIS is designed to support human judgement rather than replace it. Its analytics are transparent and configurable, allowing behavioural indicators and risk criteria to be adapted to different operational contexts whilst maintaining user trust in the underlying assessment.

As a secure cloud-hosted application, AEGIS provides a standalone intelligence and decision-support capability. Equally, AEGIS can act as a service into larger enterprise environments, enabling information from multiple sources to be assessed through a consistent analytical lens without constraining future technology choices.

Developed through iterative engagement with operational users, AEGIS demonstrates how new capabilities can be matured through experimentation and evidence-led delivery.

To find out more, visit our website or contact us.

---

innov8law

Public-sector organisations already hold many of the warning signals of tomorrow's failures: complaints, incidents, claims, misconduct, workforce pressures, financial losses, poor outcomes and declining public trust. Too often, those signals are considered separately.

innov8law Haemostasis™ is a cross-government methodology designed to help leaders connect those signals, identify where organisational harm is developing, quantify its human, social and economic impact, diagnose root causes and intervene before harm and cost escalate.

The methodology follows six stages: Target → Structure → Quantify → Diagnose → Intervene → Make the Case.

Its configurable Haemostasis Scorecard™ provides an early-warning and decision-support architecture through which different public services can select relevant indicators while retaining a common framework based on Human Value, Social Value and Economic Value.

For policing, Haemostasis™ could bring together indicators including complaints, victim experience, misconduct, workforce information, operational data, legal and financial exposure and public-confidence measures. The objective is not another complaints system, but better organisational intelligence: identifying patterns, understanding the true cost of the bleed, prioritising intervention and measuring whether action has reduced harm.

The methodology is being developed through real-world public-sector problem solving. An initial University of Reading consultancy demonstrator has applied Haemostasis™ to NHS maternity services, exploring how fragmented evidence can become board-level risk intelligence, cost-of-failure analysis and strategic recommendations.

innov8law now proposes applying this cross-government architecture to policing, initially supporting Problem 6: building and maintaining public trust, with direct relevance to Problem 13.
Stop Harm. Repair Damage. Rehabilitate Systems.

To find out more about Haemostasis™, visit our website or contact us.

InterSystems
Creative data technology

Policing cannot afford to wait years for a single future system before improving how information moves between forces, counties and partner agencies. The 2026 Police Reform White Paper says nine in ten crimes have a digital component and argues for less fragmentation and clearer national standards. Better data sharing will be central to making that ambition practical.

It is to help policing and justice partners share structured, meaningful information securely, so they can build a fuller view of people, incidents, intelligence and risk, including when cases move across county lines.
Data still sits across 43 forces, national systems and local platforms. The Police Digital Service handbook positions interoperability

as essential to sharing data across organisational boundaries, reducing duplication, and enabling analytics and AI at scale. Healthcare has faced a similar challenge: how to connect sensitive information across complex organisations without disrupting frontline services.

Shared Care Records offer a useful example. They connect sensitive information across NHS, local authority and care settings, giving staff access to more complete and up-to-date information while frontline systems remain in place.

Forces can start by making the information they already hold easier to share securely across counties and partners, while local systems modernise over time.

Why data fabric deserves attention
A data fabric approach is well suited to this challenge because it connects existing data sources rather than requiring forces to replace systems that still support daily operations. By creating a secure, governed layer across multiple environments, it can give authorised users a more coherent view of operational information in real time

To find out more, visit our website or contact us.

Kahootz provides secure workspaces for sharing information and coordinating work across organisational boundaries. Authorised participants can access current documents, discuss issues, manage tasks, record decisions and maintain an auditable history of activity in one shared workspace.

This is relevant to policing because forces increasingly need to collaborate with other forces, national bodies, suppliers and community or specialist partners. Kahootz can provide a single source of truth for this work, reducing reliance on email attachments, disconnected shared drives and informal channels. Its features include configurable access permissions, document version control, review and approval workflows, task management and audit trails.

