

BRIEFING · SEPTEMBER 2026

Artificial Intelligence in *UK Policing and Public Safety*

What the evidence actually says, what the oversight bodies expect,
and what can safely be done now.

Neil Catton

Independent Technology Strategist · Technology, Ethics & Human Purpose

NEILCATTON.COM

Prepared as a market briefing. Every figure is traced to a regulator, an inspectorate, an ombudsman, a select committee, a court, published legislation, or an operator speaking on its own record.

A note on the numbers

Almost every published figure about AI in policing was produced by someone selling AI into policing. This briefing leaves those out, and says which ones.

A chief officer reading a briefing of this kind will check one figure. If it does not hold, the rest of the document dies with it. So the rule applied throughout is narrow: a number appears here only if it can be traced to a named regulator, an inspectorate, an ombudsman, a select committee, a court judgment, published legislation, or a police force speaking on its own record about its own operations. Supplier accuracy claims, conference statistics and adoption percentages of unknown provenance are absent.

Naming what was excluded is more useful than any statistic that survived, so here is the list.

EXCLUDED — AND WHY

“Six million hours of police time, equivalent to three thousand extra officers.” Repeated across government and policing communications. No published methodology, no baseline, no definition of an hour released. It appears in this briefing only as an attributed government ambition, never as a measurement.

“£115m AI centre.” The figure given in the Police Reform White Paper in January 2026. The centre was funded at £75m over three years when it launched in June 2026. Both are used here, in their own words, and the movement is noted rather than resolved.

Twenty-one forces still using a particular assistant after the West Midlands failure. Attributed to a broadcast investigation whose method is not published. Excluded. No published figure exists for how many forces still use the tool, and that is the most consequential gap in the public record on this question.

Every supplier claim encountered — facial recognition accuracy rates, time savings for report-writing tools, detection rates for digital triage. None traceable to an operator speaking on its own record. None used.

Custody image volumes. The widely quoted figures for how many facial images police hold, and how many belong to people never convicted, date from 2022 and 2024. The legal position is stated here without them.

The figures a reader is most likely to check are sourced as narrowly as possible. The Metropolitan Police’s false-alert rate for live facial recognition comes from the force’s own annual report and is quoted in the force’s own framing. The stop and search disproportionality ratio comes from the Home Office statistical bulletin of November 2025, covering the year ending March 2025, rather than from the statistics dashboard, which still presents 2022–23.

One case is used on a narrower basis than the rest. In July 2026 the Crown Prosecution Service placed two non-existent authorities before the High Court in an extradition matter. The judgment is not published on the National Archives caselaw service and has not been read for this briefing. The case therefore appears only for what the CPS itself has said about it on its own record, and that limitation is stated where it appears.

Position stated as at 14 September 2026. Several matters described here were unresolved at that date and are identified as such in the text.

The wider market

Policing has more money than it has had in years, and almost none of its technology spending is available for anything new.

The 2026–27 settlement put up to £21.0bn into the policing system in England and Wales, an increase of up to £1.3bn on the year before — 6.7 per cent in cash terms and 4.4 per cent in real terms. Territorial forces alone received up to £18.4bn. Inside that total sits £119m of Home Office police reform investment for the year, covering a new national AI centre, facial recognition rollout and data capabilities.

Set against that, the National Audit Office found in November 2025 that forces spend around £2bn a year on technology, and that 97 per cent of it goes on maintaining legacy systems. That single proportion is the real context for every AI business case in this sector. The competition for the money is not another AI tool. It is the estate already running.

£21.0bn

Policing system funding, 2026–27, up to. An increase of up to £1.3bn on 2025–26.

97%

Of around £2bn annual force technology spending goes on maintaining legacy systems (NAO).

43

Territorial forces in England and Wales, buying technology separately. The White Paper proposes fewer, larger forces.

The workforce the technology is meant to support has been shrinking against rising demand for over a decade. Police officer numbers fell 6 per cent and police staff numbers fell 13 per cent between 2010 and 2025, while recorded crime rose 44 per cent per thousand population from 2015. In the 2026 national workforce and wellbeing survey, answered by 55,602 officers and staff, 45 per cent reported always or often feeling burnt out and 56 per cent reported always or often feeling fatigued or physically exhausted.

That combination — more money, a locked technology estate, a depleted and tired workforce — is why the productivity argument for AI lands so easily in this sector. It is also why the argument needs testing harder here than anywhere else. A tool that promises to give time back is being sold to an organisation that has no agreed way of measuring whether it did.

THE NUMBER THE AUDITOR COULD NOT FIND

The Home Office “does not yet have a shared definition of – or methodology for measuring – productivity”, and “does not know whether the anticipated £2.9 billion of benefits by 2027–28 will be realised”.

Sources — Written Ministerial Statement HCWS1285, Minister of State for Policing and Crime, 28 January 2026. National Audit Office, *Police Productivity*, HC 1380, 3 November 2025, paragraphs 2.12, 3.1 and 3.20. HMICFRS, *State of Policing 2025–26*, 8 September 2026. Home Office, *From Local to National: A New Model for Policing*, CP 1489, January 2026.

The pressure point

The capability is being nationalised. The accountability is not.

Everything being built is national. A national centre for AI, hosted by the College of Policing and funded at £75m over three years, will identify, test and scale tools across all forty-three forces, starting with pilots in up to ten of them during 2026–27 and scaling nationally from 2027. A national facial recognition system is funded at £26m. Forty additional live facial recognition units are being deployed as a nationally coordinated capability. The White Paper proposes a National Police Service that will buy technology “once rather than 43 different ways” and set mandatory national standards in technology and data.

The decision that goes wrong remains local, and personal. The Home Office’s own factsheet is explicit: individual chief officers decide what AI their force deploys, and remain accountable to a locally elected police and crime commissioner. National procurement, national assurance, national standards — and one name on the decision.

That is not a theoretical concern. It has already happened once, in public, and it cost a chief constable the end of a career.

