HMICFRS

His Majesty's Inspectorate of Constabulary and Fire & Rescue Services

How police forces and the National Crime Agency use retrospective facial recognition

Contents

Foreword 1

Summary 3

Recommendations 8

Introduction 13

The use of facial recognition technology in policing 16

- The police use different types of facial recognition technology 16
- The public generally support the police's use of RFR technology but have some concerns 17
- The existing legal framework for the use of RFR is complex 18
- The Police National Database has an RFR function 20
- There are benefits and risks to using RFR technology 21

To what extent are local, regional and national guidance, policies and governance arrangements for retrospective facial recognition fit for purpose? 23

- Guidance on the police use of RFR technology is limited 23
- National and regional governance of RFR could improve 24
- Force governance arrangements for RFR vary 25
- PND data indicates that RFR is being underused in some forces 27
- Forces need to do more to fully understand the benefits and effects of using RFR 29
- Forces need to better understand the impact of RFR on crime outcomes 30
- Some forces are improving how they collect RFR management information 31
- Forces need to improve their auditing of RFR searches 32
- The police service isn't yet meeting its obligation to delete custody images 34
- Some forces are using their own facial recognition systems 36

A new national facial recognition system will use a more accurate algorithm for PND facial recognition searches 36
Forces are missing opportunities to identify suspects 37
Forces don't always consult the public about using RFR 38
A national regulatory framework is needed to help govern the use of RFR 39
Any new code of practice on the use of RFR needs independent oversight 40

How well do police forces and the National Crime Agency train their investigators to use retrospective facial recognition in investigations? 42

Officers and staff who use RFR need better training and development 43
Some forces have developed their own training for RFR operators 43
A Home Office survey of PND facial search users produced mixed results 44
RFR training for investigators is insufficient 45
A national RFR training framework for investigators is needed 46

How well do investigators understand and follow the required investigative processes after identifying a potential facial recognition match? 48

Forces are using RFR effectively to solve crimes 48
Investigators don't always carry out additional checks before making arrests 49
Forces have different approaches to using RFR and don't always have centralised RFR teams and clear operating procedures 49
Forces should include use of RFR in their investigation policies and procedures 52
Force investigation logs don't include enough information about the use of RFR 52

Foreword

Facial recognition technology is changing the way police forces identify suspects and carry out investigations. Officers no longer need to compare images manually and can instead use retrospective facial recognition (RFR) to get results in seconds. Investigators can compare images from crime scenes with custody images held on national systems. CCTV, mobile phone footage and other digital imagery are now widely available, so use of RFR is likely to increase further.

In our inspection, we examined how police forces and the National Crime Agency use RFR. We found that the technology was providing important benefits to policing. Forces routinely use RFR to generate investigative leads, identify suspects and support criminal investigations. In many cases, it helps investigators to identify people more quickly. It also reduces the need to share images with the public. We found that when it was used appropriately, RFR could be a valuable and proportionate investigative tool.

During our inspection, we found that governance, oversight and use of RFR wasn't sufficiently consistent across policing. Legislation hasn't kept up with developments in facial recognition technology, which is contributing to uncertainty and a fragmented approach. While national bodies have provided some guidance and oversight, arrangements remain underdeveloped. There is no comprehensive statutory framework governing the police use of facial recognition technology.

The maturity of governance arrangements varies considerably between forces. Some have established policies, oversight structures and safeguards, which include equality and data protection impact assessments. Others rely heavily on limited national guidance and haven't developed local arrangements that provide sufficient assurance. We also found inconsistencies in auditing, performance monitoring and working with the public. As a result, forces often can't clearly show the effectiveness of their use of RFR or provide enough evidence of the outcomes RFR achieves.

In this report, we highlight some concerns about training and operational practice. We found that investigators didn't always receive the training and support they needed to understand the capabilities and limitations of RFR. Experienced investigators generally understood the need to treat RFR results as investigative leads that require corroboration. This understanding wasn't universal. In some cases, officers relied too much on potential matches or failed to carry out suitable follow-up enquiries.

Public trust and confidence are essential to the continued use of facial recognition technology. We found evidence of public support for the use of RFR, but this support depends on policing showing that it uses this technology lawfully, proportionately and openly. Forces must be able to show that appropriate safeguards are in place, risks relating to bias and data retention are effectively managed and that decisions informed by facial recognition are subject to human judgment and scrutiny.

In this report, we make 16 recommendations. They are designed to improve how police forces and the National Crime Agency use facial recognition technology and maintain public confidence in its use by:

- improving national and local governance arrangements;
- introducing clear national standards;
- making sure RFR is used more consistently;
- introducing clear oversight and supervision of the use of RFR; and
- improving guidance and training, especially for investigators.



Kathryn Stone OBE

His Majesty's Inspector of Constabulary

Summary

For many years, police forces in England and Wales have used images from crime scenes to help identify suspects. The introduction of facial recognition technology has transformed suspect identification. Investigators can now compare images with custody images held on national systems in seconds, rather than having to wait days or weeks. The growing availability of image sources, such as CCTV and video doorbells, means that the use of retrospective facial recognition (RFR) searches will increase.

The police use three types of facial recognition technology:

1. retrospective facial recognition (RFR)
2. live facial recognition
3. operator-initiated facial recognition.

This inspection only examined how the police and the National Crime Agency use RFR.

Since 2013, forces have routinely used the Police National Database (PND) to carry out RFR searches. Only trained licence holders can carry out RFR searches on the PND. Investigators submit images to a licence holder, who carries out the search for them.

An RFR search on the PND produces a ranked list of the most similar images. These potential matches are only to be used as an investigative lead and not as identification evidence. Investigators and PND operators must still carry out additional checks and research.

The way that forces use RFR to identify unknown suspects is likely to be more proportionate than media appeals for information. RFR helps reduce the widespread, routine sharing of images by the police with the public.

We analysed the available data and found that the public generally supported the police service's use of RFR. But continued support will depend on maintaining public confidence, openness about its use and effective safeguards.

In 2024, the National Physical Laboratory carried out an independent test of the algorithm (set of instructions) the PND uses for RFR. It found that, despite the algorithm's overall level of accuracy, at some settings people with certain protected characteristics were more likely to be incorrectly included in the search results.

To what extent are local, regional and national guidance, policies and governance arrangements for RFR fit for purpose?

The legislative and governance framework for RFR remains fragmented and underdeveloped. In some respects, legislation hasn't kept pace with the technology. The lack of specific legislation governing the police use of facial recognition and related biometric technologies appears to have created some uncertainty about the lawful basis for their use and the safeguards needed to protect the public.

During our inspection, we found that police forces in England and Wales used RFR in a fragmented way and with limited oversight. Forces couldn't clearly show performance improvements from using RFR.

Although national bodies provide some oversight and guidance, governance arrangements for RFR aren't sufficiently co-ordinated. Policing has taken steps to address concerns about algorithm bias and emphasise the need for human review and corroboration of potential matches. But further work is needed to strengthen safeguards, governance and accountability.

We found that the maturity of governance arrangements varied considerably between forces. The strongest arrangements included clear policies, dedicated oversight structures, equality impact assessments and data protection impact assessments. Some forces relied heavily on limited national guidance and hadn't developed comprehensive local policies. We also found inconsistent awareness among officers and staff of existing policies and their responsibilities when using RFR.

Forces often didn't have enough management information to understand how effectively they used RFR or to evaluate its contribution to crime investigations. National data is limited and forces' use of RFR varies considerably. This variation suggests that some forces may not be making full use of the technology's investigative potential. At the same time, limited performance data means that forces often can't clearly show the benefits, risks and outcomes of using it.

We found that many forces weren't fully complying with national audit requirements. Forces' audit processes primarily focused on how searches were carried out rather than on how investigators requested, interpreted and acted on RFR results.

The retention of custody images remains an area of concern. We found that some images which should have been deleted under existing retention rules remained available for facial recognition searches. This risks undermining public confidence and highlights the importance of ongoing national work to improve compliance, strengthen image management processes and align the treatment of custody images more closely with other biometric data.

Most forces rely on the PND for their RFR searches. Other forces have introduced local systems that search only force-level image databases. Although these systems can provide operational benefits, differing technologies and governance arrangements may create challenges for consistency, oversight and effectiveness, particularly if offending crosses force boundaries.

Future developments may offer forces opportunities to address some of these issues. Planned national facial recognition capabilities promise improved accuracy, stronger safeguards, more consistent image-retention practices and reduced risks of algorithm bias. These developments have the potential to support a more effective and consistent national approach to facial recognition.

We found that forces had different approaches to working with the public and openness about their use of RFR. Some forces had established arrangements to consult communities and publish information about their governance and use of the technology. Others had carried out little work with the public. Forces will increasingly use facial recognition technology, so they will need to be open with the public about how they use it and involve communities in discussions about its use. This will help maintain public trust and confidence.

Overall, we found that while RFR provided valuable investigative opportunities, the existing governance framework didn't provide sufficient consistency, oversight or assurance. A clearer statutory framework, stronger national standards, improved governance arrangements and more effective independent oversight are needed to support the lawful, ethical and effective use of facial recognition technology across policing.

How well do police forces and the National Crime Agency train their investigators to use RFR in investigations?

The absence of authorised professional practice guidance or a code of practice for RFR has contributed to differences in how forces and the National Crime Agency use the technology. Similarly, the lack of a national learning framework has led to inconsistent approaches to training and continuing professional development across forces. This risks creating greater differences across forces in capability and practice.

Less experienced investigators most often request RFR searches, usually in relation to volume crime offences. While some guidance and training on RFR exists, it is primarily aimed at PND operators rather than investigators.

During our inspection, we found that forces didn't always provide appropriate training to personnel who use RFR. This includes investigators. We were surprised by this finding, given the importance of the decisions made using RFR results. If personnel don't understand the technology's limitations, they may place too much weight on a potential match, fail to carry out appropriate enquiries to check the results or use the results inappropriately when making operational decisions. This increases the risk of identifying the wrong suspect, inappropriate executive action and a loss of public confidence in the police use of facial recognition technology.

We found evidence that suggested many personnel, including some licensed PND users, didn't fully understand important aspects of RFR. In a survey of PND users, some respondents were uncertain about the evidential value of RFR matches, the importance of accuracy assessments and the limitations of the technology.

We saw effective practice in some forces, particularly where specialist teams provided training, guidance and ongoing support to investigators. These approaches helped improve awareness of image-quality requirements, the interpretation of results and the need for corroborative enquiries before acting on potential matches.

The quality of images submitted for RFR searches is critical to achieving reliable outcomes. This means that investigators need a good understanding of image standards, image preparation techniques and the limitations of facial recognition technology. Effective supervision is also important, particularly as less experienced investigators often carry out the volume crime investigations that most frequently require the use of RFR.

Overall, we found that a more consistent national approach to training and professional development was needed. Investigators, supervisors and operators all require a clear understanding of image-quality requirements, the interpretation of search results and the distinction between intelligence and evidence. More consistent training would help promote effective, proportionate and lawful use of RFR across policing.

