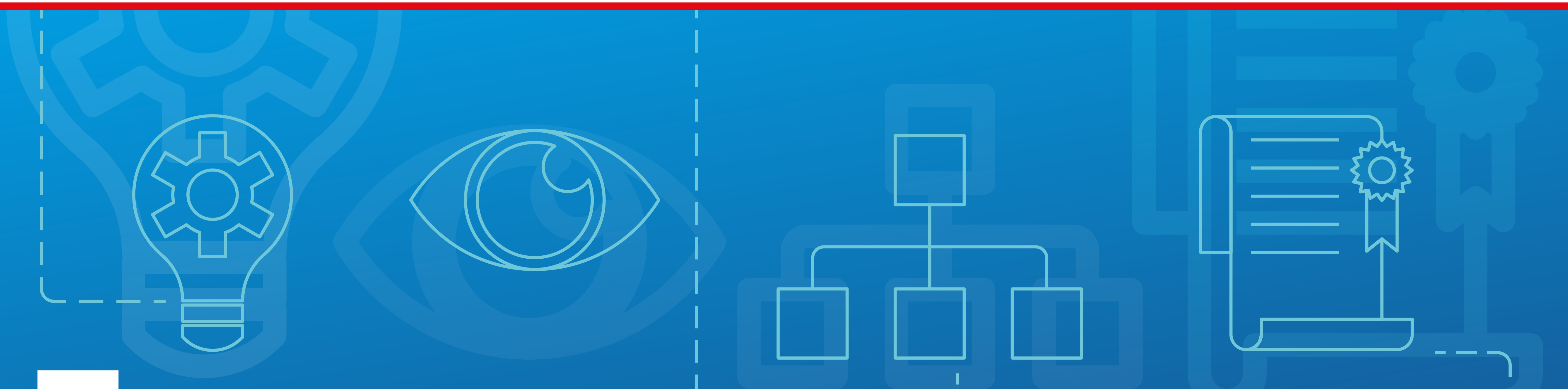
An independent Policing Insight report commissioned by Capita



From back office to business critical

Why information management should be a core policing function

CoPaCC
the police governance experts

Published by
Policinginsight

Information and acknowledgements

Credits

AUTHOR
James Sweetland
Contributing writer and researcher, specialising in policing, criminal justice, and technology policy

EDITING
Keith Potter
Editor of Policing Insight

PRODUCTION
Ian Barrett
Director of Publishing and Product Development, Policing Insight

DESIGN AND LAYOUT
David Devonport
Freelance designer

Special thanks

We are hugely grateful for the generous time and contributions to this report from key stakeholders, both current and past, sharing their expertise, experience and knowledge.

David Hamilton, Scottish Information Commissioner; **Giles Herdale**, RUSI Associate Fellow and independent expert in digital investigation and data ethics; **Stuart Hyde**, former NPCC Lead for Data Compliance; **Emily Keaney**, Deputy Commissioner of Regulatory Policy, Information Commissioner's Office; **Wayne Parkes**, former PDS Chief Digital Data and Technology Officer; **Stephen Russell**, Director of Data, Strategy and Technology, Warwickshire Police; **Owen Sayers**, information assurance and data protection specialist; **Aimee Smith**, Metropolitan Police Director of Data and Chair of the National Police Data Board; **Dave Tonks**, Digital Transformation Consultant, Justice & Policing, Capita.

From back office to business critical: Why information management should be a core policing function

An independent report, researched and produced by Policing Insight and commissioned by Capita.

Policinginsight

Policing Insight is the leading platform to keep up with the latest in progressive policing. It is where the global police and criminal justice community both consume and share knowledge, opinion and analysis. Policing Insight's subscription community consists of government, policing, third sector, academia and industry, all interested in working towards better policing outcomes.

If your organisation would like to commission an independently researched and written report from Policing Insight on an important policing and criminal justice topic, please contact **enquiries@policinginsight.com**

Read more Policing Insight reports at **policinginsight.com/reports**

Capita

As strategic partners with the Home Office, Ireland's Department of Justice and over 30 police forces throughout the UK, we're collaboratively designing, building and implementing innovative human-centred solutions to improve outcomes for the police, the judiciary and the wider public.

Our information management services to UK police forces can digitise and centralise all your paper and disparate digital records and by applying relevant controls and leveraging artificial intelligence (AI), you can search, access and share large amounts of otherwise inaccessible information within your forces more efficiently and quickly. This means you can spend more time focusing on what matters most – solving crimes and supporting victims.

We've supported many public service organisations to connect their legacy and disparate data, including digitising over 52 million patient records and business records for NHS England. We tailor our digital solutions to the needs of your organisation whilst helping to ensure that you're always fully compliant with the Data Protection Act and all GDPR requirements.

To find out more please visit us at **Capita Information Management** or contact **geoff.thompson@capita.com**

Information management stakeholder voices

“You can look at almost any public inquiry, serious case review, domestic homicide review. Any of these things will highlight poor information management, poor performance on putting together an intelligence picture, and failure to make timely decisions. These things have huge consequences and they're also things where the public have an expectation that the police will be both competent and trustworthy in using personal data.”

Giles Herdale
Associate Fellow, RUSI

“Have you really got the right capacity and subject matter expertise in your organisation to truly understand and manage the data that you've got?”

Aimee Smith
Chair, National Police Data Board

“I think information assurance is just seen as a pain in the neck – 'how do we get around this?', not 'how do we comply with it?' Or you get the other side, which is 'No, you can't do anything because of data protection', resulting in a very risk-averse environment.”

Stuart Hyde
Former NPCC Lead for Data Compliance

“People in policing recognise the issue, but it's difficult to get it high up the investment agenda. I've been in those discussions and tried to take some of this forward in policing. But in the end, it's about what forces decide should take priority: catching more criminals or protecting the information you've got?”

Wayne Parkes
Former PDS Chief Digital Data and Technology Officer

“If you can get the information right, everything else is serviced by it … We need a proper strategic approach which asks where policing can get the biggest bang for its buck from investment in information management.”

Dave Tonks
Digital Transformation Consultant, Capita

“Data management is like painting the Forth Bridge. It's a constant energy and effort… data quality and governance are parts of your business that you will always need to be focusing on.”

Stephen Russell
Director of Data, Strategy and Technology, Warwickshire Police

“I think part of the answer is that it can't just be seen as the responsibility of the data protection officer. There needs to be a cultural understanding, driven from the top, that this is the responsibility of everybody. Everybody has responsibility for thinking about basic good practice when it comes to data.”

Emily Keaney
Deputy Commissioner of Regulatory Policy, ICO

“Every national system should have a designated data controller. I know that two chief constables had no idea that they were the designated lead controller and that this meant they have personal legal responsibilities.”

Owen Sayers
Information assurance and data protection specialist and former architect for national police data systems

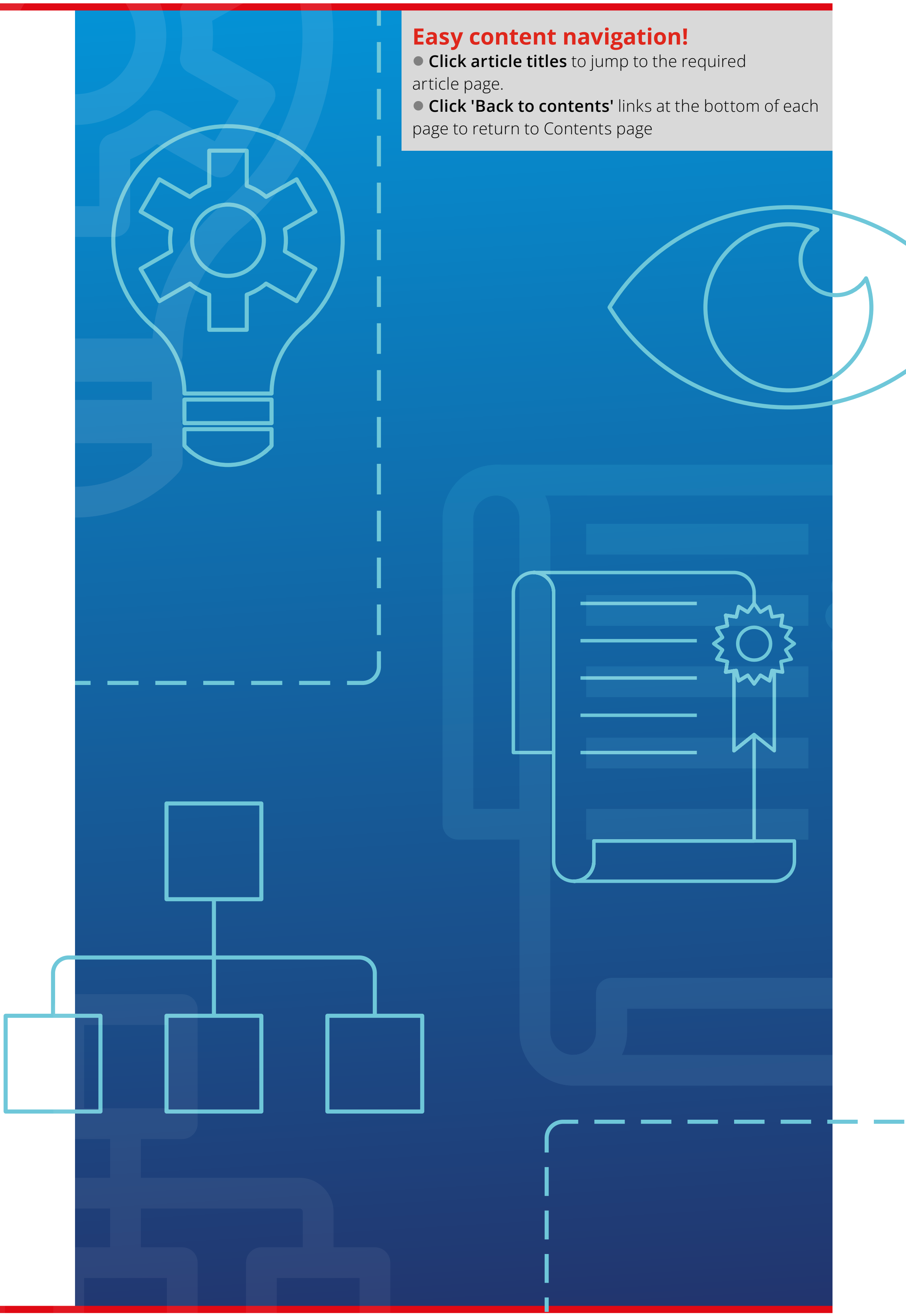
On forces being risk averse around FOI:

“There's no organisation more risk averse when it comes to data than justice organisations and, particularly, policing. One of the challenges in policing is that information can be intelligence, so people are very reluctant to let go of that information or to disclose it.”