WHAT THIS MEANS FOR A CHIEF OFFICER

A force will shortly be offered tools it did not select, assured by a body it does not control, trained on data it did not curate, to support decisions for which it alone is answerable. Nothing in the current arrangements changes where the accountability sits. The only question a chief officer can usefully ask is what they will require, in their own force, before any of it touches a decision about a person.

There is a second contradiction beneath the first, and it is one of sequence. The Government’s own consultation on facial recognition, published in December 2025, says the current legal basis “relies on common law powers and a patchwork of equalities, human rights and data protection laws”, that the framework “is complicated and difficult to understand”, and that it “does not give the police sufficient confidence to use it at significantly greater scale”. A member of the public wanting to understand the legal basis must navigate, in the Government’s own words, “four pieces of legislation and a police national guidance document”.

That consultation closed on 12 February 2026. As at 14 September 2026 its status on the Government’s own website reads “closed consultation awaiting outcome”, with the line: “We are analysing your feedback.” In the meantime the funded rollout has continued.

Sources — GOV.UK, *PoliceAI to speed up investigations and fight crime*, 10 June 2026. Home Office, *Police use of artificial intelligence: factsheet*, published 9 June 2026, updated 23 July 2026. Home Office, *Consultation on a new legal framework for law enforcement use of biometrics, facial recognition and similar technologies*, 4 December 2025, and consultation status page, last updated 23 July 2026. *From Local to National*, CP 1489.

What the sector is facing

One event contains the whole argument, and three arms of the state have now written it down.

On 24 October 2025 West Midlands Police gave a Safety Advisory Group a written risk report about a forthcoming Europa League fixture between Aston Villa and Maccabi Tel Aviv. The report stated that the most recent match Maccabi Tel Aviv had played in the United Kingdom was against West Ham United on 9 November 2023. There was no such fixture. The claim came from a search the force ran using a generative AI assistant. Away supporters were banned. The decision became a national political argument within days.

What happened next is the part that matters to a chief officer. The Home Secretary commissioned an inspection on 31 October 2025. The inspectorate reported on 14 January 2026 that the Chief Constable told inspectors the force “didn’t use artificial intelligence (AI) tools in the preparation of the SAG report”, while a different officer from the same force described the error as an AI hallucination produced by that assistant. The inspectorate recorded that it had received contradictory evidence from the force on the point. The written report also overstated the officer deployment at the earlier fixture and exaggerated the disorder, and the inspectorate concluded the force had portrayed the level of disorder as greater than it really was.

The Chief Constable retired on 16 January 2026. On 19 January the Independent Office for Police Conduct opened an independent investigation into the role officers and staff played in the decision, including a voluntary conduct referral from the force itself concerning one senior officer and a member of staff over the force’s use of AI. A referral concerning the former Chief Constable was accepted shortly afterwards. On 4 March 2026 the Acting Chief Constable, asked about the assistant, said: “I’ve turned it off.”

“West Midlands Police failed to do even basic due diligence on the information they received. This included false information that was generated by AI.”

Home Affairs Committee, Fifth Report of Session 2024–26, paragraph 13

The select committee established the rest of it on the record: that the use of the assistant “was unauthorised and not initially disclosed”; that the former Chief Constable was not told before giving oral evidence in January that the error had come from AI, and so did not intentionally mislead, but showed “a remarkable lack of professional curiosity” in not interrogating the evidential basis; and that the force was “overly reliant on inaccurate and unverified information” in a way that “undermined faith in the competence of West Midlands Police”.

THE FINDING INSIDE THE FINDING

The committee’s report makes five recommendations. Not one of them concerns police use of artificial intelligence, verification of AI-generated information, or AI governance.

Nothing in the accountability system changed as a result. The tool was turned off in one force by one acting chief constable. That is the whole of the institutional response so far.

Sources – Home Office, *Inspection of police forces’ contributions to safety advisory groups: West Midlands Police*, 14 January 2026, commissioned by the Home Secretary on 31 October 2025. Home Affairs Committee, *Maccabi Tel Aviv fan ban*, Fifth Report of Session 2024–26, HC 1553, 22 February 2026, paragraphs 13, 22, 24 and 50. IOPC, *IOPC announces independent investigation into Maccabi fans ban*, 19 January 2026. ITV News Central, 4 March 2026.

The record the technology is being fitted to

A model learns from what an organisation already does. The inspectorate has just published what that is.

In the thirteen force inspections completed under the current PEEL programme to 4 September 2026, not one force was graded outstanding or good for investigating crime. Seven required improvement and two were inadequate. The inspectorate's summary is that "none of the forces we inspected showed all the characteristics of good performance we expect to see", with persistent weaknesses in golden-hour evidence gathering, proportionate enquiries, allocation, investigation plans, victim updates and supervisory oversight. Across the same thirteen inspections, no force was graded outstanding or good for its custody environment.

The data those investigations produce sits in systems that were not built to share. The White Paper is blunt about it: forces "purchase local IT systems which operate in silos and cannot interact or share information", which "locks away useful data and restricts our ability to make informed decisions at a national level". The inspectorate adds that most police technology spending goes on sustaining old systems, and that the forty-three forces run many different ones while the Crown Prosecution Service runs a single case management system.

Policing's own strategy names the consequence without prompting. The *National Policing Digital Strategy 2025-2030*, published jointly by the National Police Chiefs' Council and the Association of Police and Crime Commissioners, states that "poor data quality, disproportionate retention and siloed data" continue to prevent policing realising value from what it has already bought.

INVESTIGATION

Nought out of thirteen

No force graded outstanding or good for investigating crime in the current inspection round. Seven require improvement, two inadequate.

40.9 per cent of victim-based offences were closed with no suspect identified in the year ending March 2026. The charge or summons rate for those offences was 7.3 per cent, up from 6.3 per cent.

DIGITAL EVIDENCE

Twenty thousand devices

Around 20,000 devices await forensic analysis, against a Government estimate that over 90 per cent of crimes now involve a digital element.

