

A report into the effectiveness of integrity arrangements in the Metropolitan Police Service

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 the public would ask and publish the answers in an accessible form. We use our expertise to interpret the evidence and make recommendations for improvement.

Contents

About us	i
Foreword	1
Introduction	3
Vetting police officers and staff	4
Vetting authorised professional practice	4
Force vetting arrangements	4
Compliance with vetting authorised professional practice	5
Capability and capacity	5
Demand and workload	6
Current vetting of the workforce	7
Designated posts	8
Transferees	8
Change of circumstances	9
Non-police personnel vetting	10
Vetting reviews	10
Vetting decisions	11
Vetting file review	12
Vetting appeals	15
Quality assurance	15
Disproportionality	16
Upholding the standards of professional behaviour	17
Promoting the standards of professional behaviour and integrating organisational learning within the workforce	17
Handling and investigating public complaints, conduct matters and other potential breaches of the standards of professional behaviour	21
Holding police officers and staff accountable for their behaviour	42

Tackling potential corruption	46
Preventing misuse of IT systems	46
Tackling potential corruption	51

Foreword

In our most recent inspection of the Metropolitan Police Service, we identified some improvements in how it manages force culture and poor behaviour.

We found that in some areas, the force had been proactive and committed in its efforts to remove people who shouldn't be working in policing. This included pursuing a case that, since our inspection, has shaped national policy and led the way for forces to be able to consider dismissal of [police personnel](#) whose vetting clearance has been removed.

I also recognise the robust stance taken by the commissioner on the vetting of those wanting to join the force. His approach, in some cases, deviates from national guidance, but it does reflect the local challenges that the force faces.

We note the historical issues and operational context of the force. We acknowledge its considerable investment in its integrity arrangements, which was demonstrated by the transformation that was underway at the time of our inspection. But the force needs to do more in all three areas that we covered – vetting, professional standards and anti-corruption.

In vetting, I am pleased that the force has enough capacity to manage demand. And personnel in the [force vetting unit](#) are well trained by the vetting academy. However, the force doesn't yet have any process to review the quality of vetting decisions. And its list of [designated posts](#) isn't accurate. At the time of our inspection, it had no plans to review the list to make sure that personnel who hold these posts are properly vetted. The force should address these risks.

We also found that the force didn't have effective oversight of contractors working on police sites and didn't properly manage their vetting.

It is clear that the force has made significant efforts to improve workforce culture and promote the expected standards of professional behaviour. It has provided force-wide training on values and standards and uses a variety of methods to reinforce those messages.

I am pleased that our case reviews of public complaints and internal [conduct matters](#) found that decision-making was mostly both reasonable and proportionate. The force's [directorate of professional standards](#) has also established a national [appropriate authority](#) forum to share learning and best practice and to promote improvements.

However, we found that the initial handling of public complaints wasn't always in line with statutory guidance. The force didn't always tell complainants that they had a [right to have the outcome of their complaint reviewed](#). And it could improve its management and supervision of complaint and conduct investigations.

In terms of the force's anti-corruption arrangements, it was apparent that teams in the [anti-corruption and abuse command](#) were working well together to make sure that the force has experienced and comprehensive in-house [covert](#) capabilities.

We found that the commissioner recognised the importance of monitoring and auditing force IT systems and had invested in technology to support this. However, some personnel still weren't downloading and activating an application that allows the force to monitor their online activity.

We also found that [intelligence](#) and investigations relating to potential corruption were stored on a wide range of disparate IT systems. This makes it difficult for the force to research and analyse information across the systems. The force has made efforts to mitigate this risk with a search tool, but it doesn't cover all the relevant systems.

The Metropolitan Police Service is going through a significant transformation in its directorate of professional standards. We saw that it was continuously promoting improvements, and we look forward to being able to comment on the results of those changes in our next inspection.

I have been, and will remain, in regular contact with the commissioner and his team.

My report sets out the detailed findings of this inspection.



Lee Freeman KPM

His Majesty's Inspector of Constabulary

Introduction

Background

When serving [police officers](#) and [police staff](#) are involved in [misconduct](#) or carry out criminal acts, it seriously reduces public trust and confidence in the police. It means the public are less likely to feel that [police personnel](#) behave in a lawful, ethical and fair manner. Public interest in police behaviour is high. The government and police service are increasing their focus on improving vetting, challenging misconduct and tackling corruption. We acknowledge this is increasing the demand placed on teams in [force vetting units](#), [professional standards departments](#) and [counter-corruption units](#). But this work is essential to making sure the right people join the police service, and all officers and staff continue to work with integrity.

Our judgments

We assessed the effectiveness of the Metropolitan Police Service's vetting, professional standards and anti-corruption arrangements. At the end of our inspection, we briefed senior officers about our findings.

Our judgments are as follows:

Area	Grade
Vetting police officers and staff	Requires improvement
Upholding the standards of professional behaviour	Requires improvement
Tackling potential corruption	Requires improvement

In the rest of this report, we set out our detailed findings about things the force is doing well and where it should improve.

Terminology in this report

Our report contains references to, among other things, 'national' definitions, priorities, policies, systems, responsibilities and processes.

In some instances, 'national' means applying to England or Wales, or England and Wales. In others, it means applying to England, Wales and Scotland, or the whole of the United Kingdom.

Vetting police officers and staff

Requires improvement

The Metropolitan Police Service requires improvement at vetting its [police officers](#) and [staff](#).

Area for improvement: The force should make sure that all non-police personnel have the correct vetting clearance to carry out their role

The force should complete all relevant checks before granting non-police personnel access to police premises or systems.

Vetting authorised professional practice

In 2025, the [College of Policing](#) published the updated [authorised professional practice \(APP\)](#) on vetting. The APP explains the role of vetting in assessing the suitability of people to serve as a police officer, [special constable](#) or member of staff. And it explains the vetting process for non-police personnel (contractors, volunteers and people who work in organisations that share police premises). For each clearance level, it sets out the minimum checks that should be completed on the applicant, their family and associates. It also gives forces examples of strategies that they could use to mitigate any risks inherent in granting vetting clearance to applicants about whom the force may hold [adverse information](#) or other concerns.

Force vetting arrangements

At the time our inspection, the [force vetting unit \(FVU\)](#) was using a bespoke vetting IT system, which was introduced in 2022. The HR department used a separate IT system, and there was no integration between the two systems. The force told us that the absence of integration, coupled with a lack of interaction between FVU staff and HR, caused problems in processing vetting applications. For example, HR didn't always inform the FVU about internal moves or promotions. This meant that data in the bespoke vetting IT system was inaccurate. To address this, FVU staff told us that they had to manually compare vetting IT system data with HR system data. In addition, FVU staff told us that the vetting IT system was slow and sometimes lost their work.

The force recognised that its vetting IT system was inefficient and, at the time of our inspection, had procured a new system. It had a comprehensive plan to manage its introduction and anticipated that FVU staff would be using the new system by March 2026.

Compliance with vetting authorised professional practice

FVUs should comply with the vetting APP. The vetting APP allows forces to deviate but requires any such decision to have a robust rationale, which must be supported at [chief officer](#) level. Any deviations should be readily identifiable and accessible for any audit, including, for example, by our inspectors or the College of Policing.

At the time of our inspection, the force was deviating from the vetting APP in several ways. It wasn't:

- re-vetting staff who rejoined the force within 60 days of leaving if they had over 12 months remaining before their original vetting clearance expired;
- re-vetting people prior to a secondment posting;
- clearing [authorised firearms officers](#) to [management vetting](#) level; and
- carrying out vetting reviews on [personnel](#) moves within the organisation.

The force was exceeding the requirements of the vetting APP by:

- completing [Disclosure and Barring Service](#) checks on some people when not required by the APP;
- using full non-police personnel vetting (NPPV) level 2 when a lower level of vetting would be sufficient;
- lowering renewal periods for national security clearance to match management vetting clearance (renewal after seven years instead of ten);
- using a vetting decision-making framework (which we discuss further in [the 'Vetting decisions' section](#)); and
- completing counter-terrorism checks on all NPPV level 1 clearances.

A chief officer has supported these deviations, and the force vetting policy provides the rationale for each of them. None of the deviations listed are likely to create any unnecessary and prolonged risks to the public.

Although the force can deviate from the APP, it should continue to review these deviations.

Capability and capacity

If fully staffed, the FVU would have enough resources to meet the demand it faces. But, at the time of our inspection, it had 28 vacancies. The force had recently approved the recruitment of ten staff, but these were temporary due to budgetary constraints.

A deputy assistant commissioner has overall command of the FVU. The force told us that the unit comprised:

- a director of vetting;
- a head of vetting;
- three senior executive managers (vetting, operations and assurance);
- 11 production managers (team leaders);
- 38 senior vetting officers (SVOs) responsible for vetting decisions; and
- 131 vetting officers responsible for carrying out vetting checks and, in each case, making a recommendation whether to grant vetting clearance or not.

Staff throughout the FVU told us that the deputy assistant commissioner provided them with a good level of support. Senior managers provide a monthly briefing to all FVU staff to keep them up to date with issues affecting the unit. During our inspection, we observed a senior manager briefing. It covered performance data, recruitment of staff into the FVU, police vetting regulations and any changes to vetting processes.

The FVU has dedicated four experienced SVOs to training staff. The force has a well-structured five-week training programme for newly appointed vetting officers. On completion, the vetting officers progress to the FVU training academy. Training academy staff mentor the vetting officers, quality assure their work throughout the process and provide feedback. Once the force assesses a vetting officer as competent, they join one of the FVU teams. The training programme takes approximately 21 weeks.

The four SVOs continue to support the development of FVU staff. For example, they help with the introduction of any changes to vetting procedures. And they have provided specific training to FVU staff to help them understand the new vetting APP.

It is encouraging to see that the force provides learning and development to everyone who has responsibility for vetting the workforce. This makes sure they are all suitably trained for their roles.

Demand and workload

The FVU and the recruitment team within Met business services work together to predict demand. Sponsors from departments with high levels of recruitment must provide 12 months of anticipated recruitment data. Analysis of this data and monthly meetings with sponsors from these departments help to forecast future vetting demand. This helps the FVU to match its available resources to meet that demand.

To further assist with managing vetting demand, the FVU has a vetting unit support services section. This allows vetting officers to focus on processing applications. Support services include:

- customer service;

- liaison with other forces and departments;
- vetting renewal extensions;
- maintaining the vetting mailbox;
- general enquires; and
- uploading change of circumstances notifications to the vetting IT system.

The FVU has developed a robust performance management framework. This allows FVU managers to monitor individual staff performance. It also helps managers to understand the FVU's workload and check the progress of applications for vetting clearance.

The force told us that the number of vetting applications awaiting progression was steadily reducing. At the time of our inspection, the force had 8,121 vetting applications that it hadn't started. Of these, there were 4,134 notifications of change of circumstances, the oldest of which was from August 2023.

In August 2025, the force introduced a new process for managing notifications of change of circumstances, which is helping. We explain this further in [the 'Change of circumstances' section](#). Based on the size of the force and the resources available in the FVU, this is a challenging but manageable workload.

Current vetting of the workforce

The Metropolitan Police Service told us that as at 15 September 2025, it had a total of 47,284 police officers, special constables, police staff and [police community support officers](#).