David Hamilton
Scottish Information Commissioner

BACK TO CONTENTS

Contents



Easy content navigation!
● **Click article titles** to jump to the required article page.
● **Click 'Back to contents'** links at the bottom of each page to return to Contents page

Forewords

Raising the profile and the standard of information management in policing

CoPaCC and Policing Insight have been producing informative reports since the early days of the business, on topics including police and fire governance, the Brexit implications for policing, police use of drones, body-worn cameras, ICT and police contact management.

This, our latest report, looks at police information management. Given the range of high-profile challenges currently facing policing – such as workplace culture, professional standards, recruitment and training, violent and gendered crime, serious and organised crime, and wellbeing – it's probably not an issue that has been at the forefront of many people's minds. Even when it comes to technology, there are plenty of other 'sexy' subjects, from facial recognition to automation and exciting new applications of artificial intelligence, that have been discussed and debated more widely. However, without addressing the fundamentals of police information management, these policing opportunities and crime challenges cannot be tackled effectively.

If the information isn't accurate, consistent, up-to-date, compliant and accessible, then the systems, processes and applications – and therefore the policing outcomes that derive from them – are going to fail, regardless of how clever, sophisticated and expensive they are!

> **"If the information isn't accurate, consistent, up-to-date, compliant and accessible, then the systems, processes and applications are going to fail.**

This independent report, produced by the Policing Insight team and commissioned by Capita, sets out the case for information management to be dragged out of the back office and into the light as a core policing function. We are pleased to present insightful contributions from current and former practitioners and stakeholders in policing information management, as well those with expertise in information compliance and ethics. We thank all the contributors for taking the time to support this work.

We hope the report contributes to raising the profile of this policing function that's crucial for successful policing outcomes, and supports the efforts of those working to raise standards and effectiveness of information management for the benefit of frontline policing.

Ian Barrett
Director of Publishing and Development, Policing Insight

Leveraging information and data is the best way to improve productivity and services

Capita's purpose is to enable organisations to maximise delivery on their desired outcomes, and it is widely understood that leveraging information and data is now the best way to secure productivity and service improvements.

However, across change programmes we all too often see internal issues associated with the state of information management hindering organisational change – and in some cases blocking timely progress all together.

So what's going on? Given that information is known to be central to effective policing within the UK, why is it that there appears to be so much 'drag' on aspirations for change generated by this particular area? What are the issues and what can be done to better support organisations and accelerate change?

While information management is a complex subject area, it is one in which progress is increasingly been made across other sectors, with much of the learning and tools developed being directly transferable into policing. Indeed, knowledge and capabilities have in many cases already been packaged into relevant professional expertise and modern platforms / toolsets which suppliers, including ourselves, are able to offer.

> **"Knowledge and capabilities have in many cases already been packaged into relevant professional expertise and modern platforms / toolsets which suppliers, including ourselves, are able to offer.**

To assist with understanding and direction setting, Capita is delighted to sponsor this report, which we hope will help to shed light on the state of play in respect to the digital management of information within UK policing.

We are particularly keen that the report provides an opportunity for leading experts to articulate their understanding of the main issues and opportunities. We look forwards to discussing the reports content and listening to the feedback.

Dave Tonks
Digital Transformation Consultant, Capita

Introduction

Information management is the priority to achieve policing's 'quantum leap' in technology

The potential of technological advances to transform policing has generated enormous excitement across the sector, but much less attention is paid to the fundamentals needed to actually deliver this kind of tech-driven policing.

Speaking at the most recent Association of Police and Crime Commissioners (APCC) and National Police Chiefs' Council (NPCC) Partnership Summit, Chair of the NPCC Gavin Stephens presented a straightforward but ambitious message.

Policing, he said, is about to take a "quantum leap forward", with new technological developments that are "awe-inspiring, daunting and exciting all at the same time". These tools, he argued, will be "the single biggest driver of reform in policing", transforming how forces across the country seek to protect the public from harm.

It's a story we hear again and again from those working at the highest levels of policing; artificial intelligence (AI), data analytics, robotic process automation, live facial recognition – the potential of all of these innovations is creating enormous excitement across the sector, and rightly so. They really could be transformative.

However, there's much less attention paid to the fundamentals needed to enable this kind of tech-driven policing. No minister, police and crime commissioner, or chief constable discusses information management in the same terms as they discuss AI. Data protection and data quality, information management and information assurance – these functions simply don't win the same headlines as the latest piece of whizzy tech.

And yet, information management underpins so much of what policing does. If forces wish to deploy new technologies effectively, the fundamentals need to be in place. Ensuring the information held by policing is of sufficient quality – that it's properly collected, indexed, managed and, where necessary, deleted – is crucial when it comes to using tools like AI fairly and effectively.

Information management is much more than just a technological enabler, important though that is. It's also about guaranteeing that the sensitive information held by policing is handled correctly, to protect the public from harm and ensure the safety of police employees.

'A wake-up call'

The recent Police Service of Northern Ireland (PSNI) data breach on 8 August 2023 – which saw the personal information (including names, locations and departments) of 9,483 police employees accidentally published online – illustrates exactly the kind of risk facing forces today.

As **a recent review of the incident** led by Temporary Commissioner and NPCC Lead for Information Assurance and Cyber Security Pete O'Doherty explains: "This is considered to have been the most significant data breach that has ever occurred in the history of UK policing." This assessment reflects both the "nature and volume of compromised data" released by the PSNI, and the risk this breach posed to police employees working and living in a society with a complex political history.

The review points to a range of challenges for the PSNI to consider, many of which will be common to other police forces across the UK. There was evidence of a "failure to recognise data as both a corporate asset and liability", a "siloed approach to information management functions", and "an organisation not seizing opportunities to better and more proactively secure and protect its data, to identify and prevent risk earlier on, or to do so in an agile and modern way".

This isn't, of course, a one-off – even for policing. As the same report acknowledges, plenty of other data breaches have already occurred. Recent cases saw Norfolk and Suffolk Police accidentally release details of vulnerable victims, Cumbria Police publish private pay data on the force website, and the Metropolitan Police and Greater Manchester Police suffer data breaches after cyberattacks on their supply chains.

Having the capability to protect your information is non-negotiable for any modern police force. As T/Commissioner O'Doherty writes in his foreword to the review: "This report not only serves to highlight how the breach occurred and what measures must be taken to prevent this from ever happening again, it is [also] a wake-up call for every force across the UK to take the protection and security of data and information as seriously as possible."

> **"The tools and technologies which are essential to fighting crime have culminated in an astonishing amount of data now being held on police systems. Ultimately, this is a positive phenomenon for policing.**

Common standards

Underpinning all of this is the reality that policing now collects more information than ever before. The tools and technologies which are essential to fighting crime – from the well-established (eg fingerprints, CCTV, ANPR) to the relatively fresh (eg near-ubiquitous body-worn video, modern biometrics, smartphone downloads, social media material) – have culminated in an

Continued overleaf ↘

astonishing amount of data now being held on police systems.

Ultimately, this is a positive phenomenon for policing. New investigative methods that pull on different sources of information can help solve complex crimes. Body-worn video footage provides high-quality evidence to facilitate prosecutions. Digital records on shared IT platforms are far easier to use and share than documents stuck in old filing cabinets – even though paper records still exist in some police stations today.

However, this also adds considerable complexity. Different types of data need to be managed in different ways, while varying legal frameworks create their own specific obligations on policing.

The Freedom of Information Act 2000 mandates the release of non-personal data held by public bodies (such as police forces) if a member of the public submits a formal request. The General Data Protection Regulation (GDPR) creates duties to properly safeguard personal data relating to police employees, such as any medical information held on a frontline officer. And the Data Protection Act 2018 Part 3 specifically regulates processing of data for criminal law enforcement purposes. The last of these is, by some margin, the most significant piece of data legislation affecting UK policing.

> **"The real danger is that policing's undervalued and underfunded information management function will fall further and further behind.**

There is longstanding national guidance available to forces to help them navigate this area. The **Code of Practice on the Management of Police Information (MoPI)** was produced in November 2005 by the College of Policing, setting out common standards for information management in forces across England and Wales. It demonstrated a clear commitment to try and establish harmonised rules around the use of police data – even if the reality was considerable variation at the local level.

In 2013, **a report by HM Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS)** into police intelligence failings concerning Jimmy Savile argued that when MoPI is followed, "the system works as intended". But it also noted: "We are not sufficiently assured that implementation has matched expectations due to the discretion afforded to individual chief officers in following MoPI, nor are we sufficiently confident that the guidance is being given full effect in all forces."