This is the queue every digital triage tool is sold against, and the reason the argument for assistive AI in investigation is the strongest one in the sector.

Two things follow for a chief officer. The first is that the case for AI in investigation and digital evidence is real, and is supported by the reader's own inspectorate rather than by a supplier. The second is that a model trained or tuned on this record inherits it. Where the record is thin — where a suspect was never identified, where a victim was not updated, where a file was not built — a system trained on outcomes will learn that thinness as normal.

Sources — HMICFRS, *State of Policing: The Annual Assessment of Policing in England and Wales 2025-26*, 8 September 2026. Home Office, *Crime outcomes in England and Wales 2025 to 2026*, 23 July 2026. *From Local to National*, CP 1489. NPCC and APCC, *National Policing Digital Strategy 2025-2030*, May 2025.

Where AI actually is

Less than the coverage suggests in most of policing, and considerably more than most people realise in one part of it.

Robotic process automation is in use in twenty-seven forces, with £10.1m invested to date. Audio-visual redaction is the clearest productivity case in the sector: the Home Office estimates that if adopted across England and Wales it could save around 11,000 days a month, roughly £1.7m a month, and as at September 2025 expected up to twenty-seven forces to take it up. Control-room triage of 101 calls, transcription, crime classification and document summarisation are all in live use or pilot across various forces.

Facial recognition is the exception in scale. Between September 2024 and September 2025 live facial recognition produced 962 arrests, over a quarter of them for offences involving violence against women and girls. Retrospective facial recognition runs at over 25,000 searches a month against the Police National Database.

THE MET'S OWN PUBLISHED FIGURES

In the year to 10 September 2025 the Metropolitan Police ran 203 crime-hotspot deployments across twelve command units. Approximately 3,147,436 faces passed the cameras, producing 2,077 alerts, of which 2,067 were true and 10 were false — in the force's own framing, one false alert for every 314,743 faces seen. The 962 arrests break down as 549 on court-issued warrants, 347 wanted by the force, and 85 for breaches of court orders or management arrangements for serious offenders.

In a six-month fixed-camera pilot in Croydon to March 2026, 173 arrests were made across 24 operations, more than 470,000 people passed the cameras, and there was one false alert, which produced no arrest.

The breakdown carries a caution the headline does not. Fifty-seven per cent of the arrests were of people already subject to a court warrant. Live facial recognition, on the operator's own numbers, is overwhelmingly a tool for finding people the system had already identified and lost, rather than for detecting offences it did not know about. That is a genuine capability, and it is a narrower claim than the technology is usually sold on.

What is missing is any national picture of the rest. The national AI centre has promised a public-facing register of local AI use. It does not exist yet. Until it does, the only way to know what a force runs is to ask that force.

Sources — Home Office, *Police use of artificial intelligence: factsheet*, updated 23 July 2026. NAO, *Police Productivity*, HC 1380, paragraph 3.8. Metropolitan Police Service, *Live Facial Recognition Annual Report*, September 2025, covering 11 September 2024 to 10 September 2025. Metropolitan Police Service news release, 13 May 2026. Home Office facial recognition consultation, 4 December 2025.

The challenges of using AI

The regulator has now audited six forces on the capability policing is scaling fastest, and made 107 recommendations.

In August 2026 the Information Commissioner's Office published an outcomes report and five audit reports covering West Yorkshire, Greater Manchester, South Wales and Gwent jointly, Essex and Leicestershire. An audit of the Metropolitan Police was scheduled for later in the year. All 107 recommendations were accepted or partially accepted.

The pattern in the findings is the useful part. Compliance was generally better for live facial recognition than for retrospective facial recognition – that is, better for the visible, controversial, heavily scrutinised capability than for the quiet one running at 25,000 searches a month. The problems the regulator identified in the quieter capability were inappropriate image sources, inappropriate retention periods, poor record-keeping of where data came from and how it was used, insufficient senior oversight and insufficient staff training. The ICO has separately raised concerns with the Home Office about algorithmic bias in the Police National Database, is monitoring cases of detriment, and has reserved the right to take further regulatory action.

“A false match can have serious consequences for people, including wrongful intervention, accusation or arrest.”

Information Commissioner's Office, 18 August 2026

Underneath that sits a question about the reference data itself. Retrospective facial recognition compares an image against custody images held on the Police National Database. In June 2012 the High Court held in *R (RMC) v Commissioner of Police of the Metropolis* that retaining the images of people who were never convicted in the same way as those who were, for a six-year period, was disproportionate and unlawful. The current position is not measurable from any primary source published recently enough to quote. What can be quoted is that the regulator found inappropriate retention periods in 2026, and that policing's own national digital strategy names disproportionate retention as an obstacle it has not cleared.

FOUR QUESTIONS A CHIEF OFFICER CAN ASK THIS MONTH

One. Which of our systems currently hold or query facial images, and on what retention rule?

Two. Who in this force is the named senior owner of each AI-assisted capability, and what did they sign?

Three. When a tool contributes to a decision about a person, what record survives of that contribution?

Four. If an assistant produced a wrong fact tomorrow and it reached a document, how would we know?

Sources – ICO, *Facial recognition in policing: earning public trust through strong data protection governance*, 18 August 2026, and *Facial Recognition in Law Enforcement Outcomes Report*. ICO, *AI and biometrics strategy update*, March 2026. *R (RMC) v Commissioner of Police of the Metropolis*, 22 June 2012. NPCC and APCC, *National Policing Digital Strategy 2025-2030*.

The threat side

In this sector the threat does not run at the money. It runs at the evidence, and at the machinery that holds policing to account.

Every sector in this series has a different threat shape, and assuming the last one transfers is the fastest way to get a briefing wrong. In insurance the threat was fraud against the firm. In social housing it was better-equipped residents. In energy retail it was impersonation of the redress route. In policing it is neither fraud nor impersonation. It is that the evidential and accountability machinery was designed for a world in which producing plausible material was expensive, and it no longer is.