How well do investigators understand and follow the required investigative processes after identifying a potential facial recognition match?

RFR is making a valuable contribution to police investigations. It is being used successfully to identify suspects and solve crimes, including serious offences. We found several examples where RFR helped investigators to generate leads quickly and supported effective investigative outcomes when combined with other lines of enquiry.

But we found that forces didn't use RFR consistently. While experienced investigators generally understood its limitations and the need to corroborate potential matches, less experienced investigators often had a weaker understanding. Some investigators didn't know that RFR results were intelligence rather than evidence and required further enquiries before officers took enforcement action. This creates a risk that people could be incorrectly identified or arrested, which could undermine public confidence in the technology.

We found that some investigators didn't always carry out enough corroborative enquiries before acting on potential matches. In a small number of cases, officers relied too heavily on RFR results, which led to inappropriate investigative action. Although some forces had strengthened their processes after such incidents, practice remained inconsistent.

The most effective arrangements were in forces that used centralised RFR teams. These teams generally provided better governance, stronger expertise, more consistent processes and clearer advice to investigators. They were more likely to validate requests, improve image quality, explain the limitations of results and support investigators in carrying out appropriate follow-up enquiries. Forces without centralised arrangements were more likely to have weaker processes and lower levels of understanding among investigators.

We also found considerable variation in the availability of local policies and operating procedures governing the use of RFR. Some forces had clear guidance setting out how searches should be carried out, how results should be recorded and what corroborative enquiries were required. Others lacked formal procedures, which increased the risk of inconsistent decision-making and misunderstanding of the technology's limitations.

We found that investigators and supervisors didn't routinely document the consideration or use of RFR in investigation plans, enquiry logs or supervisory reviews. As a result, forces often lacked clear audit trails showing how RFR results informed decision-making and whether appropriate corroboration had taken place. This limits forces' ability to assess their use of RFR, identify missed opportunities and provide effective scrutiny and governance.

Recommendations

In this report, we make 16 recommendations.

Recommendation 1

By 30 June 2027, chief constables and the director general of the National Crime Agency must make sure police forces and the National Crime Agency carry out and record a data protection impact assessment to address their use of retrospective facial recognition technology.

Recommendation 2

By 31 December 2027, the National Police Chiefs' Council should establish national requirements for collecting, analysing and reporting retrospective facial recognition management information.

The requirements should define the minimum management information that forces must collect, analyse and review to support effective oversight, audit, assurance and evaluation of outcomes. This should draw on existing good practice identified in policing.

Recommendation 3

By 31 December 2027, chief constables and the director general of the National Crime Agency should make sure police forces and the National Crime Agency routinely collect, analyse and review retrospective facial recognition information to:

- assess the effectiveness and outcomes of using retrospective facial recognition;
- identify risks and any actual or potential adverse impacts;
- support local and national governance and accountability arrangements;
- allow independent scrutiny and oversight; and
- support continuous improvement in the use of the technology.

Recommendation 4

By 30 June 2027, the National Police Chiefs' Council should review national retrospective facial recognition audit requirements to make sure audits assess both how retrospective facial recognition searches are carried out and the subsequent investigative use of search results. Audit information should include the investigator who instigated the search.

Recommendation 5

By 31 December 2027, the Home Office should provide policing with a national facial recognition system that supports the consistent, lawful and effective use of retrospective facial recognition across England and Wales.

Where forces use alternative facial recognition systems, the Home Office should make sure they are subject to equivalent standards of governance, performance testing, assurance, audit and oversight.

Recommendation 6

By 30 June 2027, the National Police Chiefs' Council should develop national guidance for police forces and the National Crime Agency on communication and consultation with the public and openness about police use of facial recognition technology.

Recommendation 7

By 30 June 2027, chief constables should make sure their forces have arrangements in place to work with local communities and maintain openness about their use of facial recognition technology.

These arrangements should include the publication of relevant policies and governance documents, opportunities for consulting and working with the public and processes for considering and responding to community concerns.

Recommendation 8

By 30 June 2027, as part of its implementation of police reform legislation, the Home Office should consider including provisions that permit police forces to:

- use algorithms to search databases for a legitimate policing or safeguarding purpose; and
- share results from these searches as required for advancing the relevant policing or safeguarding purpose.

Recommendation 9

By 30 June 2027, the Home Office should introduce a requirement for a statutory code of practice governing law enforcement use of retrospective facial recognition.

The code should include minimum requirements in relation to:

- the lawful purposes for which retrospective facial recognition may be used;
- governance, accountability and audit arrangements;
- training and competence requirements;
- the testing and assurance of facial recognition algorithms; and
- the management and use of retrospective facial recognition search results, including requirements for human review, corroboration and record keeping.

Recommendation 10

By 31 December 2027, the government should establish an independent oversight framework for the police use of facial recognition technology, including retrospective facial recognition.

The framework should clearly allocate responsibilities for oversight, complaints and assurance to one or more of the organisations with existing oversight and avoid duplication of regulatory functions.

Recommendation 11

By 30 June 2027, the College of Policing should review the content and provision of training and continuing professional development for Police National Database users who carry out retrospective facial recognition (RFR) searches.

The College of Policing should make sure personnel who use or support the use of RFR receive up-to-date training on:

- image quality and preparation;
- interpreting RFR search results;
- the limitations of facial recognition technology;
- bias, ethics and data protection considerations; and
- the appropriate use of RFR in investigations.

Recommendation 12

By 30 June 2027, the College of Policing should make sure guidance on retrospective facial recognition (RFR) is included in existing national investigator training programmes. This should include guidance on:

- identifying and recovering material suitable for RFR searches;
- preparing and submitting images for RFR searches;
- interpreting RFR search results;
- the requirement to corroborate potential matches through further enquiries;
- supervisory responsibilities; and
- continuing professional development and updates on emerging good practice.

Recommendation 13

By 31 December 2027, chief constables and the director general of the National Crime Agency should make sure all officers and relevant staff involved in using retrospective facial recognition (RFR) receive mandatory training, supported by ongoing continuing professional development. This training should cover:

- identifying and recovering material suitable for RFR searches;
- preparing and submitting images for RFR searches;
- interpreting RFR search results;
- the requirement to corroborate potential matches through further enquiries;
- supervisory responsibilities; and
- continuing professional development and updates on emerging good practice.

Recommendation 14

By 31 December 2027, chief constables and the director general of the National Crime Agency should review the retrospective facial recognition search system. They should consider either:

- establishing centralised teams in their organisations to carry out their retrospective facial recognition searches; or
- giving responsibility for carrying out their retrospective facial recognition searches to established teams such as force intelligence.

Recommendation 15

By 31 December 2027, the National Police Chiefs' Council should consider removing the facility for carrying out retrospective facial recognition searches from personnel who aren't part of a centralised or established retrospective facial recognition team.

Recommendation 16

By 30 June 2027, chief constables and the director general of the National Crime Agency should make sure force and National Crime Agency investigation policies and procedures include guidance on using retrospective facial recognition (RFR).

As a minimum, these policies should:

- make clear that RFR results provide intelligence rather than evidence;
- require investigators to record decisions and actions arising from RFR searches; and
- set out supervisory responsibilities for reviewing the use of RFR and the action taken after potential matches.

Introduction

Background

Since Victorian times, police forces in England and Wales have used images to help identify suspects. They used the 'Police Gazette' and other publications to share information about wanted people and offenders. Investigators circulated descriptions, photographs and notices of wanted criminals, which allowed forces to compare information and identify suspects. The 'Police Gazette' remained in use until 2017.

Facial recognition technology has been an important advance for suspect identification. Investigators can now compare images with custody images held on national computer systems and get results in seconds, rather than waiting days or weeks.

Since 2013, forces have routinely used the Police National Database (PND) to carry out retrospective facial recognition (RFR) searches. At the time of our inspection, we were told that investigators carried out about 24,000 RFR searches a month. The growing availability of image sources, such as CCTV and video doorbells, is likely to increase the number of RFR searches further.

During our inspection, we found that some forces operated their own alternative RFR systems. We explain this in more detail in the section on different facial recognition systems.

Forces' use of RFR to identify unknown suspects helps reduce the widespread, routine sharing of images by the police with the public. We found that the public generally supported the police service's use of RFR. But continuing public support for RFR will depend on maintaining public confidence, openness about its use and effective safeguards.

Police forces use RFR to help identify suspects in a range of investigations. For example, after an attack on a woman, South Wales Police used RFR to identify a suspect from CCTV images. The suspect was later convicted and sentenced to life imprisonment. In another case, Surrey Police used RFR to identify a man suspected of drugs offences. Investigators obtained a CCTV image showing the suspect buying a mobile phone top-up card. An RFR search returned a potential match, which officers then confirmed through other investigative methods. Officers subsequently arrested the suspect.

In 2024, the National Physical Laboratory tested the PND RFR algorithm (set of instructions) for equitability (bias). It found that, despite the algorithm's overall level of accuracy, at some settings it was more likely to incorrectly include people with certain protected characteristics in its search results.

In our inspection, we found that RFR provided a valuable investigative capability. But we also found that the police service needed to improve its governance, consistency and accountability in relation to RFR. This will help it to maximise the effectiveness of RFR and maintain public support for its use.

About us

His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) independently assesses the effectiveness and efficiency of police forces and fire and rescue services to make communities safer.

In preparing our reports, we ask the questions that the public would ask and publish the answers in accessible form. We use our expertise to interpret the evidence and make recommendations for improvement.

Our commission

On 12 November 2025, the Home Secretary commissioned HM Chief Inspector of Constabulary and Fire & Rescue Services under section 54(2B) of the Police Act 1996 and 11(2)(b) of the Crime and Courts Act 2013 to inspect the use of retrospective facial recognition by selected police forces and the National Crime Agency. This was to include reviewing practices to confirm they align with guidance and policies and confirming what training officers have received.

Our terms of reference

Our terms of reference were to address the following three questions:

1. To what extent are local, regional and national guidance, policies and governance arrangements for retrospective facial recognition fit for purpose?
2. How well do police forces and the National Crime Agency train their investigators to use retrospective facial recognition in investigations?
3. How well do investigators understand and follow the required investigative processes after identifying a potential facial recognition match?

Methodology

Our inspection fieldwork took place between 3 March and 30 April 2026. We carried out fieldwork in seven police forces in England and Wales:

- British Transport Police
- Cheshire Constabulary
- Dorset Police

- Gwent Police
- Metropolitan Police
- Northumbria Police
- Surrey Police.

We also inspected the National Crime Agency. In this report, subsequent references to police forces apply equally to the National Crime Agency.

We carried out:

- 91 interviews and focus groups with personnel in police forces and the National Crime Agency;
- reality testing, including speaking with specialist investigators, frontline personnel and supervisors; and
- a review of 416 documents, including national guidance and legislation and force records such as relevant policies, internal communications, meeting minutes, performance data and audit reports.