Nearly two decades later, in July 2023, the College of Policing has produced **a revised Code of Practice on police information and records management**, updated to reflect new legislation and offer guidance on managing corporate information. This new document should go some way to making this complex field more accessible – though the critical test is whether it leads to common standards actually taking root nationwide.

Business critical

Even with new guidance and greater awareness around the risk of data breaches, managing information properly is not easy. Forces are still recovering from years of funding cuts which have left them struggling to keep pace with even basic demand. Many police IT systems are outdated, with their replacements often suffering from delays and spiralling costs. And, across England and Wales, the 43-force model means that there are rarely common standards on information management, even as most forces use data for almost exactly the same functions.

There is an urgent case for modernisation and professionalisation of policing's information management functions. The mass of data held by policing is growing and will continue to grow ever faster, adding even more complexity.

Existing systems already hold astonishing amounts of information; the Police National Database currently contains 2 billion records from 220 individual databases maintained by over 50 law enforcement bodies. As of 2021, the Police National Computer contained records relating to a total of around 13 million people.

The real danger is that policing's undervalued and underfunded information management function will fall further and further behind. This will undermine the "quantum leap" NPCC Chair Gavin Stephens is so keen to deliver around technology, waste the crimefighting potential of data held by forces, and risk further data breaches which pose real dangers to the police and the public.

It's for all of these reasons that this report, published by Policing Insight, presents the case for treating information management as business critical, rather than a mere back-office function. The headline from all the interviews we've conducted – with senior police leaders, regulators, and subject matter experts with decades of experience both inside and outside policing – is simple. Information management should be prioritised by policing, and it should be prioritised now.

CLICK HERE
Report
Protecting From Within
A review commissioned by the PSNI and NIPB, into the PSNI data breach of 8th August 2023
nipolicingboard.org.uk

CLICK HERE
Professional practice
Code of practice on the management of police information
Prepared by: National Centre for Policing Excellence
www.college.police.uk

CLICK HERE
Report
Mistakes were made
HMIC's review into allegations and intelligence material concerning Jimmy Savile between 1964 and 2012
www.hmic.gov.uk

CLICK HERE
Professional practice
Police information and records management Code of Practice
Statutory Code of Practice and guidance setting national principles for police information and records management.
www.college.police.uk

Information is power – and modern policing needs a more strategic approach to its management

Although AI and technology are increasingly making headlines and attracting investment, there is still a concerning lack of focus on the fundamentals of information management.

For policing, as with modern businesses in every sector, information really is power. Collecting, exploiting and, where required, disposing of data is a crucial obligation for forces across the world – partly to meet legal duties and ensure regulatory compliance, but also to make the most of the information they hold to facilitate criminal investigations and protect the public.

The importance of information is increasingly well understood within policing today. It's almost impossible to attend any national conference without hearing someone emphasise the need to use information and data – whether structured records or unstructured material – to improve efficiency and effectiveness across the board.

And yet, while AI and technology increasingly win the headlines and attract lucrative investment, focus on the fundamentals of information management is still lacking. Getting the basics right just doesn't seem to garner the attention needed.

'Down the corridor'

Throughout the interviews conducted for this project, Policing Insight was told time and again that information management is generally not prioritised within policing. It usually sits low down the hierarchy within forces.

> "While AI and technology increasingly win the headlines and attract lucrative investment, focus on the fundamentals of information management is still lacking. Getting the basics right just doesn't seem to garner the attention needed.

Wayne Parkes, a former Chief Digital Data and Technology (DDaT) Officer at the Police Digital Service (PDS), suggested that information management is viewed as a back-office function that isn't the concern of others in policing. "It's just not mainstreamed at the moment. It's a view that there's a specialist department down the corridor doing information management, it's their problem not mine… But it's everybody's responsibility. I think we need to get to proper maturity in this area, and policing has been pretty slow getting to that point."

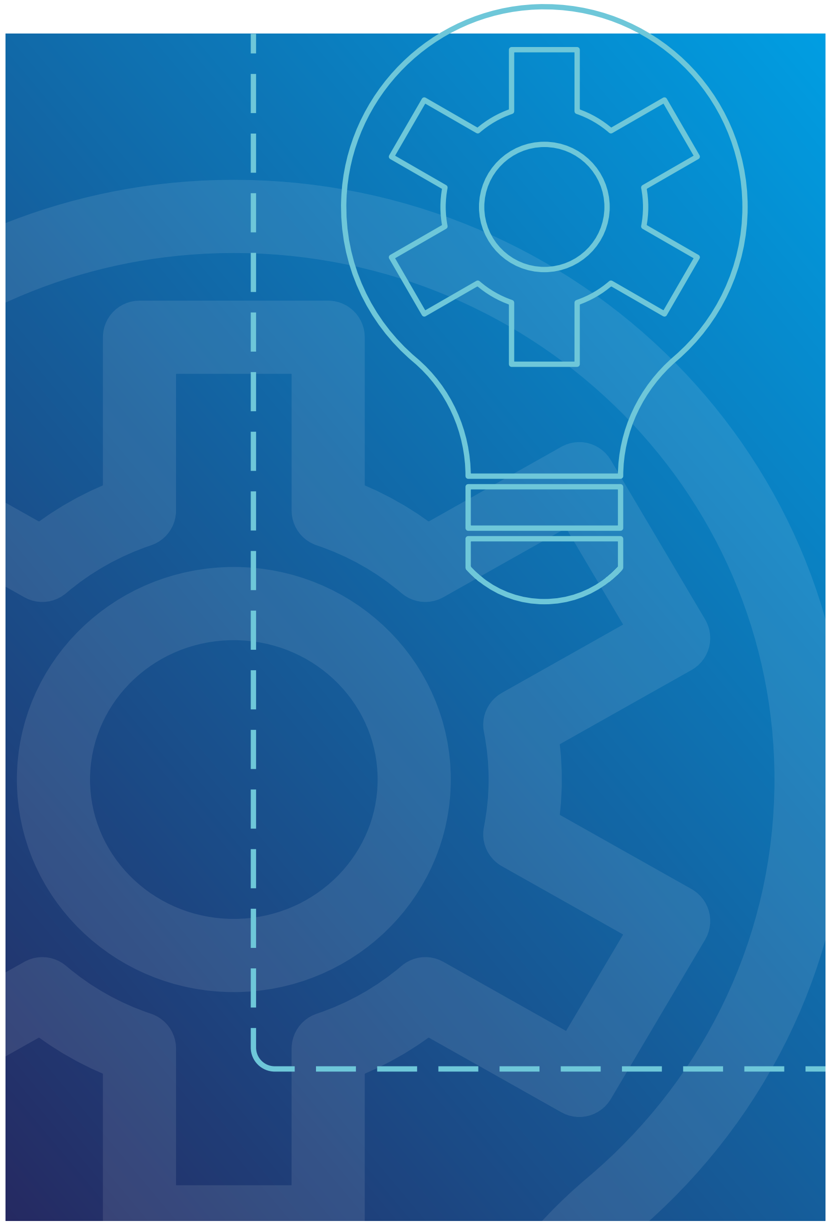
This feeds into how staff in these functions are rewarded, with poor pay limiting the ability to hire the best and most capable working in this space: "If we talk about information managers being treated like admin staff, they're also paid like admin staff, which is part of the problem," he added.

The same perception of information management was raised by Giles Herdale, an independent expert in digital investigation and data ethics and an Associate Fellow at RUSI, in strikingly similar terms. "I think there's a persistent issue with the fact that information management is not seen as frontline policing activity. It's seen as a back-office function and, by definition, a back-office function is something that is lower priority.

"I think that is entirely contrary to the actual weight of importance that information management has. I mean, how do police officers decide which way they turn when they leave the police station? How do they decide where they spend time, or who poses the greatest threat to the public, or who is at the greatest risk of harm within any community? How are any of these decisions made?"

Despite its importance as a function – and despite the fact that, as Aimee Smith, Director of Data at the Metropolitan Police and Chair

Continued overleaf ↘



of the National Police Data Board explained, staff working in these functions are “absolutely worth their weight in gold” – information management teams are not especially influential. In fact, she argued that “they are completely outvoiced and outnumbered.”

Operational failures

This persistent undervaluation of information management creates a range of risks. Perhaps the most significant is that ineffective use of the information held by policing can result in intelligence failures which have deadly consequences.

As Policing Insight highlighted in a **recent piece on the police data challenge**, the development of nationwide data systems has often directly resulted from high-profile information management failures. The creation of the Home Office Large Major Enquiry System (HOLMES) was spurred by evidence of inadequate intelligence-sharing in the Yorkshire Ripper Case, while the development of the Police National Database (PND) followed the same poor practice in relation to the Soham murders.

Little surprise then that Giles Herdale identified operational failures as a major risk not valuing information management properly. “All the indicators would be that it’s not a perfect situation. There’s a number of high-profile examples of where things have gone wrong in particular forces, whether that’s data breaches affecting personal data of officers and staff or even members of the public, or the fact that there have been operational failings due to the inability to link together relevant data fields.

“You can look at almost any public inquiry, serious case review or domestic homicide review. Any of these things will highlight poor information management, poor performance on putting together an intelligence picture, and failure to make timely decisions. These things have huge consequences; they’re also things where the public has an expectation that the police will be both competent and trustworthy in using personal data.”

Owen Sayers, a specialist in information assurance and data protection and former architect for national police data systems, pointed to similar examples of operational failure. He cited **an infamous case from 2008**, in which the Crown Prosecution Service and Met Police were forced to pay out around £600,000 after a child witness had his details passed to a gang he was testifying against. The child and his family were also placed in a police witness protection scheme for their own safety. The dangers associated with information management failures should not be underestimated.