The force told us that there were 182 people without the correct level of vetting for their role. Of these, 129 police officers, 40 police staff, 12 special constables and a police community support officer had expired clearances.

The force vetting manager confirmed that the unit knew who all the people were. At the time of our inspection, vetting staff were in the process of contacting them.

Before our inspection, operational command units and [basic command units](#) had to initiate vetting renewal applications for personnel in their command. The force told us that this system wasn't effective. The FVU often received vetting renewal applications too late to process before the vetting clearance expired. When this occurred, to allow time to process the renewal application, the FVU had to extend the applicant's vetting clearance by three to six months.

To manage the vetting renewal process more effectively, the force has transferred responsibility for renewals to the FVU. The FVU is now managing and co-ordinating all the force's vetting clearance renewals.

During our inspection, we spoke to personnel about their vetting status. Most of them were aware of their vetting level.

Designated posts

Some police roles have access to more sensitive information and require a higher level of vetting known as management vetting. When deciding if a role needs this additional consideration, forces should also review the extent to which it requires working with [vulnerable people](#). The vetting APP states that forces should keep a record of all roles requiring management vetting or additional considerations on a [designated posts](#) list.

At the time of our inspection, the Metropolitan Police Service didn't have an accurate designated posts list. The FVU told us that 12 months prior to our inspection, the force carried out a review of every post, and the FVU produced an updated designated posts list. But since then, the force has carried out a further review of posts as part of its transformation programme. As a result, the number of posts requiring management vetting increased from 5,595 to 9,177. Therefore, the designated posts list produced by the FVU no longer accurately reflected the force's current designated posts.

This means that there are people in designated posts without the correct level of vetting. The force needs to carry out a further review to make sure that all the newly designated posts require management vetting. The FVU will then need to check that officers and staff in those posts have the appropriate level of vetting. At the time of our inspection, the force hadn't carried out such a review.

We reviewed a selection of vetting files for people with management vetting clearance. In each case, the FVU had completed all the required checks.

Making sure that all designated post holders are vetted to the required level was recommendation 13 in [our 2022 national report 'An inspection of vetting, misconduct, and misogyny in the police service'](#).

Transferees

The vetting APP states that all police personnel transferring between forces should complete a new vetting application form. Police vetting clearance is required before the transfer is confirmed.

The Metropolitan Police Service's FVU requests a [professional standards department \(PSD\)](#) complaint and conduct history, as well as any [anti-corruption unit intelligence](#), from all forces in which the person has previously served. And, where required, it will make further enquiries directly with the force. The force told us that in the 12-month period to 15 September 2025, it had vetted and recruited 39 transferees.

When a transferee has any adverse information on their professional standards history, SVOs will make a recommendation about their suitability to transfer to the force. In most cases, they do this without consulting the DPS, the force's professional standards department. On rare occasions, they consult the DPS so that the force can make further enquiries about the person. If the SVO decides to grant vetting clearance to a transferee, they send an intelligence report to the DPS. SVOs aren't made aware of any subsequent action taken by the DPS to mitigate any potential risks identified.

Where the Metropolitan Police Service refuses vetting for a transferee, it informs the originating force and explains the reason for the refusal.

Where an officer wanting to transfer from the Metropolitan Police Service fails vetting in the force to which they are applying, the FVU carries out a vetting review taking account of the reason for refusal. The force considers implementing risk mitigation measures if required.

Change of circumstances

The force has taken steps to improve the workforce's awareness of the obligation to report any change in personal circumstances. The DPS provides regular messaging, training and briefings to the workforce. The requirement to update vetting is also included in the force's [annual integrity review](#). At the time of our inspection in November 2025, the force told us that 81 percent of the workforce had completed their review within the preceding 12 months. We found that personnel generally had a good understanding of when to report changes in their personal circumstances.

The force requires personnel to declare a change in circumstances by updating their record on the force's vetting system or by sending a completed form directly to the FVU. When a member of the workforce reports a change of circumstances, FVU staff carry out enquiries to identify risks. And they decide if the reported change affects the person's vetting status.

When personnel report that they have changed their address within the previous 12 months, the FVU only checks the electoral roll rather than researching any available intelligence relating to the address and occupants. By not completing full intelligence checks in these cases, the FVU may miss adverse information. This means that the FVU isn't considering potential risks when processing the change of circumstances notification.

The FVU told us that in 2023, it received 4,522 change of circumstances notifications, and in 2024, it received 8,589. In July 2025, the force provided us with vetting data showing that 4,134 of these notifications were awaiting action by a vetting officer. The oldest was dated August 2023.

At the time of our inspection in November 2025, the force had received 5,006 notifications. It told us that it had revised its process for managing these notifications. We found that the process was already having a positive effect.

The force told us that it had reduced the number of outstanding notifications to 2,600. FVU staff had carried out an initial assessment of each outstanding notification and given it a red, amber, green (RAG) rating. This meant that FVU staff were working on the notifications that they had assessed as carrying the most risk first. For example, staff were prioritising declarations of significant financial issues so that the FVU could implement early intervention and risk mitigations if required.

The force should continue with its work to reduce the outstanding notifications so that it identifies any risks and considers appropriate risk mitigations.

Non-police personnel vetting

The Metropolitan Police Service grants non-police personnel vetting (NPPV) clearance to contractors, volunteers and people who work in organisations that share police premises. The force uses the [National Police Vetting Service](#) hosted by Warwickshire Police to vet some non-police personnel.

At the time of our inspection, the Metropolitan Police Service wasn't managing its NPPV process effectively.

The FVU relies on departments that have responsibility for contractors to manage all vetting applications and renewals. The FVU isn't always notified when contracts end or when people have left contracted companies. This means that these people may still have vetting clearance. And they may still have access to buildings and IT systems when the force should have removed it. The force told us that it recognised this risk and was planning to include contractor data on the HR system, which may help.

At the time of our inspection, the Metropolitan Police Service had 4,480 non-police personnel recorded on its vetting IT system. The FVU told us that it had 1,881 NPPV applications waiting to be processed. The oldest dated back to March 2024. But the force couldn't tell us with any degree of confidence how many contractors it employed and how many didn't have vetting clearance. This represents a significant risk for the force.

Vetting reviews

The vetting APP prescribes various circumstances when vetting clearances should be reviewed. This is to make sure that the person is still suitable to hold vetting clearance. Depending on the circumstances, it will be a full vetting review or one that focuses on the specific issues that have prompted the review (such as reviewing vetting clearance following a [misconduct](#) allegation).

Annual integrity and vetting review

At the time of our inspection, the Metropolitan Police Service didn't have a process for the workforce to complete an annual integrity and vetting review in line with the 2025 vetting APP. The force told us that it was working towards a suitable process and anticipated that it would introduce it in April 2026. The force told us that its existing annual integrity review included integrity questions, such as on business interests and changes of circumstances.

Post-misconduct review

The DPS informs the FVU of all [misconduct meeting](#) or [misconduct hearing](#) outcomes. The FVU told us that it complied with the APP requirement to review a person's vetting status if misconduct proceedings resulted in a reduction in rank, [written warning](#) or [final written warning](#).

The force told us that at the time of our inspection, the FVU had carried out 228 reviews over the previous three years. Of these, 101 resulted in vetting clearance being removed, downgraded or additional risk mitigation strategies being put in place.

Other reviews

The force will review a person's vetting clearance when a financial review is necessary as part of a risk mitigation strategy.

Vetting decisions

Vetting officers are responsible for carrying out relevant vetting checks. They make a recommendation in each case. The SVO is responsible for making the final vetting decision.

During our inspection, we found that vetting decision-makers consistently used a template to help them make decisions supported by clear rationales. FVU staff refer to the vetting APP. They also refer to a bespoke vetting decision-making framework that the force has developed to guide decision-making.

The framework mandates several offences, including [domestic abuse](#), [hate crime](#) or any sexual offences, where the force doesn't allow decision-makers to grant vetting clearance. This means that they can't consider risk mitigation in such cases.

In adopting the framework, the force has made a strategic decision to deviate from the APP. We recognise that the force has done this to rectify historical shortcomings in its vetting processes. And given the size of the FVU, the framework aims to promote consistency in vetting decision-making. We encourage the force to make sure that vetting decision-makers are applying the framework equally.

Vetting interviews

Forces can use vetting interviews in certain circumstances to clarify written responses in vetting applications. These interviews can be in person or by phone. But we found that the force's FVU didn't regularly use such interviews.

We reviewed 116 cases. We found 45 cases where an interview wasn't carried out when it would have been beneficial. Of these, 27 people were granted clearance and 18 were declined. Interviews are an opportunity to gather information and give more weight to decisions. We identified this as a national [area for improvement](#) in our 2022 national report on vetting, misconduct and misogyny.

We were encouraged to find that the force had made significant efforts to increase the FVU's interview capability. SVOs told us that they had received training to identify when an interview would be beneficial, improve consistency and give them confidence in what to expect in an interview. All staff in the vetting assurance unit have also completed a bespoke interview training course.

Risk mitigation

The Metropolitan Police Service uses risk mitigation to support its vetting decisions. For example, the FVU uses financial reviews as a risk mitigation measure when an applicant has undischarged debt or other financial difficulties. This is to make sure that the applicant complies with any conditions imposed and manages their financial situation appropriately.

The force told us that the integrity assurance unit in the anti-corruption and abuse command managed risk mitigation measures. These include those relating to [notifiable associations](#), which the force refers to as declarable associations. During our inspection, we found that in all cases, the FVU granted vetting clearance without consulting the integrity assurance unit. This meant that it might grant clearance where sufficient risk mitigation couldn't be put in place.

The force produces an annual counter-corruption [strategic threat assessment](#), which outlines the threats it faces. However, the anti-corruption and abuse command hasn't shared the assessment with vetting decision-makers as recommended by the APP. FVU staff told us that they considered the main corruption threats as part of the vetting decision-making framework.

Vetting file review

We reviewed 116 vetting files from the preceding three years with vetting specialists from other forces. These files related to police officers and staff who had previously committed criminal offences or about whom the force had identified other adverse information. The files included:

- initial [recruitment vetting](#) decisions, both granted and declined;
- vetting appeal decisions;

- transferee vetting decisions; and
- post-misconduct review decisions.

Initial recruitment vetting decisions, granted and declined

We reviewed 58 initial recruitment files. These related to clearances that the FVU had granted to new applicants and to internal applicants whose vetting the FVU had upgraded to management vetting. We agreed with 43 of the 58 decisions. They were well rationalised and referenced the APP.

In 9 of the remaining 15 decisions, the recorded rationale didn't consider all identified risks or relevant risk mitigation. For example, in one case, the vetting officer hadn't explored the risk presented by the applicant's associates. Instead, the FVU simply accepted the applicant's explanation that they no longer associated with the person.

In a further example, the FVU granted clearance to someone with financial difficulties but didn't implement any risk mitigation measures, such as regular financial reviews. The FVU shouldn't have granted vetting clearance without first considering all the risks more thoroughly.

In three of the remaining six cases, we disagreed with the decision to grant vetting clearance because the risk presented by the applicant was too great.

In one case, the FVU hadn't considered the applicant's recent involvement with the police when they refused to leave a property following an argument with their partner.

