

SECURE, EFFICIENT AND STANDARDISED DATA SHARING

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



With over a decade delivering critical solutions to national policing, the NPCC Policing Problem Book felt very familiar. Through our TechUK membership, we jumped at the chance to share our thoughts and experience on solving these problems. Many of them mirror challenges we've already solved, in policing and beyond. We were asked to pick three. In this document we share our response to one of the problems.

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

Policing in the UK is delivered by 48 independent forces, each operating its own IT systems for records, contact management, and digital evidence. This fragmented landscape creates significant barriers to the sharing of data, both between and within forces. Incompatible systems, inconsistent data formats, and duplicated entry processes reduce efficiency, increase the risk of error, and hinder the ability to act on critical information.

The lack of interoperability undermines the quality of evidence, increases the number of repetitive tasks for officers, and limits the potential to improve the timeliness of investigations.

- How can policing build a system that enables secure, real-time data sharing across legacy systems? Are there alternative solutions?
- What can policing do to ensure data integrity and auditability across multiple agencies?
- How can policing reconcile and deduplicate records across disparate systems?

Based on our technologies, expertise and innovation, how could we solve this problem?

Experience solving this problem

Policing in the UK is delivered by 48 independent forces, each running its own systems for records, contact management and digital evidence. The result is data that is hard to share, easy to duplicate and slow to act on. We answer this problem from direct experience of secure information sharing across organisational boundaries. Through ResilienceDirect, we have delivered the secure platform on which the UK's emergency services, armed forces and resilience organisations share sensitive information, continuously since 2013, alongside national-scale platform and security delivery across government and regulated sectors.

Secure, real-time sharing across legacy systems: connect what exists, rather than replace it

The instinctive answer to fragmentation is convergence, a single national records system that every force adopts. Experience across government suggests that route means a decade of procurement and migration risk before any officer sees a benefit. The practical alternative is a secure sharing layer built over the systems forces already run.

Modern Zero Trust technologies make this possible without wholesale replacement. An encrypted, vendor-neutral overlay connects existing force systems, while access control sits at the application layer rather than the network. That distinction matters. Rather than simply connecting systems, the sharing layer enforces identity-aware policies that determine precisely who can reach which data, application or service, with authorisation confirmed in real time. An officer in one force reaching a record held by another does so with their identity verified and every action logged.

Our partner Cloudflare provides this capability at global scale, and we bring the delivery experience to match. We are Cloudflare's first ZTNA Authorised Service Delivery Partner in EMEA, and we design and deliver Zero Trust environments end to end, including replacing legacy VPN estates with identity-aware access across UK and international locations.

Incompatible formats are the second barrier and removing them does not require every force to rebuild. A lightweight integration and normalisation layer, running as serverless functions at the network edge, can translate between formats and present a consistent schema to any consuming system. Forces keep the records and contact systems they know and share through common standards. We have delivered this kind of consolidation

for other bodies handling sensitive data at national scale. For Social Work England, we replaced fragmented systems with a single integrated platform serving more than 96,000 social workers, connecting the public-facing service directly to case management so that information is entered once and flows through, saving hundreds of thousands of hours a year previously lost to manual processing.

For West Mercia Police, we are using Appian's data fabric to connect a new digital forensics case management platform to other force back-office systems, including records management and existing forensic tools, through API integration rather than a full rebuild and system replacement. Specialist teams keep working in the systems they already know, while case data and chain of custody information flow through to wherever they are needed, fully timestamped and auditable.

Data integrity and auditability across multiple agencies

Multi-agency sharing stands or falls on trust in the audit trail. Every access event across the sharing layer should generate a tamper-evident log, streamed continuously to force and national audit systems, so that investigators, auditors and oversight bodies can see who accessed what, when and why.

ResilienceDirect, the platform emergency services, the armed forces and resilience organisations across the UK use to plan for and respond to national disasters, shows these principles working across organisational boundaries under real pressure. More than 130,000 personnel and 8,000 organisations share sensitive planning and incident information on a platform we have delivered since 2013, with granular security controls on every object and support for gold, silver and bronze command structures. Over 3,000 major incidents have been coordinated through it. Our security practice is certified to ISO 27001 and Cyber Essentials Plus, certified for business continuity under ISO 22301, and aligned with NCSC guidance.

Reconciling and deduplicating records across disparate systems

Matching and deduplication logic can run as services within the integration layer, applying consistent rules across sources in place of manual re-keying. Capturing data once, to a shared standard, is the cheapest form of deduplication of all, because records that never fork never need reconciling.

Technology helps here, and we would be straight with policing about its limits. Reconciliation is as much a question of data standards, ownership and inter-force agreement as it is of software. This is why we would begin with a structured discovery to map what data exists, what condition it is in, and what governance needs to be in place before records flow.

We are also exploring what AI adds. Our proof of concept for the College of Policing queries structured databases and unstructured policy documents through a single interface, built on the Model Context Protocol, an open standard connecting data to multiple tools rather than locking it into one system. The underlying data store keeps a full history of every change, so questions about past performance can be answered directly, without separate historical reports. What it demonstrates is the direction of travel: investigators interrogating data across sources in real time, instead of waiting for overnight batch transfers or manual data sharing agreements.

Prove it force by force

None of this needs a high-risk national cutover. Start with two forces and one high-value use case, such as cross-border intelligence checks. Prove the access controls and the audit trail, then extend system by system and force by force. We work this way because it works. [Single Online Home](#) shows this in practice, growing from one online form serving Greater London into a national platform serving 41 forces plus British Transport Police, covering 94% of the population of England and Wales. Cloudflare Access secured every step of that rollout, giving each force safe entry without disrupting a service the public already relies on. Policing's own digital strategy calls for building once and sharing nationally. Applied to data sharing, the same approach gives every force a route to secure, standardised sharing without betting everything on a single programme.

Solving policing problems for over a decade

Our deep understanding of policing sector challenges for over a decade, enables us to deliver solutions that excel in your environment. We act as strategic partners in your transformation journey working as one team—driving real change and innovation rather than simply implementing technology.

Speak to our experts

SPEAK TO US