Problems at the top

Concerningly, several interviewees suggested that even those at the very top of policing don’t recognise the importance of information management to their forces. This may reflect some of the issues already identified: it’s often seen as a back-office function that’s low down the hierarchy, and the work of data protection staff can, by some, be viewed as a blocker to new ideas.

But, Aimee Smith argued, senior officers need to develop a better understanding of why this is such an essential and potentially risky area of police business. “Chiefs are not properly having that conversation at the moment because they don’t truly understand the risk that they’re holding with data. Everyone can keep shunting it into the future, but this issue is going to be brought increasingly to the fore.

> **“You can look at almost any public inquiry, serious case review, or domestic homicide review. Any of these things will highlight poor information management, poor performance on putting together an intelligence picture, and failure to make timely decisions. These things have huge consequences.”**
> **Giles Herdale**
> Associate Fellow, RUSI

“When people talk about legacy systems”, she added, “most of them aren’t actually legacy. They’re operational systems with data they shouldn’t hold in them, and we’re asking cops to make decisions off of them.”

The answer has to be greater attention to this topic, especially given the threat to public confidence if things go wrong. “I get the whole ‘I don’t want to use my budget now’ thing, but the risk is that we’re sitting on a ticking time bomb. People are getting more cognisant that grandfather rights [which enable policing to delay complying with the Data Protection Act in some cases] are starting to expire or of the threat of getting told off by the regulator, than they are about the actual impact on members of the public if we do things with data that we shouldn’t be holding.”

In practical terms, what are these dangers? “The risk is that, as data-savvy solicitors and criminals understand [that we’re starting to use information we shouldn’t hold], they’ll go after process in court and we will start to lose cases,” said Ms Smith.

Continued overleaf ↘

In fact, Owen Sayers told Policing Insight, there's a chance that some chiefs don't even realise they are legally responsible for some national data systems in operation today. "Every national system should have a designated data controller. They are legally responsible and can be sued directly… But I know for a fact that in two of those cases, those chief constables had no idea that they were the designated lead controller and that this meant they have personal legal responsibilities."

The great enabler

The flipside of all of these risks is that information management can be the key to unlocking so much of what policing wants to achieve. It can enable more effective approaches to tackling crime by providing high-quality data or facilitate the next wave of advanced technology – including the AI tools creating such excitement across the sector.

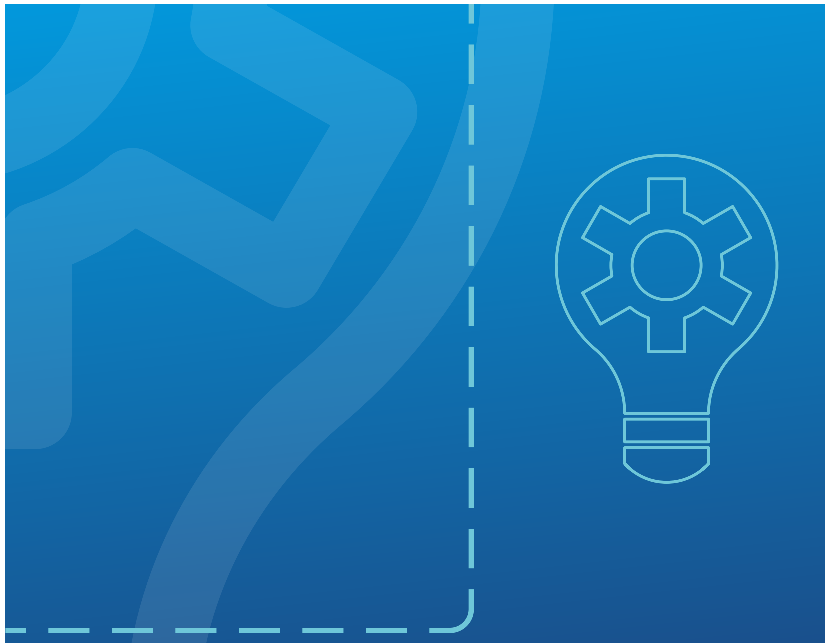
But that can only be achieved if the fundamentals are in the right place. It's still the case, Wayne Parkes argued, that policing doesn't recognise the value of the assets it holds. "If you look at a commercial company, they guard their data massively because it's their competitive advantage. They think: 'I'm never letting this information out, we'd be screwed.' But for policing, which holds such sensitive information, the mindset should be the next level up from even that private sector perspective. Instead, it's not, it's actually the next level down."

If policing's data (and the information management function that sits alongside it) were properly valued, the potential could be vast. Aimee Smith described the opportunities that could be created in the medium term: "If you do this now, your successor will have brilliant data upon which they can feel ethically and legally secure that their data science and whizzy AI will work brilliantly and reduce crime."

But this does require a view beyond the immediate crisis – a recognition that fixing the fundamentals will make it possible to deploy advanced tools in the future. "How many of the forces have done the due diligence in terms of their record holdings to make sure that they're actually ready, when they decide to push the button on the whizzy analytics?" she added. "We all want to do it – that's the opportunity data could bring, isn't it?"

However, even away from the high-tech applications, information management underpins so much of everyday policing. Dave Tonks, Digital Transformation Consultant at Capita, made this case plainly during an interview for this project. "The level of investment in this area is not – from a time and attention or from a money perspective – at the level it needs to be.

"Information is the major enabler of policing efficiency and effectiveness. It's been the case for years and we've been saying it for years. But, if it is the major enabler, why aren't we doing more in this space? If you can get the information right, everything else is serviced by it – both in terms of operational insights and in terms of efficiency of activity… We need a proper strategic approach which asks where policing can get the biggest bang for its buck from investment in information management."



> "I get the whole 'I don't want to use my budget now' thing, but the risk is that we're sitting on a ticking time bomb… The risk is that, as data-savvy solicitors and criminals understand, they'll go after process in court and we will start to lose cases."
> **Aimee Smith**
> Chair, National Police Data Board

The case for change

There is agreement on one thing. As Emily Keaney, the Deputy Commissioner of Regulatory Policy at the Information Commissioner's Office, told Policing Insight: "We need modern police forces that can use data in a way that enables them to do their job better and protect all of us more effectively." Getting information management right is the key to unlock these possibilities.

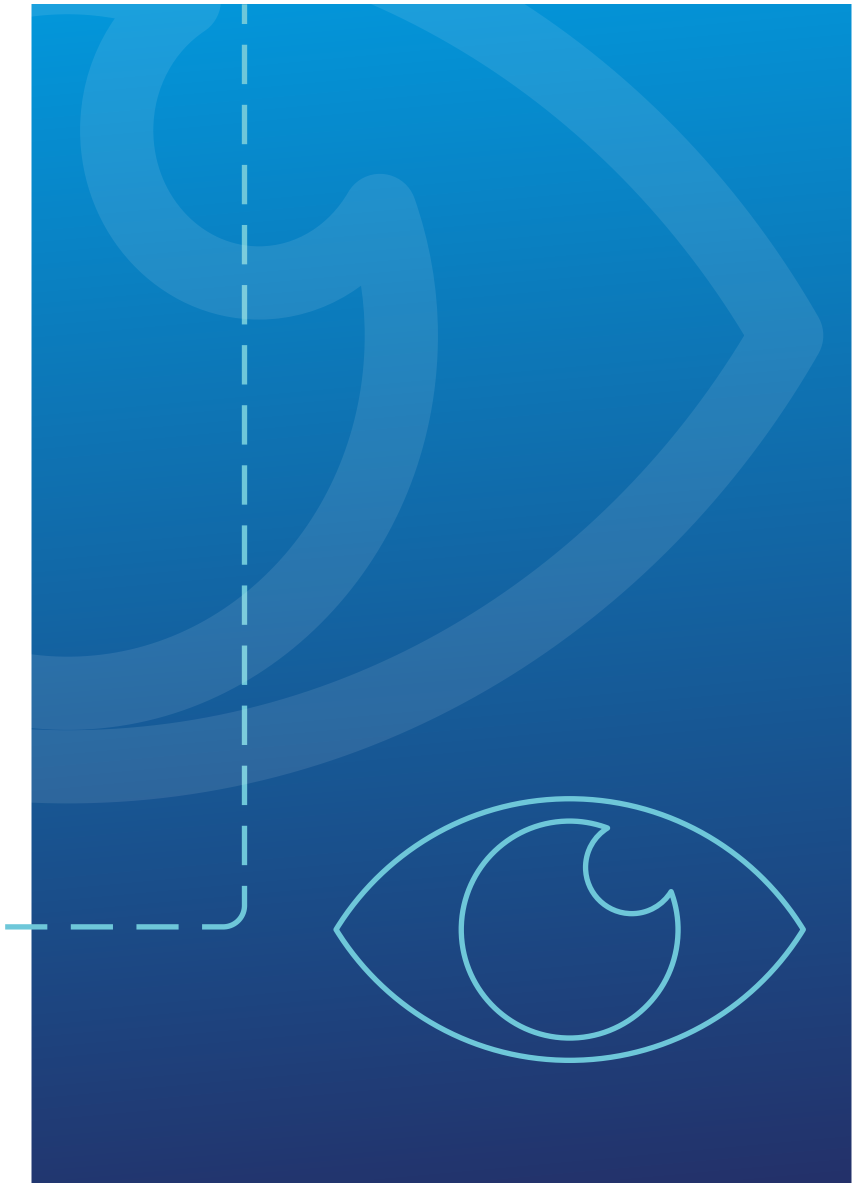
For now, it's clear that information management is not valued highly enough within policing. Digging more deeply into what's actually happening on the ground – the current state of play – reveals a troubling picture too.