We made additional visits to Merseyside Police and West Yorkshire Police to increase our understanding of various aspects of RFR. Our visit to Merseyside Police informed how we developed our inspection framework. During our visit to West Yorkshire Police, we saw its innovative FaceReveal application. We outline this example of promising practice in our chapter on guidance, policies and governance arrangements.

- We consulted representatives from other bodies, including:
- Big Brother Watch
- Liberty
- the Home Office
- the National Physical Laboratory
- the Information Commissioner's Office
- the Forensic Science Regulator
- the Biometrics and Surveillance Camera Commissioner
- National Police Chiefs' Council leads for PND and RFR
- the Association of Police and Crime Commissioners lead for RFR.

We also considered the findings from a 2026 Home Office survey of PND facial search users.

The use of facial recognition technology in policing

The police use different types of facial recognition technology

The police use three types of facial recognition technology:

1. retrospective facial recognition (RFR)
2. live facial recognition
3. operator-initiated facial recognition.

In this inspection, we only examined the use of RFR.

RFR

Police forces can use RFR after an incident or during a criminal investigation. This technology helps investigators to quickly identify potential suspects and missing or deceased people.

Investigators often obtain images from CCTV, mobile phones, dashcams, video doorbells and social media, which are called probe images. Investigators then compare probe images with existing custody images that are taken when suspects are arrested.

In principle, the police could use RFR technology to help identify victims or witnesses, but we found limited evidence of forces using it for these purposes.

Live facial recognition

Police forces use live facial recognition to analyse live video footage of people passing a camera in a public place. The technology compares these images with a predefined list of people wanted by the police, known as a watchlist. After a potential live facial recognition match, a police officer decides what action to take.

Operator-initiated facial recognition

Some police forces also use operator-initiated facial recognition technology. Officers can use a dedicated application on a mobile device to carry out a facial recognition search and help establish a person's identity. In some circumstances, this means that officers don't need to arrest a person and take them into custody just to confirm who they are. Any result returned by the technology is treated as intelligence and must be assessed by the officer before any action is taken. At the time of our inspection, a small number of police forces were testing the use of operator-initiated facial recognition.

The public generally support the police's use of RFR technology but have some concerns

In December 2025, the Home Office published the results of its survey 'Public attitudes to police use of facial recognition technology'. In the survey, 64 percent of respondents supported the police's use of facial recognition technology.

The survey didn't include specific questions to measure support for RFR, but it did examine the acceptability of different facial recognition capabilities. Survey results showed that:

- RFR had the highest level of public acceptability (97 percent) of the three facial recognition capabilities examined;
- public acceptability of live facial recognition ranged from 88 percent to 91 percent, depending on its purpose; and
- the public were most accepting of facial recognition technology when police used it to investigate serious offences or protect vulnerable people.

The results of several previous surveys have indicated high levels of public support for the use of facial recognition technology in policing. In 2019, the Ada Lovelace Institute found that about 70 percent of the UK population supported its use by the police in criminal investigations. In 2025, the Ada Lovelace Institute and the Alan Turing Institute found that 91 percent of the UK public thought the use of facial recognition technology was beneficial for policing.

In June 2025, the King's College London Policy Institute, in partnership with Liberty, carried out a survey examining public opinion of police use of facial recognition technology. It found that 53 percent of respondents agreed they were comfortable with the police service's use of RFR technology.

The findings of these surveys suggest that the public generally support the police service's use of RFR and are most accepting of its use when it may help to prevent harm or investigate serious crime.

But people don't support its use unconditionally. The Information Commissioner's Office found that people were least comfortable with the use of RFR when it involved searching against publicly accessible online images, such as those obtained from social media platforms.

The results of the King's College London 2025 survey also showed that respondents were concerned about issues such as:

- the use of RFR by private companies;
- the use of RFR to identify victims and witnesses as well as suspects;
- proposals to expand image reference libraries to include data from other agencies, such as HM Passport Office and the Driver and Vehicle Licensing Agency;
- the possible unlawful retention of custody images on the Police National Database (PND); and
- failures to carry out appropriate checks before making arrests.

In the survey, 46 percent of respondents who were uncomfortable with the police use of facial recognition technology thought that it infringed their personal privacy. Survey respondents also raised several other concerns about the police use of facial recognition technology. These included the potential for misuse, data breaches resulting from hacking and incorrect identification.

The media has often reported on concerns about the police service's use of facial recognition technology, including alleged misuse of RFR. For example, in one case, police arrested a man for a burglary that took place at a location many miles from where he lived and to which he had no known connection.

The existing legal framework for the use of RFR is complex

We found that legislation governing the use of RFR was spread across many statutes. In some respects, legislation hasn't kept up with developments in technology. This makes it more difficult for law enforcement agencies and private companies to interpret and apply the law when using RFR and for the public to understand it.

Common law provides the legal basis for police forces to use RFR. These powers arise from the core policing duties to:

- protect life and property;
- preserve order and prevent threats to public security;
- prevent and detect crime;
- bring offenders to justice; and
- uphold national security.

The use of these powers must be lawful and compatible with relevant human rights and data protection obligations. This means forces must comply with the provisions of other relevant legislation in their use of RFR technology, including:

- Human Rights Act 1998;
- Equality Act 2010;
- Data Protection Act 2018 (and UK General Data Protection Regulation); and
- Freedom of Information Act 2000.

The use of live facial recognition is examined in existing legal case law, including Bridges v South Wales Police. At the time of our inspection, no case law had specifically considered RFR.

Two laws are relevant to police investigations that involve the use of RFR

The Criminal Procedure and Investigations Act 1996 governs criminal investigations and the disclosure of evidence in England and Wales. It aims to promote openness and consistency in how investigators and prosecutors handle cases and to help make sure trials are fair.

The Act applies to all aspects of an investigation, including RFR. Records relating to RFR use aren't evidential. This means investigators must record any use of RFR during their investigation.

The Police and Criminal Evidence Act 1984 sets out the circumstances in which police may arrest a person in connection with their involvement, or suspected involvement, in a criminal offence. A constable may only exercise the power of arrest if they have reasonable grounds to believe that an arrest is necessary and that at least one of the statutory necessity criteria applies, as explained in Code G 2012 of the Police and Criminal Evidence Act 1984.

When deciding whether to arrest a person, a constable must consider the individual circumstances of the case. This includes the needs of the investigation, the nature of the offence, the circumstances of the suspect and the situation of the victim.

Officers may later take no further action if they can't find enough evidence to support a prosecution. This doesn't necessarily mean that the arrest was unlawful or unnecessary. In some cases, an arrest may help officers gather evidence that eliminates a suspect from their enquiries. It also provides suspects with several protections, including:

- free legal representation;
- limits to police powers;
- protection against abuse or mistreatment; and
- access to legal remedies such as a fair trial or compensation.

The Police National Database has an RFR function

In 2011, the Home Office introduced the Police National Database (PND) after the murders of Holly Wells and Jessica Chapman in Soham in 2002 and the subsequent Bichard Inquiry. The inquiry found shortcomings in how intelligence was shared between police forces and recommended a new national intelligence system. This led to the development of the PND, which allows information about people, objects, locations and events to be shared across forces.

The PND brings together data from all 43 police forces in England and Wales, as well as Police Scotland, the Police Service of Northern Ireland, the National Crime Agency and other organisations. It contains billions of records drawn from several hundred databases.

In 2013, the Home Office added an RFR function to the PND, which was upgraded in 2021. This function allows users to search custody images to help identify unknown persons of interest. The PND custody image database draws on individual force systems and contains more than 20 million images.

PND code of practice

The code of practice on the operation and use of the Police National Database came into force in 2010 under section 39A of the Police Act 1996. It sets out the statutory framework and national standards that govern how police forces in England and Wales share, access and manage information on the PND.

Chief officers are responsible for making sure their forces comply with the requirements of the code of practice. The National Police Chiefs' Council, through the PND national steering group, provides national co-ordination and oversight of the PND's use.

RFR searches on the PND

The police use the PND to carry out most of their RFR searches.
Typically, investigators obtain an image of an unknown person from sources such as CCTV, doorbell cameras, mobile phone footage or still photographs. This image, known as a probe image, is prepared and submitted for comparison against custody images held on the PND. The search may help investigators identify a person in the image and generate investigative leads.

Only trained licence holders can carry out RFR searches on the PND.
Investigators submit probe images to a licence holder, who carries out the search for them. To achieve the best results, probe images should, wherever possible, show a clear frontal view or side profile of the person.

An RFR search on the PND produces a ranked list of the most similar images. PND data shows that in the year ending 31 March 2026, 74 percent of submitted RFR searches returned at least one face match. Where a search returned a face match, the system usually returned multiple potential matches, with an average of between 9 and 15 for each search.

The PND manual of guidance clarifies that police forces and other agencies should apply additional safeguards when using facial searching. These include:

- trained PND users and investigators visually reviewing all potential matches, as results may include images that are clearly not the same person;
- investigators carrying out additional enquiries where a potential identification is made, as facial search results are intelligence only and not evidential; and
- investigators following Code D 2023 of the Police and Criminal Evidence Act 1984 for formal identification procedures and pursuing other viable lines of enquiry.

This means that an RFR result can only be used as an investigative lead and not as identification evidence. If investigators need identification evidence to support a charge or prosecution, they must use one of the formal identification procedures set out in Code D, such as video identification or an identification parade.

There are benefits and risks to using RFR technology

The facial search function within the PND uses a commercial algorithm to compare biometric data. It can help investigators quickly identify unknown people who may:

- present a risk to the public;
- have committed a criminal offence; or
- be at risk of harm.

An RFR search may produce a list of potential matches but a maximum of one true match. For testing purposes, the National Physical Laboratory classifies all other potential matches as false positives.

The National Physical Laboratory operates as the UK's National Metrology Institute and is owned by the Department for Business, Innovation, Science and Trade. It develops and maintains the UK's primary measurement standards and works with national metrology institutes in other countries to support the international system of measurement.

In 2024, the Home Office asked the National Physical Laboratory to assess the performance of the facial recognition algorithm in an operational setting. Its assessment examined accuracy and equitability (bias) in relation to demographic groups. It found that, under certain system settings, the false positive identification rate was higher for some demographic groups than for others. This result meant that the system was more likely to include people from those groups in a list of potential matches.

The company that operates the PND can adjust the system's sensitivity settings. The National Physical Laboratory found that, after making these adjustments, the differences in performance between demographic groups were no longer statistically significant. The changes also reduced the number of results the system returned and, in turn, reduced the likelihood of identifying a true match.

The National Physical Laboratory found that the system's performance varied between demographic groups. For example, a person's likelihood of being included in a candidate list was greater for:

- women than men;
- Asian or Black people than White people; and
- Black women than Black men.

There were similar variations in different age ranges. For example, people aged 21–29 years were more likely to be included in a candidate list than people in other age groups.

It told us that this evaluation alone couldn't determine the full extent of any bias. It emphasised that the effect of these differences in operational use depended on several factors, including the submitted image's quality, the quality of images held on the PND and the processes that forces use to review and act on matches alongside other evidence.