In a further case, the vetting decision didn't take into consideration the applicant's juvenile conviction for a violent offence. And it didn't take into account that they had applied three months after being suspended from their previous place of work following a dispute with their manager.

We also disagreed with the decision to grant higher level clearance to three members of the workforce. In one case, clearance was given without considering the applicant's recent arrest.

We reviewed 17 cases where the FVU had declined to grant clearance to new applicants or upgrade internal applicants. We agreed with 14 of the decisions. They were well rationalised and referenced the APP.

In each of the remaining two cases, before the FVU made the decision to decline the applicant's vetting clearance, it didn't explore in sufficient detail the risks the applicant posed.

We disagreed with one case where the FVU declined the application due to an isolated and historical investigation of very low value theft from an employer. The matter recorded against the applicant didn't result in a [caution](#) or conviction. In our view, the decision to decline clearance was disproportionate. In the remaining two cases, the FVU didn't consider available risk mitigation. FVU staff should have interviewed the applicants before making their final vetting decisions.

Vetting appeal decisions

During our inspection, we reviewed 14 vetting decisions where applicants had appealed the original decision not to grant vetting clearance.

We reviewed seven decisions where the applicant was granted vetting clearance after submitting an appeal. We agreed with two of these decisions.

We didn't agree with two decisions. In one case, the FVU didn't adequately explore the applicant's financial situation. In the other, it didn't mitigate significant risk posed by the applicant's family members.

In the remaining three cases, we found that the FVU hadn't carried out further enquires when they would have been useful to make an informed vetting decision. Instead, it based its decision solely on the information provided by the applicant.

We reviewed seven decisions where the applicant was declined vetting clearance after submitting an appeal. We agreed with five of these decisions.

In one of the two decisions we disagreed with, the FVU hadn't provided the applicant with the reasons for declining vetting clearance. This meant that the applicant hadn't been able to adequately challenge the decision at appeal.

In the second case, the appeal decision to decline the applicant's vetting application was disproportionate to the information recorded against the applicant's family member. And the decision-maker didn't consider potential risk mitigation measures.

Transferee vetting decisions

We reviewed 11 transferee cases where the FVU granted vetting clearance. We agreed with eight of these decisions. They were well rationalised and referenced the APP. In the remaining three, there were two cases where the recorded rationale didn't consider all relevant risks. In one, the FVU should have considered more thoroughly the risk presented by the criminal histories of the applicant's associates before making a decision. In the remaining case, we disagreed with the FVU's decision to grant vetting clearance because the risk presented by the applicant was too great.

We reviewed a further four transferee cases where the FVU declined vetting clearance. We found that the FVU didn't explore the risks the applicants presented in any significant detail in any of them.

Post-misconduct review decisions

During our inspection, we reviewed 12 post-misconduct review decisions. We agreed with 11 of them. In the remaining case, we agreed with the decision to withdraw clearance but found that the rationale wasn't clear enough. It would have benefitted from a more detailed explanation of why previous risk mitigation measures were no longer appropriate.

Vetting appeals

The legal process for vetting appeals for police officers is set out in the [Police \(Vetting\) Regulations 2025](#).

The right to appeal against the vetting decision is available to all external vetting applicants. The force vetting manager hears all the force's external appeals unless they were part of the original vetting refusal decision. In such cases, a different manager deals with the appeal.

The FVU told us that in 2023, it received 668 appeals against vetting decisions. It overturned 94 of these. In 2024, it received 649 and overturned 108. And at the time of our inspection in November 2025, it had received 241 appeals and overturned 39.

If the force vetting manager identifies that the applicant shouldn't have had their initial vetting clearance refused, they provide feedback to the original decision-maker.

Quality assurance

The Metropolitan Police Service doesn't have a formal quality assurance process for vetting decision-making. However, the quality control team in the FVU makes sure that vetting officers have carried out the correct checks. And the team also checks that vetting officers have referenced the vetting APP correctly. The FVU quality control team doesn't review the quality of the vetting decision.

At the time of our inspection, the force told us that it had recently started a quarterly vetting learning forum. Representatives from the Police Federation and Unison, a public service trade union, attend this forum. They provide feedback about the vetting decision but can't overturn it.

Attendees review 10 percent of cases from the previous three months where the SVO has disagreed with the vetting officer's recommendation. They also review 10 percent of cases where the force has upheld a vetting appeal. This is encouraging, but as only one forum meeting had taken place at the time of our inspection, it was too early for us to assess its effectiveness.

The vetting manager sometimes provides feedback to vetting officers after completing a vetting appeal. We would encourage the force to consider a wider [peer review](#) process across all vetting teams. It should also extend its quality control process to include quality assurance of vetting decision-making.

Introducing effective quality assurance for vetting decisions was recommendation 7 in our 2022 national report on vetting, misconduct and misogyny.

Disproportionality

The APP states there is a risk that vetting has a [disproportionate](#) impact on [under-represented groups](#). The APP also requires forces to monitor vetting applications, at all levels, against [protected characteristics](#). This is so forces can understand whether there is any disproportionate impact on particular groups. Where disproportionality is identified, forces must address this. The APP also states that forces should support and promote [positive action](#) for all under-represented groups in the police service.

The Metropolitan Police Service collects data on all nine protected characteristics (age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation). FVU business analysts carry out some analytical work to identify any disproportionality across all protected characteristics. They carry out more detailed analysis where there is enough data to make it meaningful. This analysis focuses on the outcomes of vetting applications from people who declare one or more of five protected characteristics (age, race, religion or belief, sex, and sexual orientation).

The force told us that between October 2023 and May 2024, the strategic insight unit examined disproportionality in all of the FVU's vetting decisions. The results revealed that the force was more likely to refuse vetting applications from Black, Asian and Mixed ethnic groups. In response, the force has commissioned the strategic insight unit to provide insight to better understand and reduce disproportionality in its vetting decision-making.

The FVU completes a report on disproportionality in vetting decisions on a six-monthly basis. It provides the report to the vetting oversight group and updates the force's '[London Race Action Plan](#)'.

At the time of our inspection, the FVU had limited interaction with people from under-represented groups who might be interested in joining the police service. We encourage the FVU to work with these groups. This may help to improve their confidence and understanding of the force's vetting arrangements.

Upholding the standards of professional behaviour

Requires improvement

The Metropolitan Police Service requires improvement at upholding the standards of professional behaviour and addressing potential breaches.

Promoting the standards of professional behaviour and integrating organisational learning within the workforce

Area for improvement: The force needs to improve its processes for collecting, sharing and evaluating organisational learning relating to the standards of professional behaviour

At the time of our inspection, the force didn't have a wholly effective process for collecting and sharing [organisational learning](#).

We found that the [directorate of professional standards](#):

- worked with the [Mayor's Office for Policing and Crime](#) to gather learning from upheld complaints reviews;
- had established a national [appropriate authority](#) forum to share learning and best practice and to lead improvements; and
- had consulted an [independent advisory group](#) to obtain feedback and learning in respect of a sample of its cases.

However, the force didn't have:

- an organisational learning board;
- an effective process for teams to highlight organisational learning; or
- an evaluation process to establish if the implementation of organisational learning had been effective.

This means that the identification and evaluation of relevant learning is inconsistent and incomplete. And there were no processes in place to track sharing and implementation of lessons learned.

Public confidence in the police depends on [police officers](#) and [staff](#) showing high standards of professional behaviour. It is important that everyone in a supervisory or managerial role leads by example in maintaining those standards. They should do this by challenging poor behaviour in others and showing the standards in their own behaviour. Each force should create and develop a culture of [organisational learning](#), which will help to raise the standards of professional behaviour in its workforce.

The standards of professional behaviour that police officers should follow are set out in two places. [Schedule 2 of the Police \(Conduct\) Regulations 2020](#) sets out the legally required standards. And the [College of Policing's Code of Ethics](#) lays out the professional standards expected from all police officers and staff. [The latest version of the Code of Ethics](#) was published in 2024.

Promoting high standards of professional behaviour

The Metropolitan Police Service uses a variety of methods to reinforce organisational learning and the standards of professional behaviour.

The force told us that it used a 'public health' approach to maintaining standards with a focus on prevention and early intervention. We found that the force provided initial training for the workforce on the expected standards and additional training for supervisors.

The directorate of professional standards (DPS), the force's professional standards department, provides training on [professional standards](#) during student officers' initial training. The force also includes standards of behaviour in the induction of new police staff. And the Code of Ethics is prominent in training overall.

The force gives additional professional standards training to police officer and staff supervisors through its leadership excellence programme. It provides the training on initial promotion and then further training targeted at [first-line](#), mid-level and senior leaders. Members of the workforce told us that these included practical scenarios, such as dealing with inappropriate comments of a sexual nature.

We found that the force didn't provide this training to those in temporary roles. This meant that it might not be adequately preparing acting sergeants to promote standards of behaviour in their teams or to identify and deal with potential breaches.

The force's internal communication working group raises awareness of the standards through various channels, including intranet posts. It also circulates videos and sends emails to the workforce. A former officer who was dismissed by the force for [gross misconduct](#) took part in one of these videos. We found that this personal contribution was an effective way to communicate the importance of maintaining standards of behaviour.

The force uses the intranet to circulate the [Independent Office for Police Conduct \(IOPC\)](#) 'Learning the Lessons' bulletin and the outcomes of [gross misconduct hearings](#). The DPS also circulated its first organisational learning newsletter in August 2025.

However, we found that many members of the workforce didn't feel they had time to access and read the information circulated by the force. [Police personnel](#) we spoke to had little recollection of DPS organisational learning or the IOPC bulletin. Some told us that they rushed through e-learning. This means that despite circulating communication and providing training on standards of behaviour, the force can't be confident that its workforce fully understands it.

In videos placed on the intranet, the [commissioner](#) has set out expectations in respect of standards of behaviour. And he reinforced the standards to all senior leaders at a 'leadership summit' following the BBC Panorama programme 'Undercover in the Police'. The programme broadcast evidence of racism, misogyny and some officers' inappropriate attitudes to use of force at a London police station.

The force followed up the summit by directing senior leaders to set out how they will promote professional standards and culture. The force will assess each leader's progress as part of their next performance development review.

In July 2023, the force introduced the '[New Met for London](#)' strategy, designed to promote its values and standards. This included providing training to the entire workforce. At the time of our inspection, phase 1 of this training had been completed by 33,000 members of the workforce. And the force was rolling out phase 2 training to 23,000 officers and staff who work directly with [victims](#). This is a significant positive initiative.

The DPS raises awareness of standards by attending some development days for officers and staff. And its [domestic abuse](#) and sexual offences team (DASO) provides training on police-perpetrated domestic abuse and sexual offences. However, members of the workforce told us that this wasn't provided consistently across the force. The DPS told us that resourcing issues affected the DASO team's capacity to provide this training to the workforce.

The workforce's understanding of the expected standards of professional behaviour

The Metropolitan Police Service checks that the workforce understands the expected standards of professional behaviour. But it doesn't check that personnel understand lessons shared through organisational learning.

The force checks workforce understanding of the standards of professional behaviour during promotion processes and through an annual [integrity health check](#), which is part of the performance development review process.