CLICK HERE
Article
The police data challenge: Complexity, scale, and the search for the 'single source of truth'
policinginsight.com
Policinginsight

CLICK HERE
Article
Payout of £600,000 after child witness put at risk
bbc.co.uk
BBC

The fractured landscape: technical debt, divergent practices and weak central guidance

Poor capacity, underinvestment, technical debt, limited standardised working and weak central guidance are just some of the serious issues currently facing police information mangement.



Understanding the true state of play in any area of policing is always difficult. With such a large number of different forces doing things in their own way – in England and Wales at least – it can be challenging to identify a coherent picture across the country.

But when it comes to information management, some common themes do emerge. Evidence of poor capacity and underinvestment, a legacy of technical debt, limited standardised working across forces, weak guidance from the centre, and even a concern that this guidance is now outdated – there's a catalogue of serious issues facing policing.

Capacity and underinvestment

At the most fundamental level, it's clear that because information management is viewed as a mere back-office function, it also fails to receive the level of investment it needs. This has created significant capability problems in an area of policing which requires people who can deal with complicated regulations and complex data systems.

This case was put concisely by Aimee Smith, Director of Data at the Met and Chair of the National Police Data Board, who asked a simple question to forces who aren't willing to build up their capabilities in this area: "Have you really got the right capacity and subject matter expertise in your organisation to truly understand and manage the data that you've got?"

In fact, as Giles Herdale (an Associate Fellow at RUSI) argued, this reflects a more pronounced long-term failure to develop information management into a fully-fledged function. "Policing has never really had a professional information management arm – it's tended to be a role that's tagged onto other roles, rather than being a core competency."

This is all underpinned by a persistent refusal to boost investment in this function, even as forces become increasingly aware of the problems they face. Wayne Parkes, former PDS Chief DDaT Officer, described this issue in the context of retention, review and disposal (RRD) regimes. "You have some forces almost whispering to say, 'Look, our RRD is terrible. We know about it and we want to try and address it to some extent'. But it's also kind of a message of 'don't mention this to anybody either'.

"I think that's actually a fairly normal situation in forces. People in policing do recognise it, but it's very difficult to get it high up the investment agenda. I've been in those discussions and tried to take some of this forward in policing. But in the end, it's about what forces decide should take priority: catching more criminals or protecting the information you've got?"

> "You have some forces almost whispering to say: 'Look, our retention, review and disposal is terrible. We know about it and we want to try and address it to some extent.' But it's also kind of a message of 'don't mention this to anybody either'."
>
> **Wayne Parks**
> Former PDS Chief Digital Data and Technology Officer

Messy development and technical debt

While a properly empowered and funded information management profession would be an improvement, there are deeper challenges facing policing in this area. One of these

Continued overleaf ↘

problems is the confusing web of police IT systems which have developed over time.

This is not simply about delays in delivering major IT programmes – although findings such as the extremely critical **Public Accounts Committee report** from 2021, which stated that the Home Office had "wasted both vital time and scarce funding without making any meaningful progress in replacing the Police National Computer and the Police National Database", tell their own story. It's really about how systems interact – or rather, how they don't.

Giles Herdale explained this problem, saying: "There is this historic legacy of police information systems, the fact that they are highly localised, quite archaic and not as connected even within individual police forces as they should be."

This is a common message from those working in this area. Dave Tonks, Digital Transformation Consultant at Capita, contrasted what's desirable for frontline staff with what's really available to them. "You want a new application as an officer that, with a touch of a button on a mobile device, provides you with a search of all systems that are relevant when you go out to a job. You want it to make sensible decisions about what to filter and show you.

"But the challenge is that the pipeline is very mixed and quite 'Heath Robinson' in nature. What we've often got are digital solutions which have been developed on a tactical basis, often creating a degree of technical debt to deliver something in the short term that ultimately makes it harder and harder to deliver the next thing."

This impact is felt directly by those trying to manage data, according to Stephen Russell, Director of Data, Strategy and Technology at Warwickshire Police. "The technical debt of policing historically has meant that managing the sheer volume of data is hard on the siloed system. There isn't this perfect view of one single system. There's a feeling that the systems, processes and governance aren't enabling us to manage our data."

Divergent practices

Another common feature is the remarkable diversity of practice around information management at the local level – a frequent challenge in the 43-force model across England and Wales in particular. While this creates opportunities for individual forces to produce best practice (a topic covered later in this report), it means that common standards are rarely found nationwide.

Emily Keaney, Deputy Commissioner of Regulatory Policy at the Information Commissioner's Office, described this nuanced picture at the local level in policing, with limited evidence of standardisation between forces. "We definitely see examples where the police are trying to be joined up and consistent across the forces. But I think, as you would expect with the model that we have, we also see examples of police forces doing it quite differently.

"We see forces doing things together as well, which may not necessarily go across all of policing, but you might have four or five forces doing something together, for example. We see a real mix, quite honestly. But there is a lot of benefit in exploring an overarching approach because it just makes things a lot more consistent."

Of course, much of this goes beyond what can be achieved by transforming the approach to information management in policing. It is, as Stuart Hyde, former NPCC Lead for Data Compliance, explained: "Mainly because the structure of policing is pretty old-fashioned. We're designed around a Victorian structure of local authorities. How can you have police forces now where one's got 36,000 officers and another has 1,000 officers? The structure is still basically the same as it was then."

Weak central guidance

This is reinforced by what some we interviewed described as a weak central voice around information management. Without consistent and compelling guidance from the national level down, it becomes more challenging for forces to adopt common standards.

> **"The technical debt of policing historically has meant that managing the sheer volume of data is hard on the siloed system. There isn't this perfect view of one single system. There's a feeling that the systems, processes and governance aren't enabling us to manage our data."**
>
> **Stephen Russell**
> Director of Data, Strategy and Technology, Warwickshire Police

Wayne Parkes suggested that this reflects a divided centre. "The centre is quite broken up into siloes and I think that's part of the problem. All of those central bodies have the same challenge around information management. Though the College of Policing, for example, would say they own practice on this, it's a lot more of a technical and digital world that they're not really into."

There's simply not enough clear leadership, he argued. "Where is the information management best practice 'centre of excellence' or something else at the centre that's going to start driving this? I don't see it anywhere at the moment."

This problem is felt keenly at the local level, according to Stephen Russell. "Sometimes there could be a little more clarity. There should be more explicit guidance than us having 27 versions of email retention across forces. The Met and Warwickshire might be working at different scales, but fundamentally they're doing the same thing.

"Those structures could give clearer guidance as opposed to sitting on the fence. With information management, I have found there is more varied practice when applying the principles into actual reality – for example, with rules around how long you keep your data. It seems odd to me that the same institutions could treat their data quite differently."

This recognition that forces are essentially engaged in the same activities makes a stronger case for common practice – a point

Continued overleaf ↘

Current state of play

Giles Herdale supported too. “There is clearly scope for more and better co-ordination across 43 forces. Although police forces are different shapes and sizes and operate in different communities, they’re all doing variations of the same set of activities. That’s reflected in the fact that they have a very common set of requirements as far as data collection and management is concerned.”

Outdated regulation

At the same time, there are additional concerns that the standards which the centre attempts to promote are no longer fit for purpose. They simply haven’t kept up with how far the modern world, and policing with it, have moved in terms of the use of information.

Across policing in England and Wales, the management of police information (MoPI) principles have defined how forces should handle the material they hold since 2005. According to the **MoPI guidance still present on the College of Policing website**, they “provide a way of balancing proportionality and necessity that are at the heart of effective police information management”.

“They also highlight the issues that need to be considered in order to comply with the law and manage risk associated with police information.”

But Aimee Smith questioned whether this approach is still up to the task. “Part of policing’s problem is that we’ve invented the rules and framework by which we do RRD – that’s MoPI. I honestly think we’re high time for a review of whether that is still the right application of the rules, or whether a more pragmatic application of a regime closer to the Criminal Procedure and Investigations Act might be better.

“You could then get rid of some things quicker and hold onto some things longer on a risk basis. That would be a sector-wide resolution to this problem going forwards. MoPI is massively out of date, and was invented at a time when – even though the principles are sound – we had filling cabinets and basic technology systems.

“We’re designed around a Victorian structure of local authorities. How can you have police forces now where one’s got 36,000 officers and another has 1,000 officers? The structure is still basically the same as it was then.”
Stuart Hyde
former NPCC Lead for Data Compliance

“We’re not in that space now. We’re in a whole database model where we’re linking information sets together, and you can’t easily pull apart whether this particular bit of information should still exist. You can’t do it because you’ve connected it all in. As a regime, MoPI is harder to apply now.”

To its credit, the College of Policing has recently revised its authorised professional practice (APP) around information management, with a **new code of practice** that evolves the MoPI principles somewhat. Ms Smith told Policing Insight that forces should be adopting this new APP, even if a MoPI-style approach is not the full answer.

But both Aimee Smith and Wayne Parkes questioned whether this new APP has been promoted widely enough within policing – indeed, it appears to have made little impact in the sector.

“There’s a new code of practice out now, but what I haven’t seen off the back of that is what happened when MoPI first came out,” explained Wayne Parkes. “Back then, there was a national programme and all kinds of efforts to implement MoPI.

“[With the new code], I don’t hear it being talked about particularly, I don’t come across it anywhere. I don’t see any real programmes of work and I’m still doing work with forces… I think there’s still a long way to go.”

Bright spots

Despite these tough criticisms, which suggest that policing is far from where it needs to be on information management, this is not all a tale of doom and gloom.

There are bright spots across England and Wales, according to those we interviewed. In Scotland, both the single force model and a long-term mindset when it comes to digital transformation appear to have created a more coherent approach to information management. In the next part of this report, we’ll explore some of this best practice and what other forces can learn from it.