To what extent are local, regional and national guidance, policies and governance arrangements for retrospective facial recognition fit for purpose?

The legal framework governing the use of facial recognition is spread across many statutes. Police use of the technology primarily relies on powers set out in common law. In some respects, legislation hasn't kept up with developments in technology. This is making matters complex and unclear. The lack of specific legislation governing the police use of facial recognition and related biometric technologies appears to have created some uncertainty about the lawful basis for their use and the safeguards needed to protect the public.

During our inspection, we found that policing in England and Wales used retrospective facial recognition (RFR) technology in a fragmented way, with limited oversight. Forces often couldn't clearly show any improvements in their performance from using RFR.

Guidance on the police use of RFR technology is limited

While the Police National Database (PND) code of practice influences how forces use RFR, it doesn't provide a comprehensive regulatory framework or detailed guidance for its use.

At the time of our inspection, no statutory code of practice governed the use of RFR. All the police forces that we visited used RFR to support their investigations. It was clear that they were relying on a range of guidance to inform their use, including:

- the PND manual of guidance;
- the College of Policing PND facial search user guide;
- the PND code of practice; and
- Home Office PND facial searching guidance.

We consider that this has led to forces developing their use of RFR in different ways. The lack of a specific regulatory framework also makes it more difficult for forces and the public to understand how legal duties apply.

National and regional governance of RFR could improve

The National Police Chiefs' Council (NPCC) has two groups with responsibilities in this area:

1. the national facial recognition technology board
2. the PND national steering group.

We attended meetings of both groups. Neither group has specific responsibility for RFR governance, but at these meetings, group members discussed the use of RFR technology.

The NPCC has set national actions to reduce the risk of algorithm bias in RFR, but the police service needs to do more

In September 2024, the NPCC lead for the PND set several national actions to mitigate the risk of algorithm bias seen in the National Physical Laboratory's test results. These actions included:

- increasing the sensitivity of the algorithm;
- reviewing and reissuing PND training and guidance;
- reviewing the PND data protection impact assessment (DPIA); and
- completing an equality impact assessment.

On 8 November 2024, the NPCC lead for the PND wrote to chief constables to inform them of technical changes to the facial search algorithm after the National Physical Laboratory's test.

The letter reminded chief constables that facial search results provide intelligence rather than evidence. It emphasised that users must visually review facial search results and develop corroborative lines of enquiry to validate any potential matches before taking operational or investigative action. The letter also included links to relevant guidance and supporting materials.

Later that month, the NPCC lead decided to reduce the algorithm setting after operational feedback from police forces and concerns that the higher setting may have limited investigators' opportunities to identify potential suspects. On 28 November 2024, the NPCC lead wrote to chief constables to explain the change. The letter stated that the revised setting would increase the number of potential matches returned by the system and provide investigators with more intelligence opportunities.

These measures aim to reduce the risks associated with bias in the algorithm while maintaining forces' operational effectiveness.

We found that most forces we visited aimed to follow this approach. But more needs to be done to reduce the risks of people being wrongly arrested. This includes having stronger governance, clear national guidance and a coherent, independent regulatory framework.

We found little evidence of regional governance of RFR use

Throughout England and Wales, regional PND user groups meet regularly and help forces to share information about PND-related matters, including RFR. These regional groups inform the PND national steering group.

In our inspection, we found little evidence of regional co-ordination or governance of forces' use of RFR technology.

Force governance arrangements for RFR vary

We found variation in how the forces we inspected managed their use of RFR. Some forces clearly understood the benefits of RFR and had established centralised teams to support its use. Others had adopted a less structured approach. We explain these differences in more detail in the section on different force approaches to using RFR.

We concluded that the effectiveness of forces' use of RFR was supported by having:

- equality impact assessments for RFR;
- DPIAs for RFR;
- a force RFR policy;
- oversight structures; and
- systems to collect relevant management information.

We discuss each of these in turn.

Equality impact assessments

The Equality Act 2010 puts a legal obligation on police forces to comply with the public sector equality duty to prevent discrimination because of a protected characteristic. Forces should set out how they will meet this duty in an equality impact assessment developed specifically for RFR.

Positively, all the forces we inspected had published an equality impact assessment for RFR.

Data protection impact assessments

Under the UK General Data Protection Regulation and Data Protection Act 2018, a data protection impact assessment (DPIA) is a legal requirement where processing of data is likely to result in a high risk to people's rights and freedoms. Police use of RFR involves the processing of personal data in this way. Forces must set out how they identify and minimise data protection risks in their use of the technology in a DPIA. While it isn't a legal requirement for forces to publish their assessments, five forces we inspected had published DPIAs relating to their use of RFR.

Two forces relied on the national DPIA for the PND. The National Crime Agency has produced a DPIA covering its use of RFR in processing small boat arrivals, which doesn't involve searching the PND image database.

We found that forces' DPIAs provided detailed records of the measures they had put in place to mitigate the privacy and data protection risks associated with using RFR.

The national DPIA for the PND provides the mitigation measures that apply nationally. But it doesn't take account of local operating models and provides only limited support to forces in managing the risks associated with their use of RFR.

Recommendation 1

By 30 June 2027, chief constables and the director general of the National Crime Agency must make sure police forces and the National Crime Agency carry out and record a data protection impact assessment to address their use of retrospective facial recognition technology.

Force RFR policies

Four of the forces we inspected hadn't developed local guidance and relied instead on limited national publications, primarily the PND manual of guidance. The other forces had developed detailed local policies and procedures that set out how they use RFR in several areas, including:

- governance
- work with the public
- testing equitability
- performance metrics
- guidance
- system security
- data management.

The policies and guidance we reviewed adequately covered the main areas we would expect forces to consider when using RFR.

But some personnel we spoke to told us that they weren't aware of the policies and guidance that governed the use of RFR and their responsibilities when they received a potential RFR match.

Force oversight of RFR

We found that forces were managing their use of RFR in different ways. For example, British Transport Police and Gwent Police held monthly facial recognition board meetings, chaired by senior leaders, to oversee the force's use of the technology. At these meetings, tactical leads reported on performance, operational issues and governance matters, so that senior leaders could provide oversight and make decisions about the force's use of RFR.

Cheshire Constabulary reported its use of RFR to a weekly crime accountability meeting. In some other forces, we found that no clear structures were in place to oversee and manage the use of RFR.

Systems to collect management information

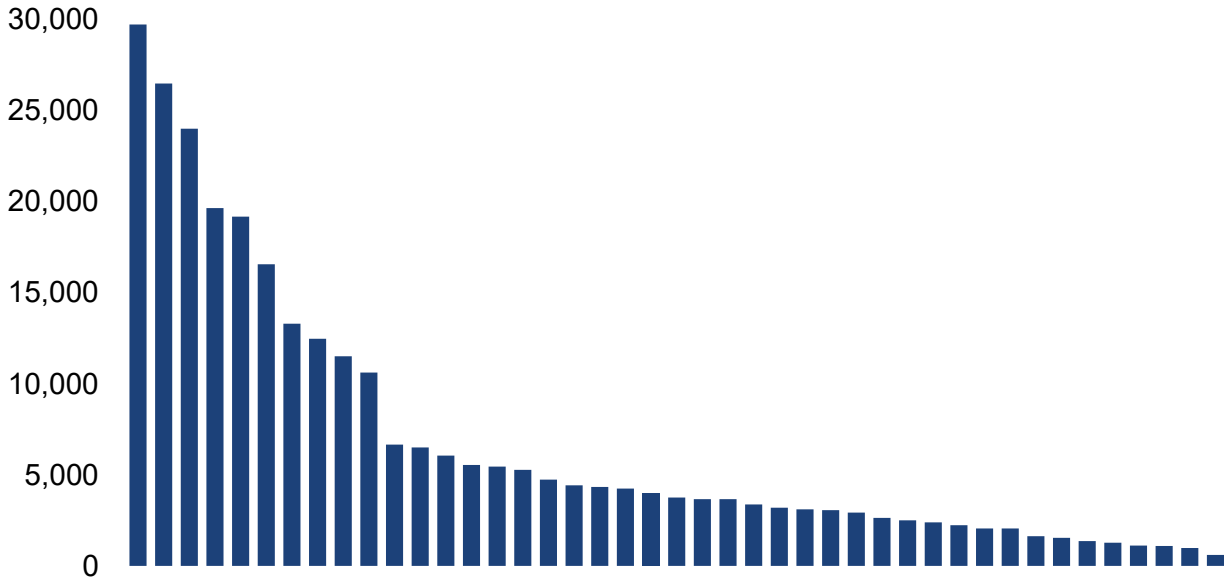
Throughout this inspection, we found that most forces held limited management information about their use of RFR. The data available from the PND was also limited and provided only basic information, such as the total number of searches carried out by forces and other agencies and the broad reasons for the search.

PND data indicates that RFR is being underused in some forces

We examined data from the PND that showed:

- the number of RFR searches carried out each month by police forces;
- the number of searches as a proportion of recorded crime;
- the average number of potential matches for each RFR search; and
- the proportions of successful and unsuccessful searches.

Figure 1: Number of retrospective facial recognition searches across anonymised forces in England and Wales between 1 April 2025 and 31 March 2026



Source: Police National Database from the Home Office

Chart description: Bar chart showing the number of retrospective facial recognition (RFR) searches that each police force in England and Wales carried out on the Police National Database between 1 April 2025 and 31 March 2026. In total, forces carried out 291,341 RFR searches during the year. The data shows substantial variation across forces, ranging from 611 to 29,742 searches. Only two forces carried out more than 25,000 searches during the year, averaging around 2,500 and 2,200 searches a month, respectively. By contrast, several forces carried out around 1,000 searches during the same period, averaging between 80 and 90 searches a month. This chart has been anonymised to illustrate national patterns and variation, rather than to rank individual forces.

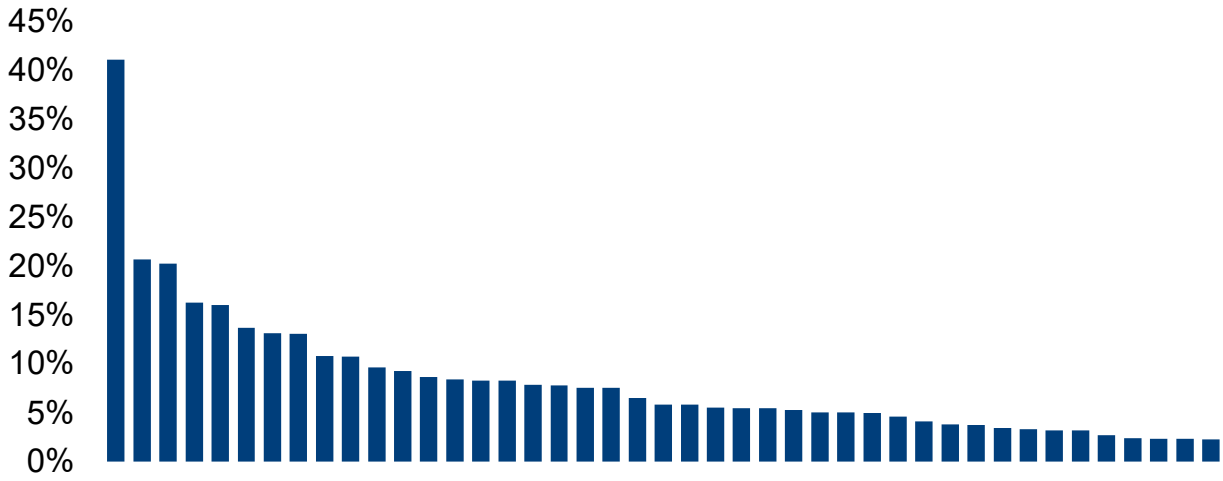
This wide variation in the number of searches suggests that forces use RFR to different extents. Given the investigative benefits that RFR can provide, we consider that some forces may not be making full use of the capability.