Kahootz is already used in sensitive public-sector collaboration across government, including through Defence Share, the Ministry of Defence's primary collaboration tool. Powered by Kahootz, Defence Share enables the MOD to share information classified up to OFFICIAL-SENSITIVE with defence industry partners, other government departments, agencies and allied nations. It provides geographically distributed participants with secure workspaces for accessing information and collaborating on complex programmes.

The same principles could support policing collaboration while complementing, rather than replacing, core operational systems and information-governance processes. Kahootz can support problem statement 13 by enabling controlled pilots, evaluation and the sharing of learning across organisational boundaries.

To find out more, visit our website or contact us.

NEC Software Solutions UK

Policing needs a stronger national model for innovation if it is to respond to emerging threats, rising demand and rapid technological change. Too often, innovation is duplicated across forces, evaluation is inconsistent, and good ideas remain trapped in local pilots. Future readiness requires a coordinated approach that allows new tools to be tested safely, assessed consistently and scaled with confidence.

NEC Software Solutions UK proposes a two-part approach: a national innovation capability, supported by a practical use case focused on Violence Against Women and Girls (VAWG).

Strategically, NEC can help create a National Policing Innovation Ecosystem, using NEC and partner products to provide interoperable services, shared data architectures and secure digital capability. This could support a national sandbox alongside PoliceAI, where emerging technologies, AI models and new operating approaches are trialled using representative or synthetic data. Built-in evaluation, performance metrics and audit controls would allow transparent assessment of benefits, evidential robustness and legal admissibility.

Operationally, this can be shown through an AI-Enabled Safeguarding Intelligence Hub for Multi-Agency Safeguarding Hubs (MASH).

The hub would analyse information from police, health, education and local authority systems to identify risk indicators, highlight VAWG concerns, generate multi-agency summaries and support consistent safeguarding decisions. It strengthens professional judgement by improving visibility of vulnerability, repeat victimisation and escalating risk.

Together, these capabilities show how NEC can help policing and the wider multi-agency system innovate safely, evaluate consistently, share learning nationally and deploy proven technologies at scale, supporting a more connected, evidence-led and future-ready police service.

To find out more, visit our website or contact us.

Simpson Associates

Public contact remains one of the most important interfaces between policing and the communities it serves. Whether through a 999 call, a 101 enquiry, an online report or another digital channel, every interaction shapes public confidence and provides valuable insight into community demand. As demand continues to grow in both volume and complexity, many forces face a common challenge: information relating to public contact is often spread across multiple systems, teams and processes. This can make it difficult to establish a complete view of an individual's interactions, ensure staff have the context they need and provide a consistent experience for the public.

Simpson Associates has more than three decades of data and analytics experience and has worked with over 65% of UK police forces. Through this experience, we have seen that forces often already hold the information needed to improve service delivery and support decision-making. The challenge is making that information accessible, connected and actionable at the point it is needed.

A more connected approach to public contact can help forces better understand demand, improve visibility across citizen interactions and support more informed operational decision-making. It also creates opportunities to reduce effort for both staff and the public while helping build confidence in policing services.
In this article, Simpson Associates explores why connected data is becoming increasingly important to modern policing and how forces can make better use of the information they already hold to deliver better outcomes for the communities they serve.

To find out more, visit our website or contact us.

Telefónica Tech's Predictive Policing Accelerator, built on Databricks, helps police forces move from reactive reporting towards more proactive, intelligence-led policing. The solution brings together data from multiple policing systems into a single governed platform, providing a real-time view of crime, emerging trends, demand and harm-based priorities. Geospatial analytics helps identify hotspots and patterns, while AI-generated insights support earlier identification of emerging risks and more targeted operational responses.