CLICK HERE
Report
House of Commons Committee of Public Accounts
The National Law Enforcement Data Programme
committees.parliament.uk
UK Parliament

CLICK HERE
Professional practice
Management of police information
college.police.uk
College of Policing

CLICK HERE
Professional practice
Code of Practice on police information and records management
college.police.uk
College of Policing

Building partnerships and improving training can deliver more best practice

While each police force has the flexibility to innovate, few excel at information management, reflecting its low perceived importance. In reality, it is critical to strategic policing.

A defining feature of the 43-force model in England and Wales is that there are dozens of policing bodies doing things differently. This creates obvious problems in delivering a co-ordinated approach and making sure common standards are embedded system wide. However, at its best, it enables local innovations to bubble up (as Police Chief Scientific Adviser Professor Paul Taylor **recently put it**), with examples of best practice emerging from force level.

In the context of information management, this benefit has yet to be fully realised. There are some examples of forces doing innovative work in this area – even if a unified UK force (Police Scotland) is the most commonly cited example of excellence – but in general, with information management still low down the pecking order in policing, the evidence of best practice is limited.

Limited best practice

Those we interviewed were clear that this is one area where few forces excel. This undoubtedly reflects the fact that forces do not generally treat information management as business critical, despite its strategic importance to policing. Aimee Smith, the Met's Director of Data and Chair of the National Police Data Board, made exactly this point. "I think there isn't one force that particularly shines. There will be a force that shines around their improvements in data quality and another that shines around use of data analytics. Is there one that shines on legacy holdings? No, not really.

"West Yorkshire probably comes closest. But that's because they listen to their head of information governance. That person is a trusted adviser to their board and so the force properly understands what the risks and challenges are."

> "There isn't one force that particularly shines. There will be a force that shines around their improvements in data quality and another that shines around use of data analytics. Is there one that shines on legacy holdings? No, not really."
> **Aimee Smith**
> Chair, National Police Data Board

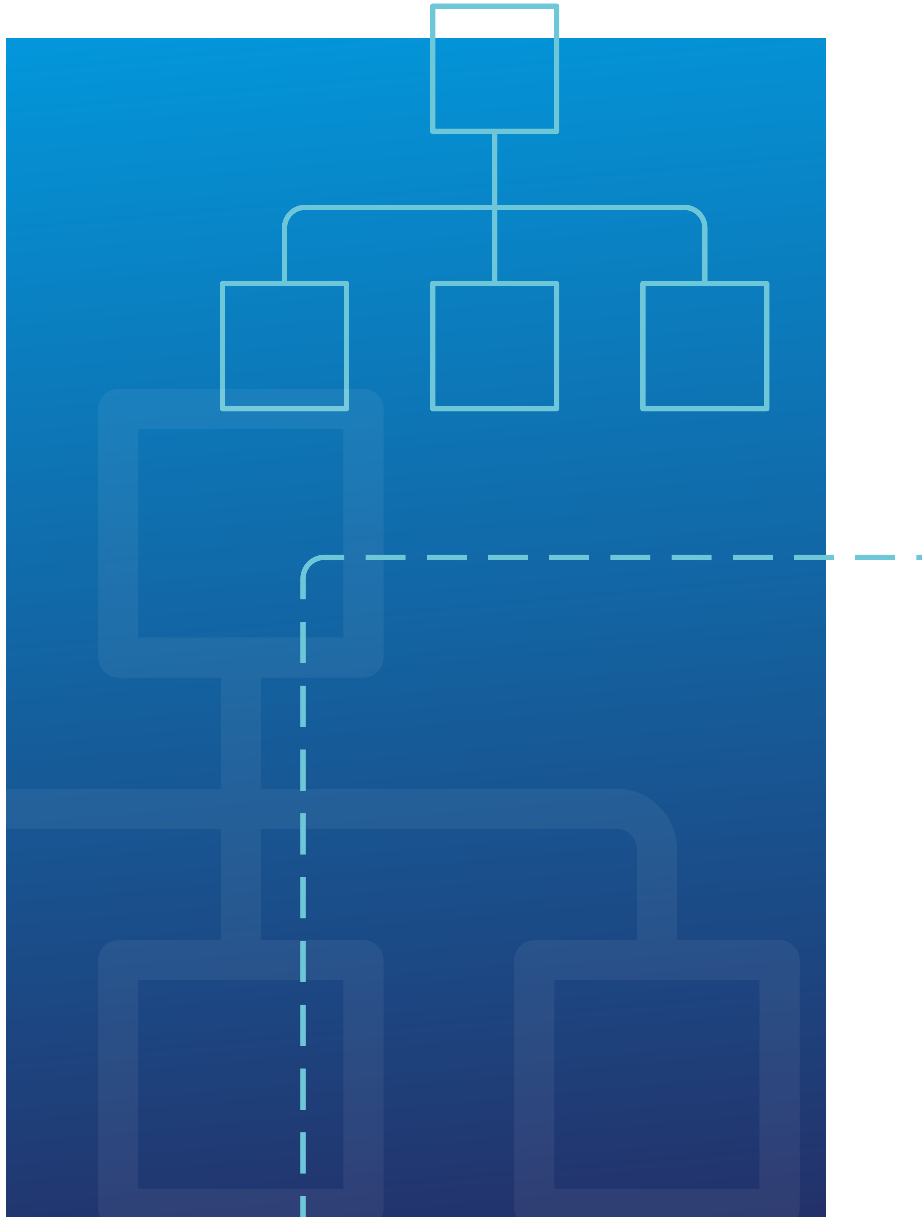
A similar message came from Associate Fellow at RUSI, Giles Herdale, who stressed that excellence is not effectively encouraged by the centre either. "There are pockets of best practice – as ever with policing, it's not that everything is universally terrible – but the good practice is often happening in spite of national systems and processes, rather than because of it."

He did point to one force as taking a more cohesive approach. "For example, in the West Midlands, I saw the difference that a big focus on creating a strong data-driven hub (which later became the National Data Analytics Service) had… There was real consideration of how data could drive decision-making and the skills and capabilities necessary to support that work. Unfortunately, at the moment, there are too few examples of that kind of holistic approach across policing."

Scottish success

One force reserved for particular praise was Police Scotland. Having moved from an eight-force regional structure to a unified single organisation in 2013, its cohesive approach to data systems

Continued overleaf ↘



and information management was regularly cited as something that forces across England and Wales could learn from.

Aimee Smith pointed to the force's work to digitise legacy records, for example. "I'd be surprised if 80% of forces [in England and Wales] don't have physical records somewhere. They will have an archive. The reason I say that is because it would have taken some real foresight to have invested in a digitisation programme – which Police Scotland is actually doing."

At the same time, its performance in complying with the Freedom of Information Act has been generally positive, according to David Hamilton, the recently appointed Scottish Information Commissioner. "It's quite clear that policing does have its own unique operational challenges in terms of the freedom of information sphere… I think, by and large, it looks pretty promising in how Police Scotland have been dealing with that. They're a team with a lot of experience behind them."

> "There are pockets of best practice – as ever with policing, it's not that everything is universally terrible – but the good practice is often happening in spite of national systems and processes, rather than because of it."
> **Giles Herdale**
> Associate Fellow, RUSI

Dave Tonks, Digital Transformation Consultant at Capita, also pointed to the work that senior leaders at his former force have done to improve information management. "Police Scotland is doing a really good job in terms of data strategy, because of the imperative created by its establishment in 2013. Denis Hamill, who is the Chief Data Officer there, has managed to secure investment in splitting data from the systems.

"He's looking to move to a federated data model, where you bring the data together and you then leverage it centrally. That means you have all your information in one place, and you can dip into that for the system you need. It's a single national information management system."

This creates a more iterative approach to data too, where new information can be collected, fed back into the centre, and then used to update records across all relevant systems. "If a system picks up a new nominal through a public protection arrangement and that's regarded as best quality information – such as if somebody got married and changed to a new surname – the write-back arrangement comes into effect," continued Dave Tonks. "All of the source systems that feed the central hub now need to take the new information into effect in their own records."

There is, he added, "a lot to this", but when it works, it demonstrates a far more advanced approach to managing police information than we see elsewhere in the UK.

Working with the regulator

Though it's clear that common information management standards are far from embedded across the system, there are some interesting case studies where policing – whether individual forces or national bodies – has worked proactively with regulators to meet their legal obligations in this area.

Emily Keaney, the Deputy Commissioner of Regulatory Policy at the Information Commissioner's Office (ICO), described engagement with central policing bodies. "A good example of us working proactively is what we've done with the College of Policing. We've worked with them quite a bit on several occasions to advise on guidance that they're developing and to ensure that data protection is considered. I think most recently we've worked with them on their records management guidance as an example.

> "There's no requirement as far as occupational competence in information management is concerned as a senior police officer, and that's really unacceptable in this day and age."
> **Giles Herdale**
> Associate Fellow, RUSI

"With the NPCC, we've engaged on a variety of different things. One of the pivotal ones that I remember was during Covid. The NPCC approached us about sharing information across different organisations about vulnerable individuals, so that they could manage issues around Covid and people potentially defying the rules."

The Deputy Commissioner pointed to more localised engagement too: "We've also had examples where police forces have approached us, particularly where they're doing things that are new or innovative or complex. The ICO has a regulatory sandbox, which is how we work intensively with organisations trying to use data in new, innovative ways to help them understand any compliance issues and work through them.

"One of the current projects in that sandbox is with Thames Valley Police, where we're working with them on the Thames Valley Partnership programme. It's a cloud-based environment where different partners, including police, local authorities, fire and rescue services, can share data and use analytics to

Continued overleaf ↘

understand the picture together. That's a good example of where organisations come to us with challenges they want to solve, and we're working closely with them on that."