In March 2025, we published our report about how effectively the police investigate crime. We found that forces didn't use PND facial searching as much as they could. This was often due to a lack of knowledge of its capabilities and a misunderstanding of the benefits it can bring to an investigation. We also found that some forces promoted its use more than others. In our report, we recommended that:

> "By 30 June 2025, chief constables should include in their investigation policies a direction stating that when an image exists, investigators should search it against the Police National Database and any other relevant databases before their force closes an investigation."

As at 1 August 2026, 24 of the 43 forces in England and Wales had completed this recommendation.

Figure 2: Retrospective facial recognition searches as a percentage of recorded crime across anonymised forces in England and Wales between 1 April 2025 and 31 March 2026



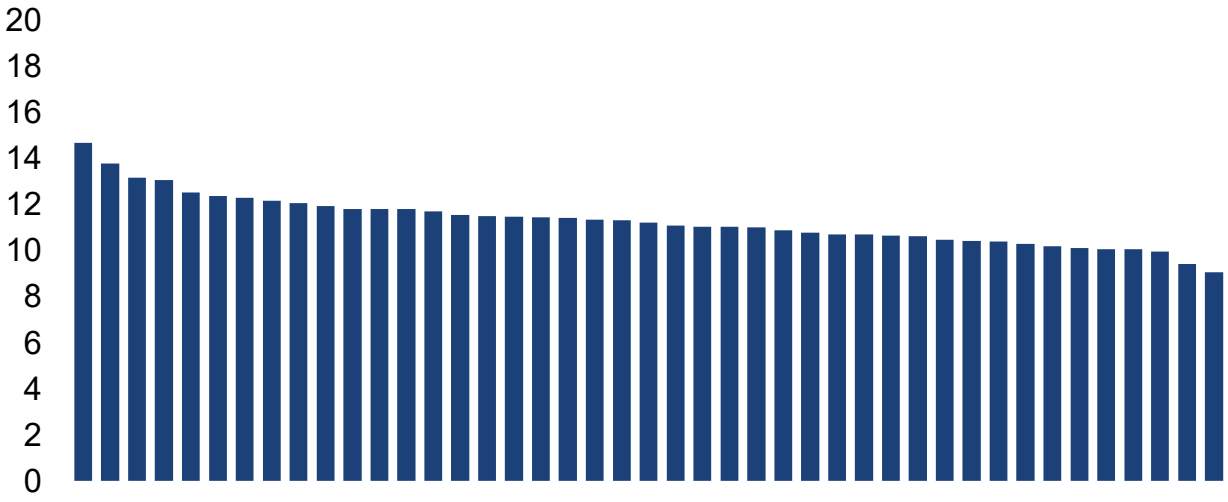
Source: Police National Database and police recorded crime from the Home Office

Chart description: Bar chart showing retrospective facial recognition (RFR) searches as a percentage of recorded crime for each anonymised police force in England and Wales between 1 April 2025 and 31 March 2026. The chart shows considerable variation in the use of RFR as a percentage of recorded crime across forces. The percentage of RFR searches relative to recorded crime ranged from 2.2 percent to 41.1 percent. Most forces (33) carried out RFR searches equivalent to less than 10 percent of their recorded crime, while only 3 forces exceeded 20 percent.

Note: We used police recorded crime for the year ending December 2025 to calculate the percentages. It was the most recent data available at the time of our fieldwork.

This variation suggests that forces use RFR to very different extents. Given the scale of the differences, some forces may not be making full use of RFR as an investigative tool.

Figure 3: Average number of images returned for retrospective facial recognition searches across anonymised forces in England and Wales between 1 April 2025 and 31 March 2026



Source: Police National Database from the Home Office

Chart description: Bar chart showing the average number of images returned for retrospective facial recognition searches carried out by each police force in England and Wales between 1 April 2025 and 31 March 2026. The chart is ordered from the highest to the lowest average number and shows variation in the average number of images returned for each retrospective facial recognition search. The average ranged from 9.1 to 14.7. Only two forces had an average below ten.

Forces need to do more to fully understand the benefits and effects of using RFR

We found substantial variation in the data that forces collected about RFR, how they collected it and how they used it. Most of the forces we inspected hadn't adopted a structured approach to collecting this data and weren't making full use of it to understand performance, identify risks and improve their use of RFR.

As a result, forces couldn't provide accurate information on their use of RFR, including:

- the number of cases with RFR matches;
- the status of each case;
- the number of overdue cases (those with outstanding actions that hadn't been completed by a deadline set by a supervisor); and
- any outcomes.

The lack of management information about how forces use RFR meant we couldn't identify cases where forces may have taken inappropriate action. For example, without data and analysis on RFR matches and how these relate to arrests and the outcomes of cases, we couldn't establish with certainty whether the bias identified in the algorithm had contributed to any wrongful arrests.

Forces need to better understand the impact of RFR on crime outcomes

All the forces we inspected found it difficult to assess the effect of RFR on crime outcomes and show how RFR contributes to detecting crime.

Some forces had attempted to measure the relationship between positive RFR matches and performance measures such as detection rates. For example, Cheshire Constabulary set up Operation Identifying to analyse investigative outcomes. It found that cases involving at least one positive RFR match were more likely to result in a positive outcome, such as a charge, caution or community resolution, than cases where no positive match was identified.

Forces found it difficult to assess RFR's contribution to investigative outcomes because they lacked consistent recording processes and systems capable of automatically extracting and analysing this information. For example, forces could record whether RFR had been used and whether a positive match had been returned. But most lacked the capability to routinely link this information to crime and case management systems and analyse case outcomes. It was often difficult for them to collect the data and assess the contribution that RFR makes to positive outcomes.

For many years, forces have quickly closed investigations for some volume crime offences because of limited lines of enquiry. The College of Policing's authorised professional practice guidance on managing effective investigations highlights the need to prioritise resources and investigative opportunities for volume crime.

We found that some forces had established teams to investigate retail crime and other volume crime offences. They told us that RFR had improved outcomes in their investigations. For example, Gwent Police and South Wales Police introduced Operation Grammica, which aims to tackle retail crime and strengthen work with local businesses. This operation helps shops to improve how they identify, collate

and provide CCTV images for RFR searches. This has increased the likelihood of successful RFR searches and helped investigators identify suspects more effectively.

The increased availability of digital evidence, together with the development of RFR technology, is likely to increase opportunities to identify suspects and detect these offences. But this is also likely to affect investigators' workloads and forces' capacity to investigate crime.

Some forces are improving how they collect RFR management information

Two of the forces we visited had introduced standardised processes for submitting RFR search requests through applications they had developed. These applications automatically record data about each RFR search. The forces use this information to create management dashboards that help them assess how effectively they use RFR and improve working practices.

Promising practice: West Yorkshire Police has developed FaceReveal software to manage retrospective facial recognition processes

In 2024, West Yorkshire Police developed software to manage its retrospective facial recognition (RFR) processes. This software allows investigators and staff who manage the FaceReveal application to submit images, format them to optimise the potential for a match and update crime recording systems with the results. It also gathers data to support effective governance.

Investigators use the system to submit all RFR requests to a centralised team. Personnel in this team then submit images to the Police National Database for searching. They assess the results and carry out further enquiries to identify additional information. The system also notifies investigators when it rejects images and explains the reasons for rejection.

The FaceReveal system automatically generates management information, which the force uses to support governance and continuous improvement.

Between 1 January 2025 and 31 March 2025, the force told us that it carried out 590 RFR searches, which resulted in 188 potential matches. During the same period in 2026, it carried out 1,000 searches and identified 290 potential matches. This shows that the force is making greater use of RFR.

The College of Policing has included an example of this practice, using facial recognition to identify suspects of knife-enabled robbery, in its practice bank.

Recommendation 2

By 31 December 2027, the National Police Chiefs' Council should establish national requirements for collecting, analysing and reporting retrospective facial recognition management information.

The requirements should define the minimum management information that forces must collect, analyse and review to support effective oversight, audit, assurance and evaluation of outcomes. This should draw on existing good practice identified in policing.

Recommendation 3

By 31 December 2027, chief constables and the director general of the National Crime Agency should make sure police forces and the National Crime Agency routinely collect, analyse and review retrospective facial recognition information to:

- assess the effectiveness and outcomes of using retrospective facial recognition;
- identify risks and any actual or potential adverse impacts;
- support local and national governance and accountability arrangements;
- allow independent scrutiny and oversight; and
- support continuous improvement in the use of the technology.

Forces need to improve their auditing of RFR searches

The NPCC develops national guidance for PND and RFR auditing. It collects and reviews audit information submitted by forces, but it doesn't audit individual forces. Forces are responsible for auditing their own activity and should provide quarterly assurance reports to the PND national steering group. The steering group reviews forces' own audit data to assess compliance and provides feedback to forces in need of improvement.

The guidance states that forces should appoint independent auditors. These auditors shouldn't check their own activity and should have a good understanding of the PND, local deployment arrangements, user behaviour and access levels. Auditors should also understand how to use the PND audit interface and be able to identify patterns, trends and anomalies within forces' use of the system.

The guidance recognises that these audits are an important safeguard. The audits help forces identify any misuse, errors or inappropriate use of the system. They also provide assurance that personnel use facial searching lawfully and proportionately.

Forces must audit at least 1 percent of all PND searches. At least 25 percent of these audits should relate to RFR searches. During our inspection, we examined how forces carried out these audits and reviewed national data provided by the NPCC.

We reviewed NPCC data on force compliance with RFR audit requirements and found that:

- 7 forces hadn't appointed an auditor;
- 2 auditors couldn't access the PND;
- 10 forces appeared to have audited more records than required; and
- 22 forces either failed to submit a return or submitted incomplete information.

Only two forces had audited the correct number of RFR searches. These findings indicate that many forces lack effective oversight of their use of RFR searches and aren't complying with national audit requirements.

During our inspection, we found variation in how forces audited PND transactions. For example:

- in some forces, it wasn't clear whether personnel used the data for any purpose beyond monitoring the number of searches carried out;
- some forces used the data to monitor the number of searches carried out by individual PND users and to assess whether they still needed a PND licence;
- some forces carried out audits through dip sampling and followed up with officers in charge of investigations when they identified concerns; and
- one force was developing a process to track investigations and report on performance, including data on the contribution that RFR makes to positive outcomes.