The force holds professional standards review meetings when it identifies patterns of behaviour related to either the performance or conduct of members of the workforce. The DPS, HR, staff associations and a senior officer from the local policing area discuss what they will do to address the performance or conduct.

Supervisors use the force's 'learning through reflection' process for dealing with minor performance or [conduct matters](#) so that in future, personnel fully understand the required standards.

The force told us that it evaluated the impact of training courses by using metrics, such as how often supervisors used the 'learning through reflection' process and the number of public complaints received. It also measured the workforce's understanding of some of the expected standards of behaviour before and after 'New Met for London' training.

Organisational learning

The Metropolitan Police Service doesn't have a wholly effective process for collecting and sharing organisational learning. At the time of our inspection, the force didn't have an organisational learning board.

The DPS organisational learning team identifies learning from internal and external sources. This includes recommendations from the IOPC and the Mayor's Office for Policing and Crime (MOPAC).

The complaint and conduct IT database, [Centurion](#), provides a platform on which organisational learning can be recorded. We expect the force to do this. However, during our case file review, we found that the force rarely recorded organisational learning on Centurion.

In August 2025, the force's internal auditors reported on the effectiveness of the professional standards units (PSUs), which are governed by the DPS. The auditors identified that the force needed a deeper focus on management information to establish trends and lessons learned to improve organisational learning. And they found that the force didn't have processes to track the sharing and implementation of lessons learned.

The force doesn't have a post-implementation evaluation process. And chief officers have limited involvement in how the force follows up organisational learning. This shows that the force's identification and evaluation of relevant learning is inconsistent and incomplete.

At the time of our inspection, the force was developing an application (app) to improve the gathering, sharing and implementation of organisational learning.

We found that the force maintained relationships with internal and external networks to help reinforce standards of professional behaviour and improve the workforce's understanding of them.

The force consults an independent advisory group to obtain feedback on a sample of DPS cases related to police-perpetrated domestic abuse and sexual violence. And it works with domestic abuse and sexual violence groups and other forces in relevant cases. This reinforces the standards of professional behaviour to external groups, generates [intelligence](#) and supports victims. The DPS works with MOPAC to gather learning from upheld complaints reviews. The force has established a national [appropriate authority](#) forum to share learning and best practice and to promote improvements.

The DPS holds regular formal internal meetings with staff associations, trade unions and support networks to discuss [disproportionality](#), vetting and other relevant themes.

However, representatives of some staff associations and networks told us that their relationships with the DPS could be more open and constructive. It was their view that the DPS was missing opportunities to gain insights from staff associations and networks.

The force tries to proactively identify and act on trends in public dissatisfaction to make improvements. The head of the DPS chairs a monthly performance meeting that considers data about the types of complaints received and the quality and timeliness of investigations.

At the time of our inspection, the force told us that it was planning to introduce a new 'culture, standards and integrity ecosystem'. The force has designed this system to bring together standards-related data, intelligence and information. It told us that this would make it easier to identify themes and trends and take appropriate action.

Handling and investigating public complaints, conduct matters and other potential breaches of the standards of professional behaviour

Area for improvement: The force needs to improve its complaints decision-making processes

The force needs to make sure that [police personnel](#) of appropriate seniority make decisions on how to handle complaints.

Our case file review showed that complaints resolution unit [officers](#) and [staff](#) of insufficient seniority were making complaint-handling decisions in cases recorded under [Schedule 3 of the Police Reform Act 2002](#).

We found that complaints resolution unit sergeants and police staff equivalents made most complaint-handling decisions in cases handled otherwise than by investigation. Additionally, this was true for some cases that the unit had decided to handle by way of investigation. In many other investigation cases, a sergeant made and recorded the decision accompanied by an entry indicating that the decision had been verbally agreed by an [appropriate authority](#).

This is contrary to the requirements of Schedule 3 of the Police Reform Act 2002, the [Police \(Complaints and Misconduct\) Regulations 2020](#), [Independent Office for Police Conduct statutory guidance](#) and the force's own [scheme of delegation](#).

A delegated appropriate authority of at least the rank of inspector or police staff equivalent must make all decisions to record and handle a complaint under Schedule 3.

Area for improvement: The force needs to improve its management of complaints handled outside Schedule 3 of the Police Reform Act 2002

This is in respect of the force's:

- logging of cases; and
- provision of meaningful outcomes to complainants.

Most complaints that the force receives are initially handled by the complaints resolution unit. However, when members of the public complain or express dissatisfaction by calling its [contact centre](#), the force adopts a different approach.

The contact centre call taker logs the call on the command and control system and triages the matter to establish if it amounts to a complaint. They forward complaints that require recording under [Schedule 3 of the Police Reform Act 2002](#) to the [directorate of professional standards](#). The call taker allocates all other complaint cases to the contact centre's complaint desk or the local area operations room supervisor for [service recovery](#).

Once the contact centre complaint desk has resolved the matter by way of service recovery, it records a 'closure code' relevant to the nature of the matter rather than an auditable complaint code. And it does this without informing the directorate of professional standards. The force doesn't record these cases on [Centurion](#), the complaints and conduct database. As a result, the data doesn't appear on the force's official complaint statistics collated by the [Independent Office for Police Conduct](#).

In 2024, contact centre call takers created 28,596 of these call logs. In 2025 up until the time of our inspection in November, it had created 24,595. It isn't known how many of these cases were complaints resolved by way of service recovery as the force doesn't record it. It is likely that the numbers are substantial.

In November 2019, the Independent Office for Police Conduct circulated guidance to all forces on how contact centre personnel should deal with expressions of dissatisfaction. The Metropolitan Police Service's process doesn't comply.

The guidance states that updates to complainants and interested parties should be regular and meaningful. We reviewed 24 complaint cases that were dealt with by the complaints resolution unit. The complainant received a meaningful outcome in only 15 of those cases.

In most of these 15 cases, the force merely told the complainant that it had forwarded their case to another team to review and then closed the case. The force didn't record the outcome of the review on Centurion. We didn't find any record of the complainant receiving any update following the review.

Area for improvement: The force needs to improve the way it handles and manages complaints and conduct allegations

This is in respect of the force's:

- formulation of terms of reference;
- provision of rationales for handling decisions and regular meaningful updates to complainants; and
- quality of complaint cases handled otherwise than by investigation.

We found that in many cases where the force had carried out an investigation, it hadn't recorded appropriate terms of reference. In our case file review, 43 of the 64 investigated complaint and [conduct matters](#) we examined didn't have terms of reference.

We found that in its initial letters to complainants, the complaints resolution unit stated that it had recorded their complaints. But in each letter we reviewed, it didn't state whether the force proposed to investigate the complaint or handle it otherwise than by investigation. As a result, the complaints resolution unit didn't state its rationale for its decision.

We also found that investigators weren't providing complainants with updates every four weeks as required by the [Independent Office for Police Conduct statutory guidance](#). Many letters we saw didn't contain enough detail. They simply stated that the investigation was ongoing rather than explaining what progress the force had made since the last update.

Between 1 April 2024 and 31 March 2025, the [Mayor's Office for Policing and Crime](#) reviewed 426 cases that the force had resolved otherwise than by investigation. It upheld 187 review applications as it found that the outcome wasn't reasonable and proportionate.

Staff from the Mayor's Office for Policing and Crime told us that the high proportion of upheld cases was due to the [directorate of professional standards](#) not dealing with the case in accordance with statutory guidance. Our review confirmed this finding.

Capacity and capability in the directorate of professional standards

Public co-operation and support help the police to reduce crime and keep people safe. Police actions that are perceived to be unfair, disrespectful, discriminatory, or corrupt can damage public confidence and trust. Each force must make sure its workforce acts ethically and lawfully. And, if the force finds any problems with behavioural standards, it must show that it acts quickly and appropriately to address them. The force should have effective governance and the right organisational structure to allow its professional standards department (known as the directorate of professional standards (DPS) in the Metropolitan Police Service) to carry out its role. It should also allocate enough resources to the task, including appropriately trained and experienced personnel.

Governance and capacity in the directorate of professional standards

We found that there were effective DPS governance, structures and processes in place in the Metropolitan Police Service.

The assistant commissioner (professionalism, trust, legitimacy) leads the DPS and is supported by a deputy assistant commissioner and a commander. The force told us that the DPS had experienced a high turnover at commander level. However, at the time of our inspection, the postholder had committed to stay in the role for a minimum of two years. This should help retain strategic knowledge and improve governance of the DPS.

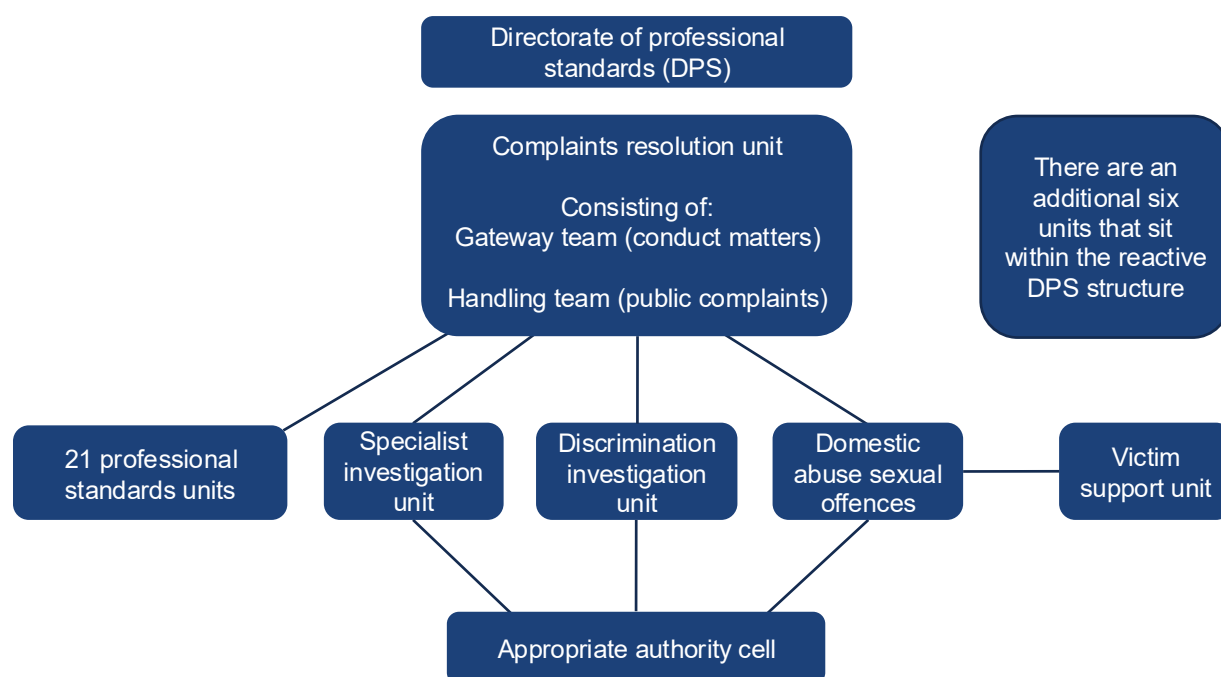
The force provided us with a scheme of delegation that sets out the level of seniority at which individual decisions can be made. However, at the time of our inspection, it wasn't signed or dated. The document indicated that an officer of the rank of inspector or above should be the decision-maker in complaint and conduct matters. We noted that the force's scheme of delegation only referred to police officers although decision-makers can also be the police staff equivalent of an inspector.