These examples, especially Police Scotland, show that some parts of UK policing are excelling around information management. However, best practice remains limited. To develop a wider culture of excellence in this area, understanding for those at the top of policing needs to improve. If more leaders in the sector understand the importance of information management, they'll be better placed to direct additional work.

Giles Herdale made an interesting comparison between the rigorous training top cops receive in some key skills and the poor development around information management. "Any senior police officer, almost without exception, will talk about how they've done their gold public order command training or gold firearms training. They'll talk about how rigorous and challenging that process was, how they need to do regular refresher training and show occupational competence in that role.

"Have any of those police officers ever done anything similar in the information management field? Have they ever seen that as being a core competence necessary to exercise command responsibilities in a highly complex modern environment? There's no requirement as far as occupational competence in information management is concerned as a senior police officer, and that's really unacceptable in this day and age."

Stuart Hyde, the former NPCC lead for Data Compliance, pointed to a similar issue. "When I was running that area in policing, it was the early days of information assurance and it became almost a challenge to get policing interested.

"If you said to many chiefs now for example, 'how does your firewall work?', the vast majority of them would never have even looked at a firewall in operation – what it looks like, how you can set it up, what you can put in, what you can take out. I think that curiosity that most cops have for criminality just doesn't apply to anything that's based on a computer."

Learning from the private sector

There are also lessons to learn from the private sector regarding information management. This reflects the reality that, as Dave Tonks noted (in line with several other interviewees), "UK policing is a long way behind the commercial sector".

Stuart Hyde made the case that public-private collaboration could help to reduce risks of data loss, for example. "Forces should work very closely with the private sector and with the National Cyber Security Centre. There's lots of information, help and availability there to ensure that forces do look after themselves."

> **"The police need to be the intelligent and informed customer. You're not going to be that intelligent customer unless you engage with private companies and go out and look at them."**
>
> **Stuart Hyde**
> Former NPCC Lead for Data Compliance

More generally, policing needs to be willing to engage with the private sector, even before contracting for a specific service, he added. "The police need to be the intelligent and informed customer. You're not going to be that intelligent customer unless you engage with private companies and go out and look at them."

Owen Sayers, a specialist in information assurance and data protection and former architect for national police data systems, pointed to a wide range of private sector expertise in this space. "In the service provider landscape, we've got them. The organisations I'm talking about are the ones that the police moved away from in order to put their stuff on Microsoft Cloud… They've got these skills in spades.

"There are about half a dozen or more providers already there today that could do it. Where we've got the lack of talent and the lack of vision, sadly, is in that IT tier in policing."

This isn't to suggest that the private sector has all the answers, however. While interviewees were clear that there is plenty more to learn from industry, there are some areas where the market still needs to catch up.

As Aimee Smith noted, the biggest crime recording systems – CONNECT and NICHE – don't offer the right options for policing around retention, review and disposal. "At the moment, the forces can't buy anything that does this any better, because there's two big competitors in the market and neither are offering a solution for this issue upfront."

Building best practice

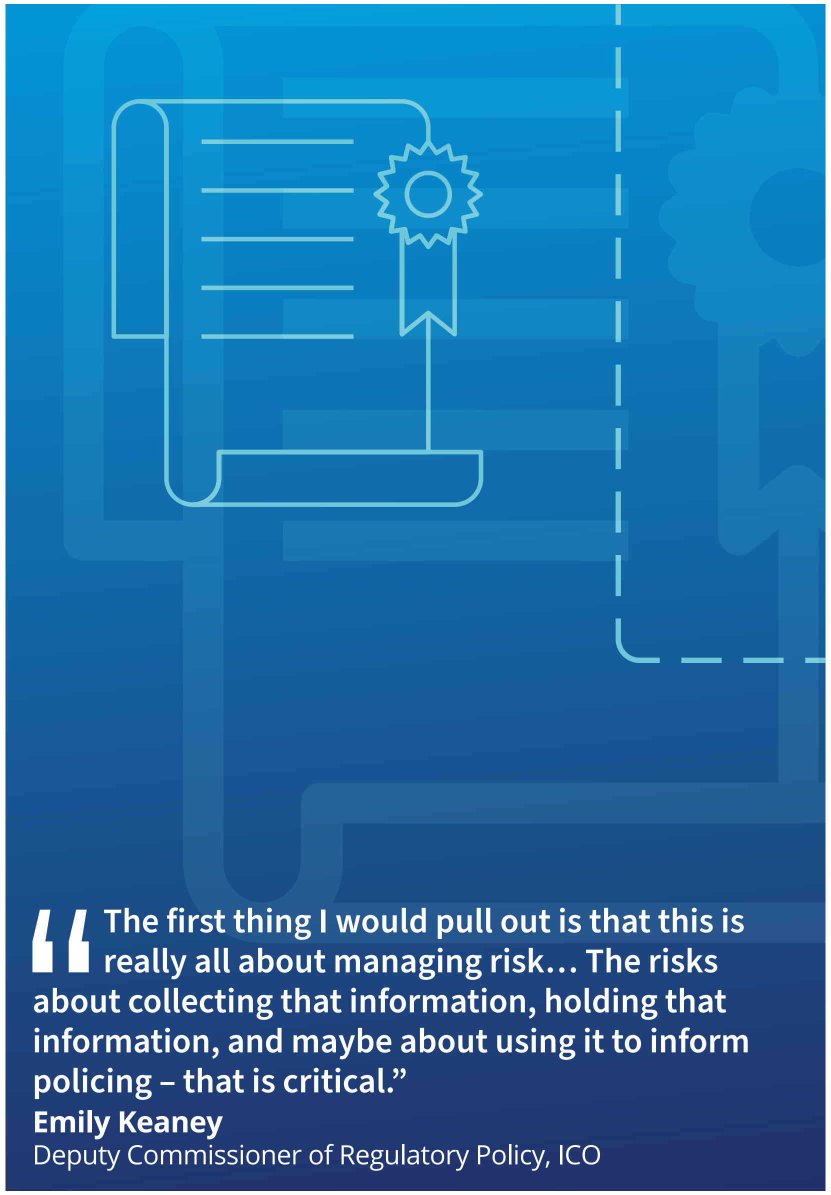
The challenge around best practice can be summed up in an observation Giles Herdale offered during an interview for this project. "Out of the initial phases of Operation Soteria, where the research team engaged with 14 forces, none of them could actually say how many rapes and serious sexual offences (RASSO) they were dealing with. Despite the fact that RASSO is a massive priority for forces, their information management systems didn't support them to give those data points."

Information management is business critical to so much that policing wants to get right, but it's still not treated as such within forces. Until this function is given the attention and investment it needs, best practice – across England and Wales at least – is likely to remain relatively thin on the ground.

CLICK HERE
Article
Policing Minister urges UK forces to 'fully capitalise' on use of 'transformative' AI
policinginsight.com
Policinginsight

Compliance and collective responsibility will be key to effective police information management for the future

As paper records have declined and vast collections of digital data have become the norm, the opportunities for policing to exploit this material have grown rapidly, but complying with data protection regulations is no easy task.



> “The first thing I would pull out is that this is really all about managing risk… The risks about collecting that information, holding that information, and maybe about using it to inform policing – that is critical.”
> **Emily Keaney**
> Deputy Commissioner of Regulatory Policy, ICO

Complying with data protection is no easy task for UK police forces. This is both because of the complexity of the legislation and guidance in this area, and the sheer mass and diversity of information that policing now collects.

As paper records have declined and vast collections of digital data have become the norm, the opportunities for policing to exploit this material have grown rapidly. At the same time, ensuring all of this information is handled properly has become a bigger challenge than ever before. Reaching compliance with all the relevant legislation is a real challenge in policing.

A new era of information

Wayne Parkes, former PDS Chief DDaT Officer, set out the challenges for forces collecting data in the digital age. “The amount of multimedia information collected now is growing exponentially. This creates a whole load of challenges in terms of both how you handle it and how you manage it through the information life cycle. It obviously makes it easier to dispose of things when they’re digital, rather than paper based. But getting those review processes right on every bit of information is an absolutely enormous effort.”

Compliance duties do add considerable complexity to the work of policing, according to Stuart Hyde, former NPCC Lead for Data Compliance. “The restrictions to ensure police use data properly and don’t breach data protection are immense – and that slows the process down. A cop can’t just go out and start filming things, then check what they’ve recorded on their mobile phone later and post it on Twitter. They are, quite rightly, responsible for the data they collect. They need the authority to do that, and it needs to be proportionate, legal, and accountable.”

Stephen Russell, Director of Data, Strategy and Technology at Warwickshire Police, emphasised how much work this can create for forces. “If I take a piece of data, I can end up applying several bits of legislation which can be competing. There’s not one rulebook for data management. Depending on how you’re using the data, in what context, and in what format, a different set of rules can apply. So it’s a complicated landscape and not an area that forces will always go to for investment.”

Complying with the Data Protection Act

As Stephen Russell pointed out, policing may hold and use data that is affected by many different pieces of legislation. For example, GDPR becomes relevant to policing when forces process personal data for non-law enforcement purposes, such as the HR records of a police staff employee. Complying with the Freedom of Information Act and the Regulation of Investigatory Powers Act may be just as important, depending on the data being exploited and how it’s handled.

Generally though, Part 3 of the Data Protection Act (DPA) 2018 is the most significant piece of legislation – this covers law enforcement processing of data, a point made clear in **guidance from the Information Commissioner’s Office (ICO)**.

Emily Keaney, Deputy Commissioner of Regulatory Policy at the ICO, explained the obligations on policing. “Data protection, broadly speaking, is principles-based regulation. So police need to consider those principles when they are thinking about how they’re using data. The first thing I would pull out is that this is really all about managing risk… The risks about collecting that information, holding that information, and maybe about using it to inform policing – that is critical.