These examples show the different levels of scrutiny and oversight that forces apply to their use of RFR and PND searches.

We found that forces' audit activity focused on the PND operator who carried out the search rather than the investigator who requested it. We consider this a weakness in the audit process. Focusing audits on the PND operator may identify whether a search was carried out correctly. It won't identify any misuse or assess whether search results were interpreted correctly or whether enough investigative work was carried out before enforcement action was taken. As a result, forces may not identify risks or poor practice.

NPCC data showed that audits of RFR searches hadn't identified any confirmed adverse incidents. Most of the issues auditors identified related to how users carried out searches rather than to the technology itself.

For example, some users failed to apply available search filters, such as gender or ethnicity, which may reduce the quality of potential matches and possibly increase bias. Auditors also identified cases where users uploaded poor-quality or unsuitable probe images, including blurred images and images containing multiple faces. These factors reduced the system's ability to return reliable matches.

Forces don't routinely collect management information on how investigators use RFR results, so the audit process provides limited assurance that officers always use those results appropriately.

The King's College London Policy Institute carried out a study in 2025 and identified that 75 percent of respondents thought the police should regularly report on errors made when using facial recognition technology.

Recommendation 4

By 30 June 2027, the National Police Chiefs' Council should review national retrospective facial recognition audit requirements to make sure audits assess both how retrospective facial recognition searches are carried out and the subsequent investigative use of search results. Audit information should include the investigator who instigated the search.

The police service isn't yet meeting its obligation to delete custody images

Section 64A of the Police and Criminal Evidence Act 1984 allows police to photograph a person detained at a police station, with or without their consent. Police forces in England and Wales upload their custody images to the PND, regardless of whether the person is charged or convicted of the offence for which they were arrested.

The College of Policing's authorised professional practice guidance on the management of police information (MOPI) sets out how forces should review, retain and dispose of custody images.

During our inspection, we found that some custody images searchable through the PND were retained in breach of MOPI principles and should have been deleted by forces.

The PND code of practice makes clear that it is the responsibility of force chief officers to decide the:

- information to add to the PND;
- information that shouldn't be added to the PND; and
- restrictions on accessing and using the information.

Chief officers are responsible for making sure their forces develop and implement appropriate procedures and systems for processing personal data in line with the provisions of the Data Protection Act 2018 and other relevant legislation.

The Protection of Freedoms Act 2012 amended the Police and Criminal Evidence Act 1984 to establish a statutory framework for retaining DNA samples and fingerprints taken from suspects. In 2017, the Home Office carried out a review of the use and retention of custody images. It found that introducing a similar statutory framework for custody images wouldn't be appropriate because biometrics for DNA and fingerprints are treated very differently to custody images. Also, police systems couldn't automate the deletion of custody images, and a manual review process would be too time consuming and resource intensive.

Instead, the Home Office introduced a framework for the review, retention and deletion of custody images. This was based on criteria such as the seriousness of the offending and the age of the arrested person. This framework is set out in College of Policing authorised professional practice guidance, which supports forces in their efforts to comply with MOPI. This approach also allows people to apply for the deletion of their custody image when forces no longer have a lawful basis to retain it.

The PND reflects the custody images held by forces. During our inspection, some interviewees expressed concern that forces still didn't always delete custody images in line with MOPI guidance. We didn't explore this in more detail as it was outside the scope of our inspection. But we concluded that some of the images used in RFR searches should have been deleted and yet were still available for RFR searches. This situation risks undermining public confidence in the police service's use of RFR.

We were reassured to find that in October 2023, the NPCC introduced Programme Tabula. This programme aims to establish a more consistent approach to managing custody images across police forces and address the variation in how forces manage custody image datasets.

The Home Office has consulted interested parties on the use of facial recognition technology. In May 2026, the King's Speech introduced the Police Reform Bill, which includes a new legal framework for facial recognition technology. This means that, subject to parliamentary approval, the bill will bring custody images within the same retention and disposal standards as DNA and fingerprints. The Programme Tabula team will:

- review the implications of the new legislative requirements;
- design an operating model that supports compliance;
- work with the Home Office law enforcement facial recognition programme to support forces in complying with new legislation;
- work with the College of Policing to review and, where appropriate, update authorised professional practice to reflect new ways of working;
- develop and provide support packages for forces; and

- support the changes that forces need to make to comply with custody image retention requirements.

We welcome this work. It is important that the police service aligns its approach to retaining custody images with other biometric data so that it is consistent and lawful. We look forward to learning how Programme Tabula will support forces in managing custody images more consistently and improving their compliance with legal and data retention requirements.

Some forces are using their own facial recognition systems

Police forces in England and Wales mainly use the PND to carry out their RFR searches. But we found that the Metropolitan Police Service had introduced its own system and that South Wales Police and Gwent Police jointly used a separate system. We were also told that other forces were considering introducing their own systems.

A limitation of these systems is that they search only local custody image databases rather than national datasets. We were told that investigators could follow up negative results from these systems with a further search on the PND. While we understand why forces have adopted this approach, using multiple systems in this way may reduce effectiveness and efficiency. For example:

- in cases that involve cross-border offending, investigators may miss opportunities to identify suspects whose images are held by different police forces;
- each system may require separate algorithm testing and assurance; and
- the use of multiple systems may make it more difficult for any future independent oversight body to scrutinise their use and for forces to audit how investigators use facial recognition technology.

A new national facial recognition system will use a more accurate algorithm for PND facial recognition searches

We have highlighted how testing identified bias in the algorithm used for facial searches of the PND. The Home Office has identified a new algorithm in a project to create a new national facial recognition system for law enforcement use.

The National Physical Laboratory found that this new algorithm could achieve a high level of search accuracy without showing significant differences in performance between demographic groups. The original system often returned multiple potential matches, but the new algorithm usually returned a single potential match for investigators to assess.

The College of Policing is developing a training programme for users of the new system. This programme will include guidance on ethics, fairness, image quality and the appropriate use of facial recognition technology.

Essex Police and Cheshire Constabulary have trialled the system on behalf of the Home Office. These trials will help the Home Office and police forces assess how the system performs in operational settings and identify any changes needed before a decision on national implementation is made.

Importantly, the new system uses a different approach to managing custody images. This dataset links to the same system that already stores biometric data such as fingerprints and DNA. Forces will upload custody images to the new system in the same way that they upload them to the PND. The system will automatically delete images when forces no longer have a lawful basis to retain them. For example, it should delete images when police take no further action or when a court acquits a suspect who has no relevant previous convictions.

This should help forces comply more consistently with custody image retention requirements and reduce the risk of inappropriate images being available for facial recognition searches. As a result, forces should be able to manage custody images in line with the retention requirements set out in the Protection of Freedoms Act 2012.

Recommendation 5

By 31 December 2027, the Home Office should provide policing with a national facial recognition system that supports the consistent, lawful and effective use of retrospective facial recognition across England and Wales.

Where forces use alternative facial recognition systems, the Home Office should make sure they are subject to equivalent standards of governance, performance testing, assurance, audit and oversight.

Forces are missing opportunities to identify suspects

Forces generally carry out an RFR search of the PND only once during an investigation. If the search doesn't identify a potential match and investigators have no other lines of enquiry, they will often close the investigation. As a result, forces may miss opportunities to identify suspects whose custody images are added to the database after the original search.

We found some evidence that forces manually resubmitted unmatched probe images for further RFR searches. For example, British Transport Police told us that it repeated searches for unmatched suspects every six months or one month before the statutory time limit expired. For less serious offences in England and Wales, criminal proceedings must generally begin within six months of the offence being committed.

The PND has a facility called triggered facial searches. This allows users to request that the system regularly carries out further searches of images that didn't initially return a good match. Such searches are carried out automatically on a weekly basis for a period of six months. No further searches are carried out unless the user reactivates the request. If the system identifies a potential match with a recently uploaded custody image, the user is notified in the normal way.

PND data shows that police forces aren't widely using this facility, possibly because it needs to be specifically requested and reactivated by the user.

By contrast, the National DNA Database automatically and continually compares all new DNA profiles against all unidentified crime scene profiles and alerts investigators when it identifies a potential match.

We consider the absence of a similar capability in RFR systems to be a missed opportunity. Future facial recognition systems should be able to automatically retain unmatched probe images and continually compare them against newly added custody images. This would help forces identify suspects who would otherwise remain unidentified and make better use of facial recognition technology as a preventative and investigative tool.

Forces don't always consult the public about using RFR

Four of the forces we inspected told us that they had consulted with the public in their areas. For example, the Metropolitan Police Service has established a facial recognition board and uses its safer neighbourhood meetings to work with its communities. But three forces told us that they hadn't carried out any public consultation on their use of RFR.

Three forces also told us that they had published material on their use of RFR, including policies, standard operating procedures, DPIAs and explanations of how they use the technology. The remaining four forces hadn't published such material and limited their communications to reporting successful uses of RFR.

This has the potential to affect public confidence. Forces should strengthen their arrangements for consulting local communities about using facial recognition technology. They should consider and respond to any concerns the public raise about how police use these technologies. This will help maintain public trust and confidence.

Recommendation 6

By 30 June 2027, the National Police Chiefs' Council should develop national guidance for police forces and the National Crime Agency on communication and consultation with the public and openness about police use of facial recognition technology.

Recommendation 7

By 30 June 2027, chief constables should make sure their forces have arrangements in place to work with local communities and maintain openness about their use of facial recognition technology.

These arrangements should include the publication of relevant policies and governance documents, opportunities for consulting and working with the public and processes for considering and responding to community concerns.

A national regulatory framework is needed to help govern the use of RFR

In our inspection, we found that the lack of a clear national framework had led some forces to develop their own RFR working practice, governance, policy and audit processes.

Between 4 December 2025 and 12 February 2026, the Home Office consulted widely with interested parties and the public about the use of biometrics including facial recognition technology. After this consultation, the Home Office proposed a new legal framework and independent oversight for law enforcement use of facial recognition and similar technologies. This will make it clear when use of these technologies is justified. The forthcoming Police Reform Bill will include these proposals.

The use of biometric technologies, including RFR, is increasing. This means that forces need a clearer statutory framework to govern how they use them. Such a framework would support the effective and consistent use of facial recognition technology and help maintain public trust and confidence.

During consultation and public debate about facial recognition technology, several issues were commonly raised. A statutory framework would provide clarity on, for example:

- the use of facial recognition technology by private companies, particularly live facial recognition;
- the use of RFR to identify victims and witnesses as well as suspects;
- facial recognition searching of data held by other agencies, such as HM Passport Office;
- the retention of custody images and the circumstances in which forces should delete them; and
- the safeguards and corroborative enquiries that officers should complete before taking executive action after an RFR match.

Addressing these issues through a statutory framework would help provide greater clarity for forces and the public about how RFR should be used and governed.