We observed a range of regular DPS meetings. Each had a specific purpose and supported good governance of DPS operational functions. Good quality management information informed the meetings, which senior leaders ran effectively.

There is a central DPS and 21 local PSUs. The central DPS consists of the complaints resolution unit (CRU), which initially handles all public complaints and conduct cases that come into the DPS, and 11 further specialist teams. These include the:

- discrimination investigation unit;
- specialist investigation unit (SIU);
- domestic abuse and sexual offences team (DASO); and
- appropriate authority cell.

Figure 1: Structure of the Metropolitan Police Service directorate of professional standards



Source: HMICFRS (based on information provided by the Metropolitan Police Service)

The discrimination investigation unit, SIU and DASO team investigate allegations of [misconduct](#) and public complaints that meet the threshold for gross misconduct. The appropriate authority cell makes decisions in relation to these gross misconduct cases. The PSUs handle and investigate allegations of misconduct and public complaints that meet the threshold for misconduct. There is 1 PSU on each of the 12 [basic command units](#) and 1 on each of the 9 operational command units.

In December 2024, the force transferred governance responsibility for the PSUs from their respective basic command units and operational command units to the central DPS. The DPS workforce, including PSU personnel, told us that this was a positive change which included:

- a reduction in caseloads in some PSUs;
- improved access to information on Centurion; and
- improved operational consistency.

We found that the force mostly had enough resources to investigate complaints and allegations of misconduct. However, we were told that capacity across the PSUs varied. This is because the force has allocated similar resources to most PSUs regardless of demand. We found that PSU investigators were carrying between 6 and 30 cases each. The force told us that it could move resources across the PSUs, but PSU personnel told us that this didn't always happen.

The CRU comprises the complaints team, which initially handles complaints, and the gateway team, which initially handles internal conduct matters. The complaints team comprises a chief inspector, 3 supervisors and 27 complaint handlers. At the time of our inspection, there were 6 complaint handler vacancies. The gateway team comprises a chief inspector, 2 inspectors and 12 sergeants. As the time of our inspection, the force was reviewing the capacity of these teams.

DPS personnel told us that the CRU had enough officers and staff to initially handle and allocate new complaints. However, these handlers have target time frames within which they must resolve complaints. If they can't achieve this, they pass the case to the relevant PSU. We found that the CRU's attempts to manage demand and meet these time frames could result in complaints not being handled in accordance with statutory guidance. Allowing the CRU more time to handle complaints might require further resources but could reduce demand on PSUs.

At the time of our inspection, DASO victim support officers (VSOs) were carrying high workloads of around 25 to 30 cases each. These cases can be lengthy and complex. We were told that there were often delays in allocating VSOs due to a lack of capacity.

Training and experience in the directorate of professional standards

DPS senior managers are generally experienced and trained appropriately to effectively carry out their roles.

Overall, we found that the DPS workforce had a good level of experience. Many members of the DPS were accredited to the [professionalising investigations programme](#) level suitable for their role. However, this was more consistent in the central DPS than the PSUs.

We found that most members of the DPS workforce had attended the relevant College of Policing-endorsed courses. The DPS workforce told us that they should attend the training approximately six months after being in post. This wasn't always possible due to availability and the timing of courses.

The DPS has developed its own in-house professional standards training. The force told us that it broadly covered the same topics as the College of Policing-endorsed courses. However, members of the DPS workforce had mixed views of the training. Some reported that it wasn't always in line with statutory guidance. For example, the training had advised them not to view [body-worn video](#) footage before making a handling decision. However, the IOPC's statutory guidance allows this.

Some DPS personnel told us that they wanted more role-specific training. And they told us that they mostly learned any specialist knowledge in their roles from more experienced colleagues. Some told us that they weren't confident in their knowledge of the relevant regulations.

The force recognises the benefit of having personnel with specialist backgrounds and knowledge in certain roles. For example, at the time of our inspection all DASO VSOs were trained in investigating sexual offences. The force has provided some specific training on areas such as discrimination. However, members of the DPS workforce told us that the force didn't provide it consistently for all teams.

We found that training records for the wider DPS workforce were incomplete and not up to date. We were unable to ascertain from the records which members of the workforce had completed which training courses.

The SIU provides the out-of-hours [on-call](#) service for the DPS. The on-call team comprises a superintendent, a chief inspector, 3 sergeants and 10–14 constables. The force told us that there was always an experienced level 3 professionalising investigations programme-accredited on-call detective superintendent available if required to initially respond to [death and serious injury](#) incidents. Other DPS units also have staff and officers on duty over weekends.

At the time of our inspection in November 2025 and as part of its transformation programme, the force was developing a target operating model. It was aiming to implement the model in March 2026. The model didn't include a proposal to increase capacity in the DPS. However, the force anticipated that existing DPS resources would be reallocated into areas of priority, such as the DASO team and complaint handling. This could leave other areas of the DPS with less capacity.

There was also a force initiative to rotate members of the workforce who had been in non-operational posts longer than ten years. Furthermore, the force was carrying out work to identify all roles in the force suitable for people with [adjusted duties](#) to move to. This would displace those already in these roles.

The combination of these three initiatives has the potential to result in the force moving established and experienced personnel to posts outside the DPS.

Processes for the identification and initial handling of potential breaches of the standards of professional behaviour

The UK government introduced the [Police \(Conduct\) Regulations 2020](#) and the Police (Complaints and Misconduct) Regulations 2020 for all forces in England and Wales. These regulations provide a flexible approach to handling conduct matters and complaints about the police.

To promote a culture of learning in police forces, the new regulations include a [practice requiring improvement](#) process. This means that complaints or conduct matters that aren't potential misconduct or gross misconduct can be resolved quickly and informally. The intention is to give the best possible response to the complainant.

We assessed whether the force made sound decisions when handling complaints and conduct allegations. This included whether the force made any necessary referrals to the IOPC and complied with statutory requirements by making handling decisions in a timely manner.

Initial handling of complaints and conduct matters

When the force receives complaints and allegations of breaches of the standards of professional behaviour, it must assess them. This is to decide whether they need to be formally recorded under Schedule 3 of the Police Reform Act 2002. This is in line with IOPC statutory guidance for the police complaints system. This process creates accurate, auditable records that can be relied on in subsequent investigations and disciplinary proceedings.

All 43 police forces in England and Wales use the Centurion software to record complaints and conduct matters that are being handled under Schedule 3 of the Police Reform Act 2002.

Initial handling of public complaints logged outside Schedule 3

Members of the public make complaints to the Metropolitan Police Service in a variety of ways. The CRU collates all complaints made to the force except those made by a phone call to the contact centre and which contact centre personnel subsequently handle outside Schedule 3. The CRU triages the complaint and decides if the matter is to be recorded under Schedule 3 or logged and handled outside Schedule 3 by way of service recovery.

The CRU forwards matters requiring investigation to the DASO team, the SIU, the discrimination investigation unit or the relevant local PSU.

The CRU allocates complaint cases that require handling otherwise than by investigation to its own complaint handlers, if they can resolve the case within 80 minutes. If not, the CRU allocates it to the relevant local PSU.

The CRU allocates complaints logged outside Schedule 3 to its own case handlers for resolution.

The way in which the CRU triages and records public complaints creates an unnecessary delay. The CRU doesn't log or record complaints on Centurion until after it has assessed and allocated the case. This is because CRU case handlers enter details of the case on Centurion themselves. The CRU logs or records cases it allocates to the PSUs or other investigative units using staff working overtime, often at weekends.

[The IOPC complaints bulletin](#) for the year ending 31 March 2025 shows that the force logged 12,039 complaints in an average of seven working days. This compares to an average of four working days for the most similar force and a national average of seven working days. The force's own performance data for the year ending 31 August 2025 shows it took an average of ten working days to log complaints.

During our case file review, we examined 55 complaint cases. In 4 cases, it took the force more than 14 working days to log the complaint. In a further 10 cases, it took between 9 and 14 working days to log the complaint. The force took 3 to 8 working days to log 23 cases and 18 were logged within 2 working days.

When members of the public complain or express dissatisfaction by calling its contact centre, the force adopts a different approach. Call takers log the call on the command and control system and triage the matter to establish if it amounts to a complaint. The contact centre forwards complaints that require recording under Schedule 3 to the DPS. It allocates all other complaint cases to its own complaint desk or the local area operations room supervisor for service recovery.

Once the contact centre complaint desk has resolved the matter by way of service recovery, it records a 'closure code' relevant to the nature of the matter rather than an auditable complaint code. And it does so without informing the DPS. The force doesn't record these cases on Centurion, so the data doesn't appear on the official complaint statistics collated by the IOPC. In 2024, the contact centre created 28,596 such call logs. In 2025, up to the time of our inspection in November, it had created 24,595. It isn't known how many of these cases were complaints resolved by way of service recovery as we were told that the force didn't keep such records. It is likely that the numbers are substantial.

In November 2019, the IOPC circulated guidance to all forces about expressions of dissatisfaction that forces were dealing with in force contact centres.

The guidance states: "If it is an enquiry of someone dissatisfied, that is resolved quickly, to the satisfaction of the complainant, then forces need not formally log it. However, if it appears that the complainant would like something more to happen than merely having their query answered, this will need to be logged in line with IOPC guidance on data capture so that the information can be extracted."

The force isn't complying with this IOPC guidance. And it means that complainants receive a different standard of service depending on how they make their complaint.

We reviewed 24 complaint cases that the CRU had resolved by way of service recovery. We found that it dealt with most of them and responded to the complainant on the day it logged the complaint.

However, in many cases, there was no record that complaint handlers had made initial contact with the complainant to understand their complaint. The complainant received a meaningful outcome in only 15 of the 24 cases.

In most of these 15 cases, the force merely told the complainant that it had forwarded their case to another team to review and then closed the case. The force didn't record the outcome of the review on Centurion. We didn't find any record of the complainant receiving any update following the review.

We found that the CRU had resolved some cases using the service recovery process without informing the complainant of their right to have their complaint formally recorded should they remain dissatisfied. The DPS told us that following a MOPAC review in April 2025, the force improved its performance in this area. And it told us that from September 2025, the CRU provided complainants with a document explaining their rights.

As a result, we examined a further ten such complaints logged and resolved by way of service recovery in early October 2025. We found in seven cases that the CRU informed the complainant of their rights and attached the document. One case had the relevant information but no document, and two cases had neither the information nor the document.

We found that in 21 of the 24 service recovery cases we examined, it was appropriate for the force to handle them outside Schedule 3. Cases where it wasn't appropriate included allegations of excessive force and racial discrimination and a case involving a complex complaint of a sensitive nature.

We found that CRU first-line supervisors [dip sampled](#) three cases resolved using the service recovery process per case handler per month. But there should have been oversight at a more senior level of the handling and resolution of complaints outside Schedule 3.

Initial handling of complaints recorded under Schedule 3

Our case file review showed that CRU officers and staff of insufficient seniority were making complaint-handling decisions in cases recorded under Schedule 3. We also found that the CRU recorded handling decisions briefly on an email to complaint handlers with little or no rationale.