The first verified British instances do not involve organised offenders. They involve the criminal justice system's own actors, and ordinary members of the public using ordinary tools for legitimate purposes.

Inside the system

In June 2025 the Divisional Court dealt with two cases together. In one, grounds for judicial review contained five case citations that did not exist. In the other, forty-five questionable citations were placed before a judge, of which eighteen did not exist at all. The court held that freely available generative tools “are not capable of conducting reliable legal research”, that those who use them have a professional duty to check the results against authoritative sources, and that “there are serious implications for the administration of justice and public confidence in the justice system if artificial intelligence is misused”.

In July 2026 the Crown Prosecution Service itself filed two non-existent authorities in an extradition matter before the High Court. The errors did not affect the outcome. The service's own account is that “the operative cause was human error in the failure to verify the authorities relied upon in formal submissions placed before the court”. The judgment has not been read for this briefing and the case is cited only for what the prosecuting authority has said about itself.

Against the case

In *R v FGD*, decided by the Court of Appeal on 24 July 2026, a prosecution turning on a single witness in a rape case was stayed by the trial judge as an abuse of process. A phone download had revealed two AI-generated documents on the witness's device: a summary of their own recollection, and a set of cross-examination questions with suggested answers. The Court of Appeal allowed the prosecution's appeal, holding that the prejudice could be managed through disclosure, cross-examination and directions to the jury. It also restated the rule and extended it to the new circumstance: the coaching of witnesses, by any means, is not permitted, and all witnesses should be discouraged from using AI to prepare to give evidence. The court invited the National Police Chiefs' Council, the Crown Prosecution Service and the Criminal Procedure Rule Committee to consider whether the use of AI in criminal proceedings should be regulated.

THE POINT FOR A CHIEF OFFICER

A complainant who used a chatbot to prepare for the worst day of their life nearly ended the prosecution. Nobody in that case did anything dishonest.

Sources – *Ayinde v London Borough of Haringey*; *Al-Haroun v Qatar National Bank QPSC* [2025] EWHC 1383 (Admin), Divisional Court, 6 June 2025. *R v FGD* [2026] EWCA Crim 918, Court of Appeal (Criminal Division), 24 July 2026. Crown Prosecution Service statement as reported, July 2026.

The volume, and the model itself

Two further pressures, one on investigators and one on the systems policing is about to depend on.

The Internet Watch Foundation assessed 8,029 AI-generated images and videos showing realistic child sexual abuse in 2025. Within that, 3,443 were videos, against thirteen in 2024. Sixty-five per cent of those videos fell into the most serious severity category, and 97 per cent of the victims depicted were girls. Every item of that material has to be found, classified, and in many cases viewed by a person, and every case built on it has to withstand a challenge about whether what it depicts is real.

At the other end, two oversight bodies have independently reported the same new pattern in their own casework. The Director General of the Independent Office for Police Conduct said in May 2026: “We do see more AI-generated complaints, people use AI to help them make a complaint... it does actually generate work, and when AI invents legislation as part of the complaint that gets more complicated.” The outgoing Commissioner for the Retention and Use of Biometric Material recorded in a report published in May 2026 that the team had “started seeing a small number of representations submitted by subjects... which they suspect may have been drafted with the assistance of AI”.

Neither of those is wrongdoing. People are using the tools available to them to engage with a system that is difficult to engage with. The consequence is nonetheless real: the IOPC received 7,088 referrals in 2025–26, a record, started 316 independent investigations, up 31 per cent on the previous year, and received 3,051 requests to review complaint outcomes, up 24.3 per cent. The proportion of those reviews upheld has fallen from 39.5 per cent in 2022–23 to 26.8 per cent in 2025–26.

Model security

The National Cyber Security Centre warned in December 2025 that prompt injection “may never be totally mitigated in the way SQL injection attacks can be”, that large language models are “inherently confusable” because they cannot reliably distinguish instructions from data, and that without addressing this misconception organisations risk breaches exceeding those seen from SQL injection in the 2010s. It explicitly challenges claims that prompt injection can be stopped, and advises secure design and resilience across AI supply chains instead of looking for a fix. For a policing estate that is about to connect language models to intelligence and case data, that is the security position, stated by the national authority, and it is not going to improve on a timetable.

Sources – Internet Watch Foundation, AI-generated child sexual abuse imagery research, 2026, reporting on 2025 data. IOPC Director General, interview with PA News, 26 May 2026. IOPC, *IOPC figures show more police referrals than ever before*, May 2026. Commissioner for the Retention and Use of Biometric Material, valedictory report 2024 to 2025, published 19 May 2026. NCSC, *Mistaking AI vulnerability could lead to large-scale breaches*, 10 December 2025.

The UK legal position

There is no AI statute for policing. There are four instruments that could have governed it, and each one is silent in a different way.

A force deploying AI today is governed by the Data Protection Act 2018, the Equality Act 2010, the Human Rights Act 1998, the Police and Criminal Evidence Act 1984 and its codes, common law powers, and guidance issued by the College of Policing. There is no bespoke rulebook, and saying so plainly is more useful than pretending otherwise.

What is less well understood is that the instruments most likely to have filled the gap have not. Four bear directly on a chief officer's position.

Forensic Science Regulator's Code of Practice 2025	Statutory, made under the Forensic Science Regulator Act 2021, in force 2 October 2025, covering thirty-six forensic science activities including data capture from digital devices, cell site analysis, CCTV recovery and specialist video and multimedia analysis. On a full-text search it contains no occurrence of artificial intelligence, machine learning, algorithm, automated or probabilistic. Facial image comparison does not appear anywhere in it, and is not a regulated forensic science activity.
Code of Practice for the PNC and LEDS	Issued by the College of Policing with the Secretary of State's approval under section 39A of the Police Act 1996, February 2023, governing the two national police databases. It sets no express requirement to record a reason at the point of access; it defers to data protection law and local auditing. It contains no mention of automated processing, algorithms or artificial intelligence.
Authorised Professional Practice	The Data Ethics and Data-Driven Technologies APP launched in June 2025, last updated July 2026, and says that AI "should not be treated as a default solution" and is inappropriate in "high-risk, high-impact situations". It is guidance officers must have regard to, not a rule they must follow.
Covenant for Using AI in Policing	Endorsed by the National Police Chiefs' Council in September 2023. Developers and users of AI in policing must give it "due regard". It names no compliance or assurance mechanism, and no body is given the job of checking adherence.