Continued overleaf ↘

Reaching compliance

"The other things I would pull out are around necessity and proportionality. It has to be necessary, you shouldn't be collecting data just on the off chance. You need to be clear about what you're collecting data for, what you're trying to achieve, and what risks might come out of that. And then, you have to make sure that what you are doing is proportionate to what you're trying to achieve."

Aimee Smith, the Met's Director of Data and Chair of the National Police Data Board, explained that policing is currently exempt from achieving full compliance with the DPA. "We were given 'grandfather rights' by the government because the technology systems we're all on are so old and some don't have delete buttons, so we can't discharge our responsibility for the review, retention and disposal (RRD) of data under our own policy. Government also said: 'We'll give you until a date in the future, by which time you must have invested in a technology system that allows it.'

"The problem is, NICHE doesn't have an RRD solution now and, by the time it does, it will take us past the date when grandfather rights cover us. For forces using CONNECT, there actually is an RRD module. But you can't turn it on because forces don't have confidence that the new records you're creating in the system are high enough quality." The current solutions in the market, she said, don't solve these compliance problems.

The issue is that forces just aren't preparing: "Whatever force it is – whether small, medium or large – they haven't been doing their due diligence in anticipation of the grandfather rights [expiring]."

In other words, a new approach is needed. Forces should adopt the updated professional guidance recently issued by the College of Policing, while also digitising their paper records and putting them into NICHE or CONNECT. But the long-term goal, she argued, should be to prioritise a few key datasets, improve the quality of data held in them, and place them in a cloud-based system. "At that point, the current types of records management system – like NICHE – will become a very old-fashioned way of doing things."

Cloud challenges?

One specific challenge around information management was raised by Owen Sayers, a specialist in information assurance and data protection and former architect for national police data systems.

He argues that the **Data Protection, Privacy and Electronic Communications Regulation 2019**, a statutory instrument that updated the Data Protection Act to reflect the impact of Brexit, creates issues for cloud-based systems used in policing.

"It had quite a big effect that most people didn't realise. It meant that you are only able to send data outside of the UK if you can't achieve your processing outcome by any other means. And, if you're one of a small number of organisations, you're never allowed to send data outside of the UK to anyone other than another law enforcement agency. That's the nub of the problem.

"Today, we've got a number of service providers who are providing services to policing for national and sub-national systems who cannot legally process that data. This covers a lot of systems – including major providers of cloud services in policing."

Anything that technically hosts data outside of the UK is in breach of the rules, he claims. "And any service used by policing, even a UK-based company, would need to have contract terms that are properly aligned with the Data Protection Act and staff who are vetted to meet police requirements. The current cloud services don't do that either", he added.

To fix things, he believes data needs to be processed "100% inside the UK" and comply with vetting terms. "You cannot have people sitting outside of the UK supporting the system – that's an international transfer. You have to move to being a fully UK sovereign model." This might look like a "regional federated cloud model which could be very easily created" by using the many "empty or semi-empty data centres we have in policing around the UK".

This would entail a major shift in approach. Deputy ICO Commissioner Emily Keaney offered an alternative view when asked what law enforcement must do when placing data into cloud systems. "Under the Data Protection Act 2018, law enforcement agencies may use cloud services that process data outside of the UK where appropriate protections are in place.

"They would need to think about the risks in the same way that they would need to think about risks associated with transfers more generally. We would expect them to be thinking about those risks in terms of where controllership sits, who has access to the data, and ensuring they've put into place appropriate mitigations for that."

> "Today, we've got a number of service providers who are providing services to policing for national and subnational systems who cannot legally process that data. This covers a lot of systems – including major providers of cloud services in policing."
> **Owen Sayers**
> Information assurance and data protection specialist

Recent reporting indicates that the ICO could be doubling down on this approach. An article by Computer Weekly states that the Scottish Biometrics Commissioner published a letter – since removed from its website – claiming the ICO is set to approve use of US cloud infrastructure by UK forces. It suggests that the ICO believes a UK-US data sharing agreement supersedes domestic data protection laws.

Enabling, not blocking

Compliance with data protection regulation is, fundamentally, a legal duty on forces. But that doesn't mean those working in data protection functions are there to hamper the operational work of UK policing. Instead, data protection can be a critical friend and an enabler of best practice, rather than a blocker of new ideas.

As someone with experience of leading the national approach to

Continued overleaf ↘

data compliance, Stuart Hyde made this very argument. "I think information assurance is just seen as a pain in the neck – 'how do we get around this?', not 'how do we comply with it?'. Or you get the other side, which is 'No, you can't do anything because of data protection', resulting in a very risk-averse environment.

"What you actually want is a lawfully audacious environment – a term they used when they created the National Crime Agency. You want people that are knowledgeable and want to push the boundaries, rather than trying to avoid doing things because it's difficult. Information assurance is difficult, you've got to have protections in place, but that doesn't mean you can't undertake any action or do nothing. You need to have that capability."

> "What you actually want is a lawfully audacious environment – a term they used when they created the National Crime Agency. You want people that are knowledgeable and want to push the boundaries, rather than trying to avoid doing things because it's difficult."
>
> **Stuart Hyde**
> Former NPCC Lead for Data Compliance

This risk that forces become unduly cautious was cited by those in regulatory roles too – such as David Hamilton, the Scottish Information Commissioner, who made this point in the context of FOI requests. "There's no organisation more risk averse when it comes to data than justice organisations and, particularly, policing. One of the challenges in policing is that information can be intelligence, so people are very reluctant to let go of that information or to disclose it."

Emily Keaney agreed that data protection should not simply be about blocking new ideas so as to avoid addressing complex risks altogether. Staff working in these roles should seek to be enablers of good practice and help policing navigate risks. "I think part of a data protection officer's role is to understand what their [police] officers are trying to achieve. What problem are they trying to solve? What's the issue they're trying to tackle? And help them, working in partnership.

"Because the other danger can come when a data protection officer is seen as somebody over there who's going to stop me doing stuff. Actually, the role of a data protection officer is not to say 'data protection says no', it's about 'OK, how can I help you do that in a way that manages risks properly?'."

Collective responsibility

At the same time, given how important this area should be to forces – especially in the digital age – complying with data protection isn't simply a job for those working in one specific part of policing. Instead, several interviewees suggested that this should be a collective responsibility, with everyone in policing being conscious of how data protection obligations could affect their own work.

As Emily Keaney explained: "I think part of the answer is that it can't just be seen as the responsibility of the data protection officer. There needs to be a cultural understanding, driven from the top, that this is the responsibility of everybody.

"Everybody has responsibility for thinking about basic good practice when it comes to data. Some of the cases where we see things go wrong can be the result of a mistake by an individual, such as sending something that they shouldn't have done. Everybody needs to have this in their minds. And that means there needs to be training and support available for everybody."

Given how important information management is to the everyday work of forces, the case for collective responsibility is even stronger. Indeed, as Aimee Smith notes, poor practice around information management could eventually have direct consequences for those on the operational side. "I think it's about whether HMICFRS moves to the point where they start assessing not just data integrity as they do now, but expand their thinking around data integrity and quality to include how you took organisational or operational decisions based on that data. Then your records management really does come under scrutiny."

According to many of those we interviewed for this report, the chances of information management being prioritised within UK policing are limited – with two exceptions. Some kind of a crisis – a vast and headline-grabbing data leak with substantial fallout, for example – might provoke radical action and remedial investment in this area. Equally, a decision by a regulator like HMICFRS to really dig into how forces are approaching information management might lead policing to sharpen up its act.

This crisis-driven response is obviously not desirable. Effective information management is strategically important to policing. It can enable efforts to solve serious crime, provide the necessary foundations for leveraging new forms of technology, and safeguard the personal data of individual citizens across the UK. Greater attention to this area is needed now, to prevent the next crisis from taking place at all.

Information management should be recognised as a fundamental, business critical part of policing. As Stephen Russell told Policing Insight: "Data management is like painting the Forth Bridge. It's a constant energy and effort… data quality and governance are parts of your business that you will always need to be focusing on."

CLICK HERE
Guidance
Law enforcement processing: Part 3 DPA 2018; and sharing with competent authorities under the GDPR and Part 2 DPA 2018
ico.org.uk
ico. Information Commissioner's Office

CLICK HERE
Legislation
The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) (No. 2) Regulations 2019
www.gov.uk
GOV.UK

CLICK HERE
Article
ICO prompts confusion over police cloud legality
www.computerweekly.com
ComputerWeekly.com

Connect legacy and disparate data to improve police productivity and performance

Unlock the full potential of your data with our expertise, tools, and processes designed to seamlessly connect and leverage your information assets.

Discover how Capita's information management services can transform your operations.

Geoff.thompson@capita.com

www.capita.com/services/services-police-forces-and-judiciary/information-management

Achieve transformative outcomes including:

Instant accessibility

Our automated workflows digitise and index files for rapid access and greater accuracy, offering a single view of multiple data sources without the risk of misplaced files.

Full auditability

Manage document lifecycles comprehensively with a full audit trail from collection, storage to destruction, ensuring complete accountability.

Compliance and security

Documents are stored securely and can only be accessed by authorised staff in line with regulatory, legal and quality requirements, while back-ups make disaster recovery easier.

Increased productivity

Centralise and simplify access to information, allowing officers and staff to focus on their duties rather than having to search through reams of data and information.

Cost-savings

Reduce the costs associated with storage and managing high-volumes of legacy data and documents by consolidating physical and digital files into one location.

Seamless integration

Introduce solutions that seamlessly bridge your existing infrastructures and deliver immediate impact without significant upfront investment.

A Policing Insight Report in partnership with Capita

Capita

CoPaCC
the police governance experts

Published by Policinginsight