We found that CRU sergeants and police staff equivalents made most complaint-handling decisions in cases dealt with otherwise than by investigation. This was also true for some cases that the CRU decided to handle by way of investigation. In many investigation cases, the decision was made and recorded by a sergeant, accompanied by an entry indicating that the decision had been verbally agreed by an appropriate authority.

The force told us that it was an agreed strategy to allow CRU sergeants and police staff equivalents to make complaint-handling decisions in cases dealt with otherwise than by investigation. It said appropriate authorities dip sampled these decisions to provide some oversight. However, senior DPS personnel told us that sergeants making handling decisions in respect of investigation cases was an error. They stated that it happened over a brief period and that the DPS had rectified it.

As a result, we examined a further ten investigation handling decisions that the CRU had made on cases it recorded in October 2025. We found three cases where the appropriate authority had made and documented the decision. In a further four cases, a sergeant or staff equivalent had recorded the decision, stating that a named appropriate authority had verbally approved it.

In the remaining three cases, a sergeant or staff equivalent had made the decision with no appropriate authority input. Handling decisions made by personnel not of sufficient seniority is contrary to the requirements of the Police Reform Act 2002, the Police (Complaints and Misconduct) Regulations 2020, the IOPC statutory guidance and the force's own scheme of delegation. A delegated appropriate authority of at least the rank of inspector or police staff equivalent must make all decisions to record and handle a complaint under Schedule 3.

However, even though CRU personnel of insufficient seniority were making handling decisions, in 50 of the 55 cases we examined, we found the decision to be reasonable.

The DPS doesn't always make relevant enquiries with other areas of the force before making a handling decision. In 22 of the 55 cases, the CRU didn't make relevant enquiries. For example, it didn't always check previous complaint and conduct history on Centurion.

We found that in its initial letters to complainants, the CRU stated that it had recorded their complaints. But in the letters we reviewed, the CRU didn't state whether the force proposed to investigate the complaint or handle it otherwise than by investigation. As a result, the CRU didn't state the rationale for its decision.

Additionally, we dip sampled 16 Schedule 3 complaint cases that the DPS had decided to handle as 'no further action'. The DPS provided a detailed explanation to the complainant in 14 of the 16 cases we reviewed. But we found that in 7 of the 16 cases, 'no further action' wasn't an appropriate outcome. In 2 of the cases that the DPS had reviewed, a more appropriate outcome would have been 'unable to determine whether the service was acceptable'.

In other cases that the DPS had investigated, we found that the complainant wasn't informed of whether the service was acceptable or not.

During our case file review, we also saw examples where the DPS had finalised complaint cases incorrectly. In one case, investigators incorrectly told a complainant that the force didn't have to provide an outcome letter and the complainant didn't have a [right to review](#) because the complainant wished to remain anonymous. In another example, the DPS incorrectly closed a case as 'no further action' as the complainant withdrew from the process. Enough information was available in both cases to have provided an outcome letter and the right of review. All these examples suggest that investigators lack understanding of the IOPC statutory guidance.

The DPS told us that the CRU focused on "quick wins". It stated that 80 percent of CRU work was the service recovery of cases outside Schedule 3. A member of the DPS workforce told us that the CRU was "strapped by demand and not able to give a gold level of service".

We found that the CRU was compromising on standards to manage demand. Examples included:

- low quality, generic initial letters lacking detail sent to complainants;
- limited contact with complainants;
- decisions made at an inappropriate level; and
- cases sent for review and then immediately closed.

Initial handling of conduct matters

Since March 2024, the Metropolitan Police Service has improved the way it handles conduct cases by introducing a gateway team. The gateway team carries out fact finding on each reported matter. This is to determine whether it needs to record the case as a conduct matter or if the force can deal with it as a grievance or performance issue. According to the force's internal reports, in the year ending 31 May 2025, there was a 30 percent reduction in recorded cases compared with the same period the previous year. In the year immediately prior to our inspection, the gateway team recorded 3,396 conduct allegations.

The process means that the force doesn't record conduct matters promptly. Its performance data shows that in the year ending 31 July 2025, it took an average of 16 days to formally record cases.

Our case file review showed that the gateway team made, recorded and rationalised handling decisions using a template to maintain consistency.

We found that in 52 of the 55 conduct cases we reviewed, the gateway team had adequately documented and rationalised decisions. But in 14 cases, the gateway team hadn't updated those who made the allegations with the handling decision.

We found the handling decision to be inappropriate in only 4 of the 55 cases. In each of these cases, we considered that the allegation didn't justify disciplinary proceedings and the force should have dealt with it another way.

We found that appropriate authorities of the correct rank or grade made conduct handling decisions. And in 46 of the 55 cases, the gateway team had recorded and considered the complaint and conduct history of the person facing the allegations.

The gateway team allocates matters requiring further investigation to other DPS investigative teams.

At the time of our inspection, the force was developing a computer-based 'Professionalism App'. The app will provide members of the workforce with a template to complete when reporting conduct matters. It will provide examples and guidance about what constitutes misconduct. The force anticipates that this will add further consistency and efficiency to the way in which it reports, records and handles conduct matters.

Initial actions relating to complaint and conduct cases

The appropriate authority must refer a complaint or conduct matter to the IOPC when it includes certain types of allegations. These include a serious assault, a serious sexual offence or serious corruption. They also include any criminal offence or behaviour that is liable to lead to disciplinary proceedings and which, in either case, is aggravated by discriminatory behaviour on the grounds of race, sex, religion or other [protected characteristics](#).

In 2 of the 26 cases that required mandatory referral to the IOPC, the force failed to make the referral. The two cases included domestic abuse offences and an allegation of perverting the course of justice.

In 26 of the 110 complaint and conduct cases we examined, there was an allegation of police criminality. In six cases, it appeared that the force had failed to identify and acknowledge the presence of a crime or had failed to record and deal with it appropriately. These included potential offences under the [Computer Misuse Act 1990](#), the [Data Protection Act 2018](#), the [Protection from Harassment Act 1997](#) and the [Road Traffic Act 1988](#).

It may, in some cases, be proportionate for a force to deal with a matter as internal misconduct rather than as a crime. But the force should record a clear rationale for this decision.

In the 110 complaint and conduct case files we examined, we found that 19 contained elements of discrimination or sexual misconduct. The force correctly identified and recorded 11 of them.

During our file review, we saw use of the terms 'learning through reflection' and [reflective practice review process](#). Investigators and complaint handlers used both terms in similar cases we reviewed, to the point where it was clear that there was misunderstanding of the meaning of each. The force told us that it used its 'learning through reflection' process as an informal measure. It said that the reflective practice review process was more formal and was used where it finds no misconduct but that

the person would benefit from learning from the case. We urge the force to clarify to case investigators and complaint handlers how these two processes should be used.

Accessibility of the public complaints system

Forces in England and Wales have a statutory obligation to promote access to their complaints system and to make sure the public can use it. The force should make sure that its complaints system is accessible to everyone. This includes people with protected characteristics and those from [hard-to-reach communities](#).

The Metropolitan Police Service has some measures in place to make sure its complaints system is accessible. The public can make complaints using an online form, by email to the force, via the IOPC and by calling the contact centre.

The force's culture, diversity and inclusion team works with communities that lack trust in, or are less likely to work with, policing. The team's work includes raising awareness of how members of the public can access the complaints system.

The force also operates an 'engage channel', which is a community online reporting app, to provide a link between the public and local policing teams. The app includes a language translation function. The public can use this app to look for information from the force about making a complaint and receive the relevant guidance.

However, we didn't find other evidence of specific initiatives to improve the accessibility of the complaints system.

The Metropolitan Police Service doesn't consistently support complainants who may need additional help. In 17 of the 55 complaint cases we examined, complainants may have needed additional support. This included, for example, when the complainant indicated that they had a disability. The force provided extra help to ten of the complainants, but it failed to recognise that six complainants may have needed additional support. In one case, the force recognised the need for extra help but didn't provide it.

Processes and governance for investigating and resolving public complaints and conduct matters

The standard of investigations

Investigations are an opportunity for the force to address the concerns of the public and the workforce. They help forces to learn and improve and, where necessary, to hold officers and staff accountable. They can be lengthy and have a major impact on everyone involved. So it is extremely important that they are both thorough and proportionate to the seriousness of the allegation or concern.

The Metropolitan Police Service is relatively timely at finalising cases by investigation. The IOPC complaints data for the year ending 31 March 2025 shows that the force took an average of 272 working days to finalise complaint cases by investigation that didn't involve [special procedures](#). This was the same as the most similar force average of 272 working days and a national average of 234. In cases involving special procedures, the force took 309 working days to finalise the case. This compares to an average of 397 working days in the most similar force and a national average of 329 working days.

However, in cases handled otherwise than by investigation, the force took longer to finalise them than the most similar force or the national average. The IOPC complaints data for the year ending 31 March 2025 shows that the force took an average of 174 working days to finalise Schedule 3 complaints otherwise than by investigation. This compares to an average of 124 working days for the most similar force and a national average of 124 working days.

We found substantial evidence to suggest that the force had carried out thorough and proportionate investigations in both conduct and complaint cases. When the force finalised complaint cases otherwise than by investigation, its approach was also proportionate.

On conclusion of cases, we saw ample evidence that the investigating officer or case handler had prepared a final report or outcome letter that was comprehensive and well written.

In many cases where the force had carried out an investigation, we found that it hadn't recorded appropriate terms of reference. And many cases lacked an investigation plan.

We reviewed 64 investigated complaint and conduct cases. We found that 43 didn't have terms of reference and 32 didn't have an investigation plan.

In some cases, the force stated terms of reference for the first time in final letters to complainants. But these were generic, not specific to the case in question, and it appeared that investigators had cut and pasted them from other letters. We saw that in some cases, investigators had prepared action lists, which outlined what they had completed and what was outstanding. These didn't constitute a formal investigation plan.

In [our 2022 national report 'An inspection of vetting, misconduct, and misogyny in the police service'](#), we recommended that forces should produce and follow an investigation plan, endorsed by a supervisor.

We found that in 34 of the 48 complaint and conduct cases that required a [severity assessment](#), the DPS had completed them in a thorough, proportionate and timely manner. And it carried out a subsequent review of the severity assessment in 29 of those cases.

When reviewing the 64 investigated complaint and conduct cases, we found that the DPS didn't consistently maintain decision or policy logs. In most cases, it had documented the handling decision, severity assessment and final determination. But in many cases, we found no record of other decisions made during the investigation or the rationale for them.

In 39 of the 64 cases, supervisors had carried out reviews. We expected to see monthly supervisory reviews in addition to the reviews triggered by the Centurion system at three and six months. However, we found that supervisors didn't complete many of the reviews or recorded very little or no detail. Some were a cut and paste entry from a previous review. Very few cases had regular, meaningful supervisory reviews of progress.

Similarly, we found that investigators weren't providing complainants with updates every four weeks as required by the IOPC statutory guidance. And many updates we saw didn't contain enough detail and simply stated that the investigation was ongoing.

The force isn't using Centurion in a standardised way to record cases. And its retention of documents is also inconsistent. We found that investigators were using Centurion, and other shared folders, as they saw fit. Some DPS teams have created their own standalone spreadsheets to record some investigation progress. This is a risk for the force as there is no direct link between the information held on these spreadsheets and the information held on Centurion.