The courts have been asked the question once, and answered it narrowly. In *Thompson and Carlo v Commissioner of Police of the Metropolis*, decided by a Divisional Court on 21 April 2026, challenges to the Metropolitan Police's live facial recognition policy under Articles 8, 10 and 11 were dismissed. The court held that "the breadth of a power is not determinative" and that the central question is whether discretion is constrained by sufficiently clear rules and safeguards, finding the policy's chain of command "a far cry from the 'hunch' or 'professional intuition' of an individual officer". No challenge was brought under section 149 of the Equality Act.

What that judgment upholds is a force's policy, not a statutory framework. It is a ruling that one operator's internal rules were good enough, inside a legal framework the Government itself calls a patchwork.

Sources – Forensic Science Regulator, *Code of Practice 2025 (Version 2)*, in force 2 October 2025. College of Policing, *Code of Practice for the Police National Computer and the Law Enforcement Data Service*, 23 February 2023. College of Policing, Data Ethics APP and Data-Driven Technologies APP, published 17 June 2025, updated 8 July 2026. NPCC, *Covenant for Using Artificial Intelligence in Policing*, 28 September 2023. *Thompson and Carlo v Commissioner of Police of the Metropolis* [2026] EWHC 915 (Admin).

The change almost nobody has written about

Policing does not sit under the automated decision-making rules everyone has been briefed on. It has its own, and they moved twice in a year.

Most AI briefings for UK organisations are built on section 80 of the Data (Use and Access) Act 2025 and Article 22 of the UK GDPR. Law enforcement processing sits outside that regime entirely, in Part 3 of the Data Protection Act 2018. Two changes were made inside Part 3 that a policing audience has largely not been told about.

The decision rules were replaced

Sections 49 and 50 of the Data Protection Act 2018 were substituted by new sections 50A to 50D by the Data (Use and Access) Act 2025, commencing on 19 June 2025 and 5 February 2026. A decision is now solely automated where there is “no meaningful human involvement in the taking of the decision”. A significant decision based wholly or partly on sensitive processing may not be taken solely automatically unless explicit consent or specific legal authorisation applies. Safeguards require that the person is given information about the decision and is able to contest it. The Secretary of State may make regulations defining what meaningful human involvement means.

The Information Commissioner’s own summary of the effect, written for law enforcement agencies, is that the Act “allows you to use people’s personal information to make significant automated decisions about them in more circumstances, so long as you continue to apply appropriate safeguards”.

The logging duty was trimmed

Section 62 of the Data Protection Act 2018 requires logs to be kept of consultation and disclosure of personal data in law enforcement processing. As originally enacted, those logs had to make it possible to establish the justification for, and the date and time of, each consultation and each disclosure.

DATA (USE AND ACCESS) ACT 2025, SECTION 82 – IN FORCE 19 AUGUST 2025

“In section 62 of the 2018 Act (logging of law enforcement processing) – (a) in subsection (2)(a), omit ‘justification for, and’, and (b) in subsection (3)(a), omit ‘justification for, and’.”

The statutory duty to log *why* personal data was consulted or disclosed has gone. Who, and when, remain. The change was made to reduce burden, and forces may still capture a reason as a matter of local policy. But the Code of Practice governing the two national police databases sets no requirement of its own on the point – it defers to data protection law – and data protection law is where the requirement used to be.

The timing is what makes this a board matter rather than a compliance footnote. The statutory floor for explaining why data was looked at was lowered in August 2025. The national AI centre designed to link and surface that data across forty-three forces launched in June 2026. Any force that wants to be able to answer, in two years’ time, why a particular record was consulted before a particular decision will have to require that itself.

Sources – Data Protection Act 2018, Part 3, sections 50A to 50D and section 62, as amended, read on legislation.gov.uk. Data (Use and Access) Act 2025, sections 80 and 82. ICO, *The Data Use and Access Act 2025 – what does it mean for law enforcement agencies?*, updated 19 June 2026.

Beyond the UK — and inside it

Europe has drawn a line policing has to understand. So, increasingly, has Scotland.

The European position

The EU AI Act's prohibitions took effect on 2 February 2025. Two of them matter here. Real-time remote biometric identification in publicly accessible spaces for law enforcement purposes is prohibited, subject to narrow exceptions. So is the untargeted scraping of internet or CCTV material to create or expand facial recognition databases. Other law enforcement uses of AI that may interfere with fundamental rights, and remote biometric identification generally, are classified as high risk under Annex III, with obligations applying from 2 December 2027. The Digital Omnibus did not move that date for biometrics; systems integrated into regulated products move to 2 August 2028.

The common error is to say the EU has banned police facial recognition. It has not. It has prohibited one specific mode of it and placed the rest in a high-risk regime whose obligations begin in December 2027. The more interesting comparison for a UK chief officer is the second prohibition, on building facial recognition databases from material gathered for another purpose. That is a question the UK has not answered in legislation at all.

Three regimes in one country

England and Wales have a consultation awaiting outcome. Scotland has a statutory Scottish Biometrics Commissioner and a statutory code of practice; the Commissioner wrote to the Cabinet Secretary for Justice in May 2026 urging primary legislation before any police use of live facial recognition, and in September 2026 published the view that the Scottish Government's public space surveillance strategy is out of date. Northern Ireland has no biometrics commissioner, and the Chief Constable's accountability report to the Policing Board in June 2026 contains no AI or facial recognition content at all.