Recommendation 8

By 30 June 2027, as part of its implementation of police reform legislation, the Home Office should consider including provisions that permit police forces to:

- use algorithms to search databases for a legitimate policing or safeguarding purpose; and
- share results from these searches as required for advancing the relevant policing or safeguarding purpose.

Recommendation 9

By 30 June 2027, the Home Office should introduce a requirement for a statutory code of practice governing law enforcement use of retrospective facial recognition.

The code should include minimum requirements in relation to:

- the lawful purposes for which retrospective facial recognition may be used;
- governance, accountability and audit arrangements;
- training and competence requirements;
- the testing and assurance of facial recognition algorithms; and
- the management and use of retrospective facial recognition search results, including requirements for human review, corroboration and record keeping.

Any new code of practice on the use of RFR needs independent oversight

A new statutory code of practice is needed. At the time of our inspection, no single organisation provided independent oversight of the police use of facial recognition technology.

In its 2023–24 annual report, the Biometrics and Surveillance Camera Commissioner observed that "the use of facial recognition technology remains contentious" and highlighted "potential regulatory and policy deficiencies in its widespread roll-out".

Several regulatory bodies already have responsibilities that relate to RFR, including the:

- UK Biometrics and Surveillance Camera Commissioner
- Information Commissioner's Office
- Forensic Science Regulator.

In addition, the statutory PND code of practice gives HM Inspectors of Constabulary responsibility for monitoring chief officers' compliance with the code, associated guidance and standards.

These existing arrangements may provide a basis for a future oversight model.

We don't believe that the government should create a new regulatory body to oversee RFR. We also don't consider it appropriate for any single existing body to take sole responsibility. This is because responsibilities already overlap and new technologies will continue to emerge.

Instead, the government should allocate responsibility for overseeing concerns and complaints to one or more of the organisations with existing oversight.

Recommendation 10

By 31 December 2027, the government should establish an independent oversight framework for the police use of facial recognition technology, including retrospective facial recognition.

The framework should clearly allocate responsibilities for oversight, complaints and assurance to one or more of the organisations with existing oversight and avoid duplication of regulatory functions.

How well do police forces and the National Crime Agency train their investigators to use retrospective facial recognition in investigations?

The absence of authorised professional practice (APP) guidance or a code of practice for retrospective facial recognition (RFR) has contributed to differences in how forces use the technology. Similarly, the lack of a national learning framework has led to inconsistent approaches to training and continuing professional development (CPD) across forces. This risks creating greater differences across forces in capability and practice.

During our inspection, we found that forces didn't always provide appropriate training to personnel who used RFR operationally. This included investigators.

We were surprised by this finding, given the importance of the decisions made using RFR results. If personnel don't understand the technology's limitations, they may place too much weight on a potential match, fail to carry out appropriate enquiries to check the results or use the results inappropriately when making operational decisions. This increases the risk of identifying the wrong suspect, inappropriate executive action and a loss of public confidence in the police use of facial recognition technology.

Often RFR searches are carried out by less experienced investigators, usually in relation to volume crime offences. While some guidance and training on RFR exists, it is primarily aimed at Police National Database (PND) operators rather than investigators.

The College of Policing hasn't published APP guidance on RFR. It also told us that RFR wasn't included in initial police training or investigator training programmes.

Officers and staff who use RFR need better training and development

We found that national training focused on PND users. It involves a five-day training course aimed at new PND users, which includes a single session on RFR. This session focuses on how users submit images for RFR searches. It doesn't provide guidance to investigators on how to assess, interpret and use RFR results in an investigation.

We noted that the College of Policing has produced a PND facial search user guide. The guide provides advice to PND users on how to plan and carry out RFR searches on the PND. It explains the purpose of facial searching and includes examples of good practice that illustrate the potential benefits of using RFR. But the guide is intended for PND users who carry out searches. It offers limited guidance for investigators who request searches and use the results in their investigations.

Some forces have developed their own training for RFR operators

RFR operators are PND-trained officers and staff who submit probe images on behalf of investigators. We found that the availability of CPD opportunities for these users varied between forces. Some told us that their forces provided structured programmes to maintain and develop their expertise. Others told us that they relied primarily on updates to national guidance and practice, such as through email distribution groups for PND users or the College of Policing's Knowledge Hub.

Gwent Police and South Wales Police share an RFR system. Personnel who use this system must complete an annual CPD portfolio to maintain their accreditation. If they don't comply with this requirement, the forces remove their accreditation and require them to complete refresher training before reinstating it.

Some of the forces we inspected had developed additional training for personnel who carry out RFR searches. For example, the Metropolitan Police Service has 40 trainers who provide instruction to RFR users on using the system. At the time of our inspection, it told us that it had trained approximately 1,000 personnel to use its RFR system.

The National Crime Agency has worked with Liverpool John Moores University to train some of its personnel in comparing probe images with potential matches. This training aims to improve how personnel compare RFR results. It uses a structured, five-step comparison process based on scientific principles. At the time of our inspection, the National Crime Agency told us that 22 personnel in specialist roles had completed this training.

While we didn't assess the effect of this training on outcomes, we found that the forces that had invested in additional training generally appeared to have more structured arrangements for RFR use and governance.

A Home Office survey of PND facial search users produced mixed results

In 2026, the Home Office carried out a survey of PND facial search users. It analysed 779 user responses from across all 43 police forces in England and Wales, the National Crime Agency and British Transport Police. The Home Office shared its survey findings with us.

It found that 96 percent of frequent users agreed or strongly agreed that they had the necessary skills to use PND facial search, which is significantly higher than 85 percent of infrequent users. And 73 percent of frequent users agreed or strongly agreed that they felt confident that the appropriate safeguards were in place to make sure PND facial searches were unbiased, which is significantly higher than 65 percent of infrequent users.

It found that 78 percent of respondents said that they always or usually considered accuracy when assessing a potential match, and 18 percent reported that they sometimes considered accuracy. A small number rarely did, never did or didn't know.

Respondents to the Home Office PND survey were less clear about the evidential value of a PND facial search match. Around one third of respondents (34 percent) either incorrectly believed or weren't sure whether a PND facial search match meets the evidential requirement for recognition under Code D 2023 of the Police and Criminal Evidence Act 1984. But 66 percent of respondents correctly recognised that a match doesn't meet this evidential threshold.

In the survey, 86 percent of respondents reported having received training (51 percent reported this training was more than a year ago, and 35 percent reported it had taken place within the last year). But 14 percent of respondents didn't recall having received any training. Of the 86 percent of respondents who reported having received training:

- 89 percent reported it covered how to submit images;
- 60 percent reported it covered understanding the results of RFR;
- 49 percent reported it covered the risks and limitations of RFR; and
- 45 percent reported it covered preparing images for searching.

These results appear mixed. Given that the survey targeted PND licence holders, we would have expected the survey's findings to reflect higher levels of training and confidence.

We expected that more survey respondents would report having received training on how to interpret RFR results and understand their appropriate use. These are important aspects of the process, especially for personnel who make or support operational decisions based on RFR searches.

Recommendation 11

By 30 June 2027, the College of Policing should review the content and provision of training and continuing professional development for Police National Database users who carry out retrospective facial recognition (RFR) searches.

The College of Policing should make sure personnel who use or support the use of RFR receive up-to-date training on:

- image quality and preparation;
- interpreting RFR search results;
- the limitations of facial recognition technology;
- bias, ethics and data protection considerations; and
- the appropriate use of RFR in investigations.

RFR training for investigators is insufficient

Training only PND licence holders isn't sufficient because it doesn't provide forces with the capability to use RFR effectively. Forces must make sure that all personnel who are likely to use RFR understand how the system operates. Investigators must also understand that RFR results provide intelligence only and that they must carry out further enquiries before taking any action.

We found limited evidence of any training for investigators. Some personnel told us that they had received little or no training, CPD or updates on RFR. For example, some officers in a focus group told us they had a limited understanding of what a match meant and whether it was enough to justify arresting the suspect.

In some forces, we found that guidance documents were available on force IT systems. But some personnel told us that they were unaware of this guidance. In two forces, some personnel told us that they relied on informal word-of-mouth methods to learn how to use RFR.

We did find some examples of PND licence holders providing awareness training and CPD to frontline personnel. These included:

- RFR sessions in relevant training courses;
- RFR roadshows for frontline personnel; and
- training videos sent to users and made available on force intranets.

While we welcomed these examples, they weren't sufficiently widespread.

Innovative practice: Cheshire Constabulary trains investigators to use retrospective facial recognition

Cheshire Constabulary uses a centralised team to carry out its retrospective facial recognition (RFR) searches. Personnel in this team complete a five-day online facial recognition training course provided by the US Federal Bureau of Investigation. The course strengthens their understanding of facial features and provides guidance on techniques to enhance image quality for search purposes. The constabulary also carries out ongoing proficiency testing to assess their competence in RFR searches.

Personnel from this team provide training and support to improve understanding of RFR across the constabulary and help make sure officers and staff use the technology consistently and appropriately. This includes material on the constabulary intranet, training videos and posters with QR code links to RFR resources.

The constabulary effectively shares guidance on submitting images for RFR searches through its IT systems and regular constabulary communications, including topic-specific bulletins.

A national RFR training framework for investigators is needed

During our inspection, we were told about the importance of probe image quality to effective RFR searches. If investigators don't follow established standards for submitted images, the quality of search results may be affected. Factors such as cropping, image size and image orientation can influence search performance.

Importantly, any potential match from an RFR search provides intelligence rather than evidence. All investigators must understand this and carry out appropriate further enquiries before taking any action. Each investigation is different, so forces can't define every step that investigators should take after an RFR match. But investigators must take all reasonable steps to avoid wrongful arrest. Most frontline staff we spoke to understood this, but some staff didn't display the same depth of knowledge.

Supervisors must monitor the progress of investigations that their teams manage. Less experienced personnel are likely to carry out most RFR searches, so effective supervision is essential.

The College of Policing has published APP guidance that sets out quality standards for recovering and processing images from CCTV and other digital media. Investigators who submit images for RFR searches must follow these standards.

But the College of Policing told us it didn't consider that separate APP guidance for RFR was necessary. Instead, it supports integrating guidance on RFR into existing investigator training programmes, including initial investigator training and the professionalising investigation programme.

We agree with this pragmatic approach. It would make this guidance more accessible to RFR users and easier to update in response to developments in RFR technology and practice. But we believe that training should address several important areas, specifically:

- inconsistencies in users' understanding of the importance of image quality;
- how to interpret the results of RFR searches; and
- the action RFR users should take after a potential match.

Recommendation 12

By 30 June 2027, the College of Policing should make sure guidance on retrospective facial recognition (RFR) is included in existing national investigator training programmes. This should include guidance on:

- identifying and recovering material suitable for RFR searches;
- preparing and submitting images for RFR searches;
- interpreting RFR search results;
- the requirement to corroborate potential matches through further enquiries;
- supervisory responsibilities; and
- continuing professional development and updates on emerging good practice.