We found no evidence that the force provided formal training to personnel using Centurion or that there was any effective policy or guidance on its use. This makes it difficult for colleagues, supervisors or case handlers to find relevant material. We urge the force to standardise its approach to the use of Centurion.

Welfare support for personnel involved in complaint and conduct investigations

Police forces need to make sure that they always consider the welfare of all police personnel involved in a professional standards investigation. This includes personnel accused of wrongdoing, those who have made allegations and those investigating.

The Metropolitan Police Service considers the welfare of accused police personnel. At the time of our inspection, it had recently taken steps to improve the welfare support it provided to officers and staff under DPS investigation.

An officer of superintendent rank leads the force's welfare support provision. In September 2024, the force published the results of a survey it had circulated to 5,000 members of the workforce, of whom 1,500 responded. This showed that the force needed to improve welfare support for police staff and officers under investigation. The force set up a working group to help achieve this. This included, for example, helping accused personnel to reintegrate into the workforce following the conclusion of their case.

The force has approximately 2,000 trained volunteer welfare support officers (WSOs). They carry out their role in addition to their normal duties. The force's website states that "they can be appointed in circumstances where it is likely the individual may benefit from additional support during a challenging time in their career or their personal life". The force mainly uses WSOs to provide support in conduct and employment tribunal matters.

The force has a guidance document dated December 2023 that sets out the roles of WSOs and their managers. It includes a section on supporting personnel who are subject to a DPS investigation. The document also provides DPS contact numbers for WSOs to use in emergency situations out of hours.

Chief inspectors voluntarily carry out the role of welfare co-ordinator and are located on individual basic command units and operational command units. Due to their seniority, the force is confident that they will be aware of any officers or staff in their borough or command unit who are under investigation. And it is confident that they will be able to identify personnel who need welfare support and request the allocation of a WSO. Personnel under investigation can also nominate a person of their choice to support them through the misconduct process. This can either be a trained WSO or a colleague.

We were pleased to see that DASO VSOs worked with victims of police-perpetrated domestic and [sexual abuse](#). This included providing updates to the victims, familiarising them with disciplinary processes and accompanying them to [misconduct](#) or court hearings when they were giving evidence. Victims can be both members of the public or police personnel. At the time of our inspection, there was a four-month backlog in the force assigning a DASO VSO to a victim. However, the DASO team prioritised urgent cases if a hearing was imminent.

We found that some personnel weren't aware of the welfare support available. We also found that the force provided little or no support to personnel who reported wrongdoing, other than through line managers.

Beyond line management support, we saw limited evidence that the force provided routine welfare support to DPS personnel who handle and investigate cases. The force told us that it had provided some DASO team and SIU personnel with training on trauma impact prevention techniques. It has also provided this training to personnel working on Operation Onyx, which is an initiative to reassess historic sexual offences or domestic abuse cases involving force officers and staff.

The force told us that it recognised the adverse effect on DPS personnel carrying out investigations and that a working group would be considering how it could improve support for them.

Some personnel expressed concern that the force had disbanded well-being teams approximately six months before our inspection. Many weren't aware of any other welfare and well-being provision. However, the force told us that the role of the well-being teams was to provide more general support than WSOs. For example, they would provide support if an officer was injured or following traumatic incidents. The force said that it envisaged replacing the well-being teams with a single volunteer in each policing area. This would be in addition to the dedicated WSOs.

The force told us that it had developed a new policy on designating officers and staff as interested persons in misconduct proceedings. The policy states that where the subject is a police officer, the force will give victims and reporters of wrongdoing the status of an interested person. This means that they will receive regular case updates. Under the policy, the status of interested person won't apply where the subject is police staff. We understand that this was due to a concern over potential infringement of [Article 8 of the European Convention of Human Rights](#).

At the time of our inspection, the force hadn't formally agreed the policy, but it told us that it had already implemented the principles. We urge the force to address the disparity in the support it provides to officers and staff.

Suspension and restriction of members of the workforce and accelerated procedures

The Metropolitan Police Service does consider suspending or redeploying the accused person.

It also uses [accelerated procedures](#) in certain cases. This is so that police officers appear quickly before a chief officer who can dismiss them, if appropriate, where there is incontrovertible evidence of gross misconduct.

The force told us that it now had a much better understanding of the use of accelerated misconduct hearings and that it explored more opportunities to hold them. In 2023, the force held 62 accelerated hearings. In 2024, it held 82, and in 2025, it had held 69 by October.

The force has a suspension policy, dated September 2024, which outlines the suspension process. It applies to all police officers and special constables up to the rank of deputy assistant commissioner. The policy states that an officer of at least commander rank must make suspension decisions and carry out a subsequent review every 28 days.

The suspensions review team carries out the administration and management of the suspended officer list, which makes sure they are reviewed every 28 days.

In March 2025, the force developed a policy on restricting the duties of officers and special constables who are facing allegations of gross misconduct.

Members of the workforce told us that before it was introduced, some local area senior officers were approving and recording some restrictions that the DPS wasn't aware of. Under the new policy, a DPS officer of at least superintendent rank, or staff equivalent, must approve all restriction decisions. The DPS records all restrictions on Centurion.

The force reviews restrictions every three months or sooner if circumstances have changed.

At the time of our inspection, the force told us that it had suspended 175 officers and staff and had restricted the duties of a further 583 personnel. We reviewed 110 complaint and conduct cases. We found that in only 17 of the 51 cases where it was appropriate to consider suspension or restriction, the force recorded that it had done so.

We compared the force's [barred and advisory lists](#) records from 2024 to 2025 with the data held by the College of Policing. The College of Policing creates and maintains the list from data provided by the force.

We examined five barred list cases selected from force records and five from College of Policing records. In all ten cases, the force had made the required notification. It had also recorded it on Centurion and on the [Police National Database \(PND\)](#).

We examined five advisory list cases selected from force records and five from College of Policing records. We found that the force had made the necessary notification on nine occasions. In six cases, we found no record of the notification on Centurion. In three cases, the force hadn't made a corresponding entry on the PND.

As described in [the 'Consistency and fairness in decision-making' section](#), the force has decided not to progress with gross misconduct hearings where the subject resigns, unless there are exceptional circumstances. These circumstances include discrimination offences and violence against women and girls. If a case isn't progressed to a gross misconduct hearing, the officer won't appear on the barred or advisory lists. The force told us that it was mitigating this risk by making an entry on the PND.

College of Policing records indicate that there have been 61 of these cases since the force introduced the policy. We examined five cases where the hearing wasn't progressed and found that only four had a PND entry. This means that if the officer applied for a policing role in the future, there is nothing in place to alert the recruiting force that a previous gross misconduct investigation had taken place. We urge the force to satisfy itself that there are no other cases where it should have made a PND entry. And it should make sure that, in future, all relevant cases result in a PND entry.

We raised this issue with the force at the time of our inspection.

The service provided to complainants

An important part of creating and maintaining trust and confidence in policing is providing a good level of service to complainants.

Complainants can expect to be involved in an investigation from the outset. They are entitled to:

- receive a copy of the terms of reference for the investigation;
- provide their account of events; and
- receive regular, meaningful and timely updates.

We examined whether the force has effective processes in place to make sure it provides a good level of service to complainants.

We also examined the number of cases where complainants exercised their right to review and how many of these reviews were upheld by the IOPC or the local policing body, MOPAC.

Our case file review showed that the Metropolitan Police Service provided an acceptable level of service to most complainants and that the outcome was reasonable and proportionate. This was particularly the case where the force recorded the case under Schedule 3.

In some cases, when complainants are dissatisfied with the outcome of an investigation, they can ask the IOPC for a review. Between 1 April 2024 and 31 March 2025, the IOPC finalised 246 applications for a review of complaint cases that the force had investigated. It found that 83 had outcomes that weren't reasonable and proportionate.

During the same period, the IOPC carried out 271 reviews of complaint cases that the force had concluded otherwise than by investigation. It found that 72 cases had outcomes that weren't reasonable and proportionate.

MOPAC finalised 28 complaint investigation reviews during the same period. It found that in nine cases, the outcome wasn't reasonable and proportionate. It reviewed 426 cases resolved otherwise than by investigation and upheld 187.

MOPAC personnel told us that this high proportion of upheld cases was due to the DPS not following statutory guidance. The top two reasons were that the force hadn't addressed or fully understood the complaint and/or hadn't pursued all reasonable lines of enquiry. We examined 11 upheld reviews. We found that in nine cases, MOPAC upheld the review because it had been handled poorly.

Information sharing

It is important that the force gathers and shares [adverse information](#) about members of its workforce. This helps to make sure that it maintains professional standards and identifies and mitigates risks. In our inspection, we examined:

- whether the force can record adverse information;
- whether departments holding this information shared it appropriately within the force; and
- whether the force considered such information when making decisions about complaint and conduct cases.

Recording and sharing of adverse information

The Metropolitan Police Service regularly shares relevant information between some departments and has an established process for doing so.

We found that the DPS shared information about personnel with HR, local policing areas and the Police Federation through its professional standards review meetings. The chief inspector (professionalism) from the local policing area chairs the monthly meeting. Typically, participants consider an individual's:

- complaint and conduct history;
- expenses;
- [notifiable associations](#), which the force refers to as declarable associations;
- business interests; and
- other relevant topics.

It then decides on a course of action. The meeting also provides the force with opportunities to take preventative measures through early intervention.

The professional standards review meetings are an alternative to a [people intelligence meeting](#). But they don't include representatives from the [anti-corruption unit and abuse command](#), legal services, the [force vetting unit](#) and the training department.

The force told us that it proposed to remove the local chief inspector (professionalism) roles through its transformation programme changes. This may have an impact on how the DPS and local policing areas share information.

The force also told us that it was developing a DPS 'fusion intelligence cell'. The cell will bring together information from selected force databases and develop intelligence to identify issues and learning. It will draw on data sources such as sickness, overtime, complaints, absence, misconduct and sensitive intelligence. The cell will send information to the relevant team for action. At the time of our inspection, the force was still developing this initiative, so we were unable to judge its effectiveness.

We found that the Metropolitan Police Service routinely considered relevant information from grievances, employment tribunals and civil litigation cases to identify potential breaches in standards of professional behaviour. The force also reviews cases where a court has acquitted a member of the workforce, or they are subject to no further action, to determine if there is any misconduct.

The DPS holds a daily management meeting that is attended by representatives from across the department. It shares time-critical information, such as arrests of members of the workforce, disciplinary proceedings, court proceedings and media interest. The meeting also makes sure that the force is taking appropriate action in respect of significant incidents in the previous 24 hours.

Considering relevant information

We found that the DPS considered previous complaint and conduct history in most cases before making handling decisions.

Our case file review showed that the DPS made enquiries with other areas of the force before making a handling decision in 46 of 55 conduct cases. It only made enquiries in 22 of 55 complaint cases.

To improve the accessibility of information across the DPS, the force has developed the 'Combo Checker'. All DPS Centurion users can use the tool to search 25 other relevant databases, including:

- complaint and conduct history;
- disciplinary findings;
- [unsatisfactory performance](#) information;
- 'learning through reflection' and reflective practice review process history;
- vetting information; and
- HR information.