Any national capability built for "UK policing" is being built across three different oversight regimes, one of which is arguing for a law before deployment rather than after it. A force operating across a border, or a supplier selling across all three, needs to know which one it is standing in.

A STANDARD THAT EXISTS, AND THAT NOBODY IS REQUIRING

ISO/IEC 42001, the international management system standard for artificial intelligence, is published and certifiable, and BSI operates an evaluation scheme for the trustworthiness of AI facial recognition. Facial recognition suppliers have certified to both. No UK policing body requires either of them as a condition of purchase. A voluntary standard being adopted by sellers rather than demanded by buyers is a gap a single procurement clause can close.

Sources — European Commission, AI Act regulatory framework page, last updated 3 August 2026. Scottish Biometrics Commissioner, correspondence of 27 May 2026 and publication of 1 September 2026. PSNI, *Chief Constable's Accountability Report to the Northern Ireland Policing Board*, 4 June 2026. ISO/IEC 42001; BSI AI facial recognition trustworthiness evaluation.

What can be done today

The strongest governance in UK policing is currently being written by individual forces, not nationally. It can be copied.

Two forces have published, of their own accord, the thing the national system has not produced. Surrey and Sussex Police publish a joint artificial intelligence policy stating that human oversight is mandatory for all AI-supported decision-making, that no decision which could affect a living person may be fully automated, and that all AI-influenced decisions must be explainable, auditable and attributable to a human decision-maker. It requires the force's information management function to maintain an internal AI register recording what systems are used, what decisions result from them, how bias was assessed and what algorithms are involved. Sussex Police separately publishes an inventory of its AI by category and status, distinguishing what is operational from what is a pilot and what is exploratory, and states that AI is used only for decision support and that operational decisions remain human-led.

That is a governance position a chief officer can adopt this month without waiting for legislation, a national register, or a revised code. Seven things follow from it, in rough order of how quickly they pay.

- **Publish an inventory.** Every tool with an AI component, its purpose, its status and its named senior owner. The national register does not exist; the two forces that built their own did not wait for it.
- **Write the two lines that matter.** No decision affecting a living person is fully automated, and every AI-influenced decision is attributable to a named human. Both are already in force in a published UK police policy.
- **Reinstate the reason.** Require a recorded policing purpose at the point of access to national systems as a matter of force policy, whatever the statutory floor now says.
- **Take audio-visual redaction seriously.** It is the clearest productivity case in the sector on the Government's own estimate, it touches no decision about a person, and it releases time in exactly the place the inspectorate says time is lost.
- **Triage digital evidence, do not judge it.** Twenty thousand devices are waiting. Assistive triage that surfaces and orders material for a human is defensible; anything that scores or concludes is not, yet.
- **Separate the two facial recognition capabilities.** The regulator found compliance worse in the quiet one. Retrospective searching against custody images needs a retention answer, an image-source answer and a senior owner before anything is scaled.
- **Put verification in the report-writing path.** The West Midlands failure was not a model failure. It was a document that reached a decision without anyone checking a checkable fact.

Sources — Surrey and Sussex Police, artificial intelligence policy 1236/2026, published under freedom of information. Sussex Police, published response on artificial intelligence, updated January 2026. NAO, *Police Productivity*, HC 1380, paragraph 3.8. HMICFRS, *State of Policing 2025-26*.

Tomorrow

The useful way to sort AI in policing is not by how clever the system is. It is by where accountability sits when it is wrong.

Three levels need distinguishing, because a board can govern them differently and a supplier will rarely draw the line for you.

LEVEL ONE

Assistive

Prepares, summarises, surfaces. A person decides. Accountability is unchanged. Almost all defensible value in policing sits here today — redaction, transcription, triage, search.

LEVEL TWO

Augmentive

Recommends within bounds, with reasoning and a confidence measure. A person confirms or overrides, and the override is recorded. The review has to be demonstrably meaningful, not a box.

LEVEL THREE

Adaptive

Decides within a defined envelope. Oversight moves to the envelope rather than the decision. Accountability moves to whoever sets and monitors it. This is a reasoned projection, not an observation.

The West Midlands failure is the reason this matters more in policing than in most sectors. The tool involved had no decision authority of any kind. It was a general assistant, used to answer a question, and the answer travelled into a written risk report, through a Safety Advisory Group, into a decision that was argued about in Parliament. An assistive tool is not a low-risk tool. It is a tool whose risk is carried entirely by the verification step around it — and in that case there was none.

0 to 12 months

Inventory, named ownership, the two governance lines, and verification built into any path where machine-generated text can reach a document that leaves the force. Audio-visual redaction and transcription scaled. Retrospective facial recognition retention and image sources resolved before anything else is added. This is the window in which the national centre's first pilots run in up to ten forces.

12 to 36 months

National tools arrive with national assurance attached. The work is deciding what your force will additionally require before they touch a decision, and building the record that shows a human review was real. Expect a statutory framework for biometrics, an ICO code of practice on automated decision-making, and the EU high-risk obligations landing in December 2027 for anyone operating across that border.

36 months and beyond

Augmentive use in triage, prioritisation and case-file quality becomes normal, and the governance question becomes whether the human review is demonstrably meaningful rather than whether a human was present. Adaptive use inside a defined envelope becomes technically possible before it becomes legally or publicly acceptable.

THE HONEST CAVEAT

The third horizon is a reasoned projection and should be read as one. Two things could change it entirely: the shape of the biometrics legislation the Government has committed to but not yet introduced, and whether the first serious AI-related failure in a live investigation happens before or after that legislation arrives.

Sources — GOV.UK, *PoliceAI to speed up investigations and fight crime*, 10 June 2026. European Commission, AI Act timetable. Home Affairs Committee, HC 1553. Home Office inspection letter, 14 January 2026.