Integrated with Databricks Genie, the accelerator also enables officers, analysts and operational leaders to explore governed policing data using natural language, without relying on specialist technical skills or predefined reports. Users can investigate trends, drill into patterns and answer operational questions more quickly, helping translate data into actionable intelligence at the point of need. This supports better resource allocation, more targeted prevention activity and more informed decision making.

The approach is designed around responsible AI, with governance, transparency and human oversight embedded into the platform. This enables predictive insight to support professional judgement rather than replace it, helping forces adopt AI in a way that is accountable and aligned with policing principles.

To find out more, visit our website or contact us.

TJA Associates offers a practical, outcome-led solution to Problem 13. Its core proposition is that policing should not treat data, innovation, emerging technology and mobility as separate issues, but as connected operating-model challenges that require governance, collaboration, evaluation and business change as much as technical capability.

TJA provides the discipline to make innovation repeatable and measurable, linking horizon scanning, Business Case development, stakeholder engagement, evaluation, benefits realisation and procurement support into a pathway from idea to impact.

TJA's product/case-study offer is not a single technology platform; it is a structured consultancy and delivery approach that helps NPCC and partner organisations define the problem, convene the right stakeholders, shape operating models, translate complex data

into actionable intelligence requirements, manage delivery and measure benefits. This means TJA can address many Problem Book challenges where the barriers are interoperability, trust, evidence quality, public confidence, supplier engagement, governance and adoption. Find out more at TJA Associates.

To find out more, visit our website or contact us.

Through the Knowledge Transfer Partnership (KTP) programme, we are working in close collaboration with Devon and Cornwall Police (DCP) to embed innovation, evaluation, and strategic foresight into its culture and operations through the use of computer and data science. The headline aim of the KTP is to improve strategic management decision making through the use of digital tools such as artificial intelligence (AI) and digital twins, and to build confidence and a culture change within DCP.

The position is jointly funded by DCP and Innovate UK, whose aim is to translate cutting edge research into real-world impact. But the police are no longer able to participate in KTPs and so this route to funding projects long enough to establish close collaborations and knowledge exchange is now closed.

To find out more, visit our website or contact us.

Untrite THRIVE is a Force Intelligence Platform that works inside the 999 and 101 control room. It listens to the live call, applies the force's own THRIVE risk methodology as the conversation happens, and drafts the structured record: incident log, risk assessment, vulnerability and repeat-victim flags, formatted for the force's systems. The operator stays focused on the caller, then reviews and signs off every output. THRIVE is real-time, human-in-the-loop and auditable by design, not a black box and not an autonomous decision-maker.

We lead with evidence, not promises. THRIVE has run live at Humberside Police since 2024, funded by the force, the Police Digital Service and the Office of the Police Chief Scientific Adviser, and aligned with the NPCC AI Strategy and the new PoliceAI centre.

An independent University of Sussex evaluation of more than 1,252 calls found repeat victims identified far more often (up 19 percentage points, from 58% to 77%), 93% operator agreement with the AI's risk assessment, and around eight minutes saved on a typical domestic abuse call. The full evaluation report is available on request.

THRIVE addresses several of the thirteen problem statements at once, including Problem 13: a live, independently evaluated template for evidence-first innovation before anything scales.

One proven system, addressing the challenges where policing needs it most.

To find out more, visit our website or contact us.

---

whitespace

Policing is generating and handling ever-growing volumes of digital evidence. The challenge isn't simply capturing more information, but helping officers and investigators review, understand and use that evidence effectively while reducing manual effort and maintaining strong governance, assurance and evidential integrity.
Whitespace helps policing organisations turn operational challenges into trusted, governed AI capability. Rather than offering a one-size-fits-all product, we work alongside operational teams to understand where friction exists, define the outcome, and rapidly design, develop and test AI capabilities around that need.

We're already working with Microsoft and a large UK Police force to co-design an AI capability supporting the secure processing of taped and video interviews. The capability is designed to support translation, transcription, summarisation and structured outputs, helping reduce processing pressure while maintaining human oversight, accuracy and operational trust.