Recommendation 13

By 31 December 2027, chief constables and the director general of the National Crime Agency should make sure all officers and relevant staff involved in using retrospective facial recognition (RFR) receive mandatory training, supported by ongoing continuing professional development. This training should cover:

- identifying and recovering material suitable for RFR searches;
- preparing and submitting images for RFR searches;
- interpreting RFR search results;
- the requirement to corroborate potential matches through further enquiries;
- supervisory responsibilities; and
- continuing professional development and updates on emerging good practice.

How well do investigators understand and follow the required investigative processes after identifying a potential facial recognition match?

Most retrospective facial recognition (RFR) searches on the Police National Database (PND) relate to volume crime. Less experienced investigators usually lead these investigations. The more experienced detectives we spoke to generally understood the procedures they should follow, but this wasn't always the case with less experienced investigators.

For example, some investigators didn't understand that potential RFR matches provided intelligence rather than evidence and must be corroborated before officers took further action. In one force, more than half of the participants in a focus group didn't know that RFR results were for intelligence purposes only. We noted that the force involved didn't train its investigators in the use of RFR. We have commented on this in the chapter 'How well do police forces and the National Crime Agency train their investigators to use retrospective facial recognition in investigations?'

This lack of understanding is deeply concerning. If forces misuse facial recognition technology or arrest people without carrying out appropriate checks and corroborating enquiries, they will undermine public confidence and trust in the technology and its use by the police.

Forces are using RFR effectively to solve crimes

We found many examples of investigators using RFR to solve crime.

In Cheshire Constabulary, officers responded to a report of a knife-point robbery in Crewe. They carried out an urgent RFR search within 10 minutes and identified a suspect. Officers then reviewed CCTV footage from Crewe railway station as they believed the suspect had travelled to London. This footage showed the suspect boarding a train. British Transport Police officers stopped the train, arrested the suspect and recovered the stolen property.

In Dorset Police, officers obtained CCTV images after a violent assault. The suspects wore balaclavas to conceal their identities, but officers identified a facial tattoo on one offender. Officers carried out social media enquiries and identified images of a person of interest and known associates. They submitted these images for RFR searches, which generated potential matches. Officers arrested two men because of these enquiries. The court later convicted both men of aggravated burglary.

In Gwent Police, officers investigated a reported sexual offence on a bus. They obtained CCTV records of the incident, which included 64 pages of images and video stills. The investigating officer identified a suitable image for submission to RFR. The RFR search generated a potential match. Officers then gathered supporting evidence and arrested the suspect.

Investigators don't always carry out additional checks before making arrests

During our inspection, we spoke to a range of investigators, including detectives with many years of service and inexperienced frontline personnel investigating volume crimes. Many understood the limitations of RFR. But others didn't, particularly frontline investigators.

Some officers told us that high demand on response teams could reduce opportunities to carry out further enquiries before acting on potential RFR matches. In another force, some officers told us that managers had, at times, encouraged them to progress investigations quickly after positive RFR matches.

In one force, after carrying out an RFR search, investigators circulated details of a suspect on the Police National Computer for arrest in connection with a series of shoplifting offences. Officers arrested the suspect in another force area and transferred him to the investigating force. Investigators subsequently established that the suspect didn't match the image of the offender. The force determined that investigating officers hadn't carried out any further enquiries before circulating the suspect for arrest. The force told us that it had since improved processes within its central RFR team to prevent a similar incident in the future. These changes included greater scrutiny of positive matches involving older PND images, additional corroborative enquiries and supervisory oversight. We welcome the steps the force has taken.

Forces have different approaches to using RFR and don't always have centralised RFR teams and clear operating procedures

Forces must make sure only trained users carry out RFR searches on the PND and that they comply with the PND manual of guidance. But we found notable differences in how forces used this capability. These differences included the use of centralised RFR teams and the presence of clear operating procedures.

Centralised RFR teams are more efficient and effective

During our inspection, we found that some forces used centralised teams to carry out their RFR searches. But we found that other forces took a less structured approach, with investigators identifying trained PND users to carry out searches on their behalf.

Overall, we found that the forces using centralised teams to carry out their RFR searches exercised greater control over the process. Personnel in these teams were generally more experienced and had a clearer understanding of what was required.

This provided several benefits. For example:

- personnel on these teams received better training;
- the validity of RFR search requests was checked;
- better quality images were submitted for searching;
- personnel had improved understanding of search results, which, in some cases, helped them to carry out further enquiries before returning results to investigators; and
- investigators received results that included clear explanations that they represented intelligence only and set out any further work required.

This is consistent with the findings from the Home Office survey of PND facial search users. Frequent users were more confident and more likely to have received recent training than infrequent users.

In contrast, we found forces that didn't have centralised RFR teams were more likely to have weaker processes. For example:

- PND licence holders who didn't work in a centralised RFR team carried out RFR searches less often;
- results were returned to investigators without an explanation of their limitations; and
- investigators were less likely to understand that potential matches were for intelligence purposes only.

These forces were also generally lower users of RFR.

We consider that investigators in forces with a centralised RFR team receive better support than those in forces without one. During our inspection, we found that centralised teams generally had stronger governance, greater expertise and more consistent processes for the use of RFR.

Recommendation 14

By 31 December 2027, chief constables and the director general of the National Crime Agency should review the retrospective facial recognition search system. They should consider either:

- establishing centralised teams in their organisations to carry out their retrospective facial recognition searches; or
- giving responsibility for carrying out their retrospective facial recognition searches to established teams such as force intelligence.

Recommendation 15

By 31 December 2027, the National Police Chiefs' Council should consider removing the facility for carrying out retrospective facial recognition searches from personnel who aren't part of a centralised or established retrospective facial recognition team.

Not all forces have clear operating procedures that govern the use of RFR

Three of the forces we visited had operating procedures that set out how personnel should carry out RFR searches and respond to potential matches. For example, these procedures require personnel to:

- return results using an online force template that includes guidance on handling the information;
- record results on the investigation log within the force crime recording system and clearly state that they are for intelligence purposes only;
- attach a document to the crime record that includes both the submitted image and the PND image; and
- complete, or consider completing, specified corroborative enquiries before taking any further action.

One force had produced a draft operating procedure that was waiting for chief officer approval. But three forces had no guidance or processes for RFR. The absence of clear guidance limits consistency and may lead to a poor understanding of RFR processes, including the distinction between intelligence and evidential use. For example, in one force without local RFR guidance, we were told about a case in which supervisors directed officers to arrest a suspect based solely on a potential RFR match that wasn't supported by additional enquiries. Investigators in the same force also told us that they had received no training on the use of RFR.

During our inspection, we considered whether forces should require senior officer approval before carrying out RFR searches. We concluded that such a requirement wouldn't be appropriate. It could introduce unnecessary bureaucracy and discourage investigators from using RFR where it may assist an investigation.

But we recognise that stronger safeguards may be appropriate when forces use more intrusive facial recognition capabilities or search image datasets beyond those routinely held by policing. For example, in some serious investigations, the police may want to search images held by HM Passport Office to help identify unknown suspects when other investigative opportunities have been exhausted. In these circumstances, it may be appropriate to require additional authorisation and to restrict use to the investigation of serious crime.

Forces should include use of RFR in their investigation policies and procedures

Not all the forces we visited had investigative policies and guidance that covered the use of RFR. This may make it harder for forces to make sure investigators use RFR consistently and appropriately.

Forces should establish policies and procedures that govern the use of RFR. As a minimum, these should:

- make clear that RFR results provide intelligence rather than evidence;
- require investigators to record decisions and actions arising from potential RFR matches on force crime recording systems; and
- require supervisors to review and endorse decisions relating to RFR results.

These measures should help forces use RFR more consistently, improve oversight and reduce the risk of officers acting without enough supporting evidence.

Force investigation logs don't include enough information about the use of RFR

Police forces in England and Wales use a range of systems to record crime and manage investigations. During our inspection, we considered reviewing a sample of investigations in each force. We intended to include cases where forces had used RFR as well as cases where they could have used it but didn't.

But, partly because of limited management information, we found no reliable way to identify cases in which forces had possibly missed opportunities to use RFR. As a result, we couldn't assess how consistently forces considered or used RFR as part of their investigations. The same limitations also prevent forces from assessing whether they are making full use of RFR and from providing effective audit, scrutiny and oversight of its use.

In each force we visited, we asked to see some investigations that involved the use of RFR. We also discussed RFR and checked crime files during reality testing. We examined what investigators and supervisors had recorded on investigation logs.

In British Transport Police, we found that supervisors had an active role in decision-making after a potential match. Investigation plans set out the lines of enquiry and the corroboration required before officers took further action. Supervisors should review RFR reports during case reviews and make sure officers consider and act on them appropriately.

In one force, we examined two investigations that involved a potential match from an RFR search. We found no entries on the force crime recording system that logged any additional checks or enquiries the investigator had carried out after receiving the RFR result.

In our 2025 inspection on how effectively the police investigate crime, we found that some forces didn't use investigation plans effectively. As a result, we recommended:

> "By 30 September 2025, chief constables should make sure their force has a clear policy relating to investigation plans. They should make sure their force communicates this policy to officers and staff."

As at 1 August 2026, 22 of the 43 forces in England and Wales had completed this recommendation.

Investigators should carry out further enquiries to corroborate a potential RFR match before taking any action. Even when personnel understand this requirement, applying it involves judgment. Less experienced investigators may not fully understand what is required and may take a different approach from more experienced colleagues.

For these reasons, forces must make sure investigators clearly record their decisions and actions on investigation logs. This should include instances where investigators decide not to take any further action after a potential match from an RFR search. Supervisors must review this activity and make sure investigators comply with force policy.

Clear audit trails are important because they help forces understand how investigators use RFR results. They provide assurance that officers make decisions based on appropriate enquiries and corroborating information.

During our reality testing, we found that investigators and supervisors didn't consistently record the use of RFR in investigation plans, enquiry logs or supervisory reviews. In many cases, there was no clear record of whether RFR had been considered, used or discounted as an investigative opportunity or of any rationale for subsequent decisions. This made it difficult to understand how RFR had informed investigations and limited forces' ability to provide effective oversight and scrutiny of its use.

As a result of our inspection, we concluded that:

- supervisors and investigators should record the use of RFR in investigation plans;
- if a potential match is identified, investigators should record further corroborative enquiries on investigation logs;
- supervisors should include updates on RFR activity in their review entries;
- when closing an investigation, officers should record whether they used RFR, the outcome or the reasons for not using it; and
- supervisors should confirm that officers recorded whether they used RFR, the outcome or the reasons for not using RFR before authorising investigation closure.

Recommendation 16

By 30 June 2027, chief constables and the director general of the National Crime Agency should make sure force and National Crime Agency investigation policies and procedures include guidance on using retrospective facial recognition (RFR).

As a minimum, these policies should:

- make clear that RFR results provide intelligence rather than evidence;
- require investigators to record decisions and actions arising from RFR searches; and
- set out supervisory responsibilities for reviewing the use of RFR and the action taken after potential matches.

November 2026 | © HMICFRS 2026

hmicfrs.justiceinspectorates.gov.uk