Benefit realisation

Every hours-saved figure offered to a force this year rests on a measurement system the National Audit Office says does not exist.

This is the section a chief officer should read before signing anything. The claims in circulation are large and specific: six million hours of police time a year, the equivalent of three thousand officers freed from desk duties, a million hours a year from redaction alone if every force adopts it. They are government ambitions, and they may prove right. What can be said with confidence is that the body making them has told its auditor it cannot currently measure whether they land.

The NAO found in November 2025 that the Home Office “does not yet have a shared definition of – or methodology for measuring – productivity” in policing, and that it “does not know whether the anticipated £2.9 billion of benefits by 2027-28 will be realised” from the programme already running. The inspectorate, separately, cites a figure of up to fifteen million police hours releasable through science and technology innovation, and does not publish the derivation.

None of that makes the tools worthless. It makes the baseline the force’s own responsibility.

A worked example

Audio-visual redaction is the strongest case available and shows how to do it. The Home Office estimate is around 11,000 days a month nationally, roughly £1.7m a month, if the technology is adopted across England and Wales. To turn that into something a force can hold a supplier to, three numbers have to exist before procurement, not after: how many hours the force currently spends redacting, measured rather than estimated; what proportion of that volume the tool can actually take, by file type and case type rather than in aggregate; and what happens to the released time – whether it returns to investigation, absorbs existing overtime, or disappears.

Measure before, not after	A baseline taken after deployment is not a baseline. Three months of current-state measurement is the cheapest insurance available on an AI business case.
Count the verification cost	Every assistive tool creates checking work. If the check is real it takes time, and that time belongs in the benefit calculation. If it is not real, the West Midlands case is what that looks like.
Measure quality, not only volume	The inspectorate’s findings are about investigation quality, not throughput. A tool that increases volume while quality stays where it is has not helped the thing the reader is graded on.
Publish the result	Including where it did not work. The sector has no shared evidence base on what AI actually delivers in policing, and the first forces to publish honest numbers will set the standard everyone else is measured against.

Sources – NAO, *Police Productivity*, HC 1380, 3 November 2025, paragraphs 2.12, 3.1 and 3.8. HMICFRS, *State of Policing 2025-26*. GOV.UK, *PoliceAI to speed up investigations and fight crime*, 10 June 2026.

A way in

Eight workstreams. The first three are a natural first step of six to eight weeks.

None of what follows requires a decision about a product. It is the work that has to be done before a product decision can be made safely, and most of it is work a force can do with people it already has, given a structure and someone to hold the pen.

01	Readiness assessment	What the force already runs with an AI component, who owns each item, what data it touches, and where the verification steps are. Most forces discover more than they expected.	4–6 weeks
02	Use case identification and triage	Candidate uses sorted against the accountability ladder and against the inspectorate's findings, so effort goes where the force is actually graded weakest.	3–4 weeks
03	Regulatory and legal position paper	Part 3 of the Data Protection Act as amended, the logging position, the biometrics consultation, the APP and Covenant status, and what the force will require beyond the statutory floor.	3–4 weeks
04	Board and executive governance	Named ownership, the two governance lines, the register, and what reaches the chief officer team and the police and crime commissioner, in what form and how often.	4 weeks
05	Threat and integrity response	Synthetic material in evidence, AI-assisted complaints and reviews, prompt injection exposure in any connected system, and what the force does when a document containing a machine-generated error is discovered.	4 weeks
06	Benefit realisation framework	Baselines measured before deployment, verification cost counted, quality measured alongside volume. Runs in parallel with the rest.	3 weeks
07	Build, buy or partner evaluation	What to take from the national centre, what to buy, what to require contractually — including certification against the standards that already exist and nobody is asking for.	4–6 weeks
08	Twelve-month mobilisation roadmap	Sequenced, costed, with the decision points named and the things that will not be done named as well.	2 weeks

The first three form a natural first step of six to eight weeks: know what you have, know what is worth doing, and know what you are required and what you are choosing to require. This sector has no single commencement date to work back from. The real deadline is the national centre's own timetable — pilots in up to ten forces through 2026–27 and national scaling from 2027. Every force will therefore settle what it allows, who signs it off and what it records during this financial year, whether or not anyone convenes a meeting to settle it. Six to eight weeks fits comfortably inside that.

CONTACT

Neil Catton — independent technology strategist, working across a fractional and advisory portfolio.
nc@neilcatton.com · neilcatton.com · writing.neilcatton.com

Sources

Everything in this briefing, in one place, so that any figure can be checked at its origin.

Government and Parliament

- Home Office, *From Local to National: A New Model for Policing*, CP 1489, January 2026.
- Home Office, *Consultation on a new legal framework for law enforcement use of biometrics, facial recognition and similar technologies*, 4 December 2025; closed 12 February 2026; status "awaiting outcome" as at 14 September 2026.
- Home Office, *Police use of artificial intelligence (AI): factsheet*, published 9 June 2026, updated 23 July 2026.
- Home Office, *Crime outcomes in England and Wales 2025 to 2026*, 23 July 2026.
- Home Office, *Police powers and procedures: stop and search, arrests and mental health detentions, England and Wales, year ending 31 March 2025*, 6 November 2025.
- Home Office, *Inspection of police forces' contributions to safety advisory groups: West Midlands Police*, 14 January 2026.
- GOV.UK, *PoliceAI to speed up investigations and fight crime*, and the Policing Minister's speech on the launch of PoliceAI, both 10 June 2026.
- Written Ministerial Statement HCWS1285, final police funding settlement 2026-27, 28 January 2026.
- Home Affairs Committee, *Maccabi Tel Aviv fan ban*, Fifth Report of Session 2024–26, HC 1553, 22 February 2026.
- Prime Minister's Office, *The King's Speech 2026: background briefing notes*, 13 May 2026.
- House of Commons Library, *Policing in the UK: current structures and proposals for reform*, updated 18 August 2026.