This work demonstrates our broader approach to digital evidence. Depending on the operational need, this could include capabilities that support evidence review, information access, workflow support and earlier operational assurance.

Our approach combines Solutions Engineering with Collective, our sovereign AI operating system, providing a secure and governed foundation for developing operational AI capabilities while retaining organisational control over data, deployment and AI.

The aim is not to replace investigators or automate policing. It's to help forces apply AI responsibly to validated operational problems, improve the speed and consistency of evidence handling, reduce unnecessary administrative burden and strengthen assurance.

To find out more, visit our website or contact us.

To meet the demands of modern intelligence-led policing, police forces need to overcome legacy limitations and set up strong digital foundations.

With solid digital foundations, forces can use assistive AI to reduce cognitive load and free officers to focus on intelligence-led tasks.

Tools like AI assistants, document summarisation, semantic search across case files, and intelligent redaction reduce repetitive work and speeds up digital evidence processing. Though full auditability, explainability, and human-in-the-loop oversight is essential.

Speak to our AI team to learn about our tools via this link.

The biggest barrier to innovation is often culture. Adopting AI can mean navigating structural complexities – that's what our research of national security civil servants found in our recent whitepaper.

With our public sector clients, we use co-design workshops (Transformation Days) to start that culture change and de-risk innovation. These sessions bring officers and leaders together to reach alignment, rapidly prototype in safe environments, and turn ideas into a clear business case and plan.

To find out more, read our whitepaper or contact us.

Conclusion

The challenges set out in the Policing Problem Book are not static, and neither is the response to them. As technology continues to evolve at pace, and as the demands on policing shift in turn, the solutions industry can offer must evolve with them.

The techUK Policing Solutions Book is intended as a living document. It will be reviewed and updated regularly, ensuring it continues to reflect the latest capabilities from techUK's membership, as well as any changes to the problems and priorities identified by the NPCC.

techUK remains committed to supporting this ongoing dialogue between industry and policing, ensuring the Book continues to serve as a practical and current resource, rather than a static reference point. By maintaining this shared focus, industry and policing can continue to work together to turn identified problems into deployable, lasting solutions, and to ensure policing has access to the tools it needs, both now and in the future.

We encourage members to continue engaging with this initiative, submitting new and updated solutions as they emerge, so that the Book keeps pace with innovation and remains a genuine reflection of what industry can offer policing today and tomorrow.

techUK reiterates that no endorsement, prioritisation, or recommendation of any individual solution is implied by its inclusion in this resource. Its purpose remains to demonstrate the depth of capability within our membership, in support of the shared ambition between industry and policing.

techUK's Justice and Emergency Services Programme

techUK's Justice and Emergency Services (JES) Programme represents technology suppliers working across the public safety and criminal justice sectors. The Programme builds strong, trusted relationships between industry and public sector customers, convening forums that encourage open engagement, unlock innovation, explore emerging technologies and address the barriers to digital transformation. Our work is structured around three core portfolios (policing, justice, and fire and rescue) and extends into related areas including digital interoperability, VAWG and RASSO, fraud and economic crime, retail crime, and legal tech. This means members can engage across the full range of policy and operational issues affecting the sector.

To find out more or get involved, contact the JES team at jesteam@techuk.org.

techUK
FOR WHAT COMES NEXT

About techUK

techUK is the trade association that brings together people, companies and organisations to realise the positive outcomes of what digital technology can achieve. With over 1,100 members across the UK, techUK creates a network for innovation and collaboration across business, government and stakeholders to provide a better future for people, society, the economy and the planet.

By providing expertise and insight, techUK supports our members, helps the government understand the impact of their policies on business, and draws together the industry and public sector to agree the right approach to how digital technology policy is developed and implemented.

linkedin.com/company/techUK

@techUK

youtube.com/user/techUKViews

info@techuk.org

Image credits | iStock by Getty Images and Adobe Stock