Inspectorates, regulators and oversight bodies

- National Audit Office, *Police Productivity*, HC 1380, Session 2024–2026, 3 November 2025.
- HMICFRS, *State of Policing: The Annual Assessment of Policing in England and Wales 2025–26*, 8 September 2026.
- HMICFRS, inspection of the police role in safety advisory groups for public events, September 2026.
- Information Commissioner's Office, *Facial Recognition in Law Enforcement Outcomes Report* and five force audit reports, August 2026; *AI and biometrics strategy update*, March 2026; *The Data Use and Access Act 2025 – what does it mean for law enforcement agencies?*, updated 19 June 2026.
- Independent Office for Police Conduct, independent investigation announcement, 19 January 2026; *Deaths during or following police contact, England and Wales 2025/26*; annual referral figures, May 2026.
- Biometrics and Surveillance Camera Commissioner, response to the Home Office consultation, 12 February 2026; Commissioner for the Retention and Use of Biometric Material, valedictory report 2024 to 2025, published 19 May 2026.
- Scottish Biometrics Commissioner, correspondence and publications, May to September 2026.
- National Cyber Security Centre, *Mistaking AI vulnerability could lead to large-scale breaches*, 10 December 2025.
- Forensic Science Regulator, *Code of Practice 2025 (Version 2)*, in force 2 October 2025.

Sources

Legislation and case law

- Data Protection Act 2018, Part 3, sections 50A to 50D and section 62, as amended. Data (Use and Access) Act 2025, sections 80 and 82. Forensic Science Regulator Act 2021. Police Act 1996, section 39A.
- *Thompson and Carlo v Commissioner of Police of the Metropolis* [2026] EWHC 915 (Admin), 21 April 2026.
- *Ayinde v London Borough of Haringey; Al-Haroun v Qatar National Bank QPSC* [2025] EWHC 1383 (Admin), 6 June 2025.
- *R v FGD* [2026] EWCA Crim 918, 24 July 2026.
- *R (RMC) v Commissioner of Police of the Metropolis*, 22 June 2012.

Policing's own publications, and other sources

- NPCC and APCC, *National Policing Digital Strategy 2025-2030*. NPCC, *Covenant for Using Artificial Intelligence in Policing*, 28 September 2023, and the £115m AI centre release of 27 January 2026.
- College of Policing, *Data Ethics APP*, *Data-Driven Technologies APP* and *AI guidance*, June 2025, updated July 2026; *Code of Practice for the Police National Computer and the Law Enforcement Data Service*, 23 February 2023.
- Metropolitan Police Service, *Live Facial Recognition Annual Report*, September 2025, and news release of 13 May 2026.
- Surrey and Sussex Police, *artificial intelligence policy 1236/2026*; *Sussex Police*, published response on artificial intelligence, January 2026; *West Midlands Police* and *Greater Manchester Police*, published AI statements and policies.
- PSNI, *Chief Constable's Accountability Report to the Northern Ireland Policing Board*, 4 June 2026.
- Internet Watch Foundation, *research on AI-generated child sexual abuse imagery*, 2026, reporting 2025 data.
- European Commission, *AI Act regulatory framework*, last updated 3 August 2026. *ISO/IEC 42001* and the *BSI AI facial recognition trustworthiness evaluation*.

About the author

Neil Catton is an independent technology strategist working across a fractional and advisory portfolio — fractional CTO and CIO roles, AI board briefings, AI readiness reviews, technology due diligence, data strategy, and programme recovery. He is the author of *The Next Evolution*, *The Cognitive Crucible* and *The Shadow System*, and writes at writing.neilcatton.com on technology, ethics and human purpose.

He has spent more than thirty-nine years in technology across more than twenty sectors, including public sector, central and local government, justice and policing. Current work in public safety includes advisory to a group established by senior former police officers, covering an AI and data mesh programme for UK custody data and the ethical use of AI in policing. That engagement is one strand of the portfolio rather than the primary role, and no organisation named in this briefing has been engaged, approached or consulted in preparing it.

How this briefing was produced

Research began with the regulators, inspectorates and oversight bodies, then legislation read directly rather than in summary, then the published statements of police forces about their own operations. A figure appears here only where it can be traced to a named regulator, inspectorate, ombudsman, select committee, court judgment, published legislation, or a force speaking on its own record about its own operations. Where a claim rests on the absence of something — a statutory code that does not mention a technology, a committee that made no recommendation — the full document was searched before the absence was stated. Figures that could not meet that standard are listed in section one rather than quietly dropped.

In keeping with this report’s own argument: this briefing was produced with AI assistance, used transparently and kept under direct human editorial control throughout. Every source was verified; every judgement was reviewed by Neil Catton before publication.

NOTICE

- 1. This briefing is not legal, regulatory, financial or professional advice, and should not be relied on as such.
- 2. The position is stated as at 14 September 2026. Several matters described here were unresolved at that date — in particular the outcome of the Home Office biometrics consultation, the content and introduction of the Police Reform Bill, and the IOPC investigation referred to in section four — and may since have moved.
- 3. Third-party sources are cited in good faith. Readers should verify any figure at its origin before relying on it.
- 4. Named organisations appear only where a regulator, inspectorate, ombudsman, select committee or court has placed them on the record, or where they have published the material themselves. They are used illustratively. None has been engaged or approached.
- 5. No advisory or client relationship is created by receipt of this document.
- 6. **Independence.** The author holds no vendor affiliations, reseller agreements, referral arrangements, commission interests or equity positions in anything referenced in this briefing, and has received no payment from any organisation named in it.
- 7. © Neil Catton 2026. Circulated for the recipient’s internal use.

Version history

VERSION	CHANGE	DATE
v1.0	First publication.	14 Sep 2026
v1.1	Language pass. Sections one, six and ten reworded, plus one card label and the methodology paragraph. No figure, source or finding changed.	14 Sep 2026
v1.2	Four wording changes in body copy, including one self-referential sentence in section one. No figure, source or finding changed.	15 Sep 2026