Holding police officers and staff accountable for their behaviour

Area for improvement: The force needs to improve its understanding of potential disproportionality in the handling, investigation and resolution of complaints and conduct matters

We found that the force carried out some work to address [disproportionality](#) in its processes. And a disproportionality board meets quarterly to consider some related work across the force. However, the force still has work to do.

The [directorate of professional standards](#) doesn't carry out any formal, detailed analysis to establish if there is any disproportionality across the nine [protected characteristics](#) in its investigations and decision-making.

In November 2023, the strategic insights unit identified that the force was more likely to refer Black and ethnic minority members of the workforce to the directorate of professional standards. It made recommendations to tackle ethnic disproportionality at all stages of the [misconduct](#) process. At the time of our inspection, the force had only completed 5 of the 22 recommended actions.

Consistency and fairness in decision-making

Officers and staff must be held accountable in a fair and impartial way. And decision-making needs to be consistent. The force must make sure that its approach to complaints and conduct matters, and the resulting outcomes, are proportionate to the allegations and investigation findings.

The Metropolitan Police Service has some processes in place to review the fairness, consistency and proportionality of its approach to DPS decision-making. However, we found that some aspects of the force's decision-making in relation to complaints and conduct investigations weren't always consistent and fair.

We found that CRU decisions on initial handling were largely consistent, fair and proportionate. The CRU holds a daily meeting chaired by a chief inspector where the appropriate authorities can raise cases for discussion. Furthermore, along with the DASO team and the SIU, the CRU attends an escalation panel held by the force every two weeks. This meeting discusses cases where there is a lack of consensus on decision-making, which includes recording decisions, [severity assessments](#) and case allocation.

The appropriate authority cell makes decisions in relation to both misconduct and gross misconduct cases. We were told that it held [benchmarking](#) exercises to make sure that decisions were consistent. We were also told that the outcomes of these exercises weren't routinely shared with appropriate authorities in the PSUs.

The PSUs' appropriate authorities make decisions on cases dealt with otherwise than by investigation and investigations not subject to special procedures.

Benchmarking exercises aren't completed across appropriate authorities from different PSUs. We would encourage all appropriate authorities to carry out further benchmarking exercises and share the learning.

Appropriate authority cell officers have also set up a national appropriate authority forum. The [National Police Chiefs' Council](#) has agreed the forum's terms of reference. Representatives from all England and Wales police forces, as well as the IOPC, attend. The forum, which had been operational for approximately 18 months at the time of our inspection, meets quarterly. It discusses topics such as changes in legislation and cases of interest. And the position of chair rotates through the forces.

There was a perception among some personnel that appropriate authority decision-making was inconsistent and dependent on who was on duty that day. However, our review of 110 complaint and conduct cases didn't identify disproportionality in decision-making or outcomes.

We also found that some personnel felt in cases where a chief officer was the subject, appropriate officer decision-making was more lenient and unfair. We reviewed ten such cases and found that in four of them, the decision-making wasn't wholly in line with statutory guidance.

The force also appears to have inappropriately taken, or tried to take, the most minor form of resolution. And appropriate authority recorded decision-making and rationalisation in some of these cases wasn't as comprehensive or transparent as it should have been. This is concerning and could give rise to the perception that the force deals with cases involving chief officers differently.

In respect of protected characteristics (not rank or seniority), the force carries out some work to address disproportionality in its processes. A force-wide disproportionality board meets quarterly. In addition, the force recently commissioned an independent review of disproportionality across the force. And subsequently, in November 2025, it published a review of structural racism, '[30 Patterns of Harm](#)'.

However, we found that the force still had progress to make in addressing disproportionality within its complaints and misconduct processes.

In November 2023, the strategic insights unit identified that the force was more likely to refer Black and ethnic minority members of the workforce to the DPS. The disproportionality board made recommendations to tackle this at all stages of the misconduct process. We reviewed the action tracker developed by the force to track progress against the recommendations. We found that it was undated and didn't have target timescales for actions to be completed. At the time of our inspection, it indicated that the force had only completed 5 of the 22 recommended actions.

While the force is taking some steps to prevent and identify disproportionality, the DPS doesn't carry out any formal, detailed analysis to establish if there is any disproportionality across the nine protected characteristics in its investigations and decision-making. At the time of our inspection, the force was developing a professional misconduct reporting app. This should improve its ability to collect data related to other protected characteristics.

To fully understand the extent to which disproportionality exists, the reasons for it and take action to address it, the DPS should carry out a detailed analysis of disproportionality across the nine protected characteristics.

There is also disproportionality in the number of cases that the force found to be ‘not proven’ at [misconduct meetings](#) (55 percent), compared to misconduct hearings (13 percent). We were told that this may be due to the chairs of misconduct meetings putting too much emphasis on mitigating factors at an early stage. The force is aware of this disparity. At the time of our inspection, it was planning steps to address this, which included providing further training for misconduct meeting chairs.

In June 2024, the SIU had approximately 1,600 live cases. This volume resulted in the misconduct hearings unit struggling to arrange hearings to meet demand. In May 2024, the force agreed a policy stating that it wouldn’t hold a misconduct hearing for any officer who resigned during a gross misconduct investigation unless the case met certain exceptional criteria and it was in the public interest to hold the hearing. Officers who don’t face a hearing aren’t placed on the College of Policing’s barred list. In these circumstances, and to mitigate the risk to the public, the force updates the officer’s PND record as an alternative.

The force consulted numerous stakeholders when developing this policy, including the IOPC, the Home Office and the National Police Chiefs’ Council lead. Most cautioned against this approach. Certain organisations can apply to search the PND as part of a vetting process, but it isn’t publicly available in the same way as the barred list. This means that the force places some officers on the barred list, but not others who may also be guilty of gross misconduct but didn’t face a hearing. We understand that only 2 of the 43 police forces in England and Wales adopt this approach.

While we recognise the force’s approach is pragmatic, we would expect to see its use limited to the minimum necessary duration. And in all but the most demanding of circumstances, we would dissuade any other forces from adopting this approach.

Tackling potential corruption

Requires
improvement

The Metropolitan Police Service requires improvement at tackling potential corruption and preventing misuse of IT systems.

Preventing misuse of IT systems

Lawful business and IT monitoring capability

Lawful business monitoring is a legitimate way for forces to monitor their information systems and methods of communication. It allows forces to identify improper use of communication devices. This includes inappropriate contact with [vulnerable people](#), computer misuse, unlawful access to police records and wrongful disclosure of police data.

The counter-corruption ([intelligence](#)) [authorised professional practice \(APP\)](#) (unpublished) gives guidance on IT monitoring and states that the use of monitoring and auditing software has significant prevention, intelligence gathering and enforcement advantages. For example, such software allows the force to create alerts that immediately notify investigating [officers](#) when sexualised language is used in external communications, or if a specific police record or data has been unlawfully accessed or printed.

Most forces can use IT monitoring to gather corruption-related intelligence to help identify corrupt people. It can be particularly useful to monitor [police personnel](#) who are of concern to the force, and to identify irregular access to systems. The force can use automated checks:

- when investigating people where there are integrity concerns;
- where mitigations are required because of [notifiable associations](#), which it refers to as declarable associations;
- where the vetting process has raised concerns; and
- to make sure that access to force data is for a lawful policing purpose.

Use of IT monitoring software to tackle corruption

We identified IT monitoring as an [area for improvement](#) for the Metropolitan Police Service in [our 2018/19 PEEL inspection report](#).

And proactive IT monitoring was a recommendation in [our 2022 national report 'An inspection of vetting, misconduct, and misogyny in the police service'](#).

At the time of these reports, the Metropolitan Police Service was one of very few forces in England and Wales that didn't have any proactive IT monitoring capability. During this inspection, we were pleased to see that the force had responded with considerable élan. In 2023, it introduced IT monitoring software, and it has continued to vastly improve its IT monitoring capability.

The [anti-corruption and abuse command's \(ACAC\)](#) digital exploitation team (DET), high-tech crime unit and electronic-discovery unit use a combination of three separate IT monitoring software tools. This means that they can monitor and audit almost all of the force's IT systems across mobile and desktop devices.

But the force told us that there were still significant gaps in its overall IT monitoring coverage. This is the result of three factors.

Firstly, the force has identified difficulties in proactively monitoring some of its IT systems. This is primarily due to several of the force's IT systems not being fully compatible with its IT monitoring software. ACAC personnel are working with the force's digital, data and technology department to try to develop solutions to address this gap.

Secondly, some of the DET's methods of proactive monitoring of force-issued mobile devices are only fully effective when users download and activate a specific application (app) on their device. At the time of our inspection, the force told us that despite being instructed to do so, up to 8 percent of the workforce hadn't yet downloaded or activated the app.

DET personnel have directly contacted these members of the workforce. Some reported technical difficulties, which the DET has been able to resolve. The force recognises the corruption risk associated with these 'non-compliant devices'. Senior leaders told us that they were determined to achieve as close to 100 percent compliance as possible. The force told us that people who failed to comply may ultimately face formal [misconduct](#) proceedings.

And thirdly, the force told us that it had identified an unknown number of devices forming part of what it referred to as a 'grey estate'. Personnel are using mobile phones, SIM cards, laptops and tablets in their roles that aren't linked to force IT systems. This means that the DET can't use the force's IT monitoring software to routinely and proactively monitor how personnel are using them. In some cases, the force has procured these devices for operational use in certain specialist roles.

But some [basic command units \(BCUs\)](#) and operational command units (OCUs) have purchased devices outside the usual procurement processes.

At the time of our inspection, a steering group chaired by the force's director of service integration was trying to reduce this grey estate. It was working with OCU commanders and the data and technology department to complete a full stocktake of these devices and identify who has them. The force will then determine if the retention of any of the devices is justified. And it will consider how the DET can best audit their use to prevent and detect potential misuse. But until this work is complete, a significant but unknown number of IT devices fall outside the force's IT monitoring regime.

The force recognises that this is a significant corruption risk and has recorded the gaps in IT monitoring on its risk register. The DET, high-tech crime unit and electronic-discovery unit are still able to carry out some auditing of many individual systems. This goes some way to overcoming the proactive monitoring difficulties. It mitigates some, but not all, of the potential risks.

To maximise the proactive use of its improved IT monitoring capability, the force has created a dedicated team within the ACAC. The DET comprises 25 personnel, led by a detective inspector. The DET is bigger than entire counter-corruption units in most forces. It is a significant investment in IT monitoring resources. The DET is dedicated to routinely carrying out a wide range of activities to proactively monitor IT use across force systems. The high-tech crime unit and electronic-discovery unit support this work by carrying out proactive and intelligence-led monitoring of some systems.

DET personnel are developing a good level of IT monitoring expertise. They meet regularly to share practice. They consider any new areas of proactive monitoring to exploit. For example, at the time of our inspection, DET personnel had recently reviewed some very serious [gross misconduct](#) cases. This helped them to identify types of high-risk behaviour to further improve their monitoring methods.

The DET's approach is resulting in the development of numerous effective and innovative methods of proactive IT monitoring. These methods help the ACAC to identify potential misconduct and corruption. This includes improper contact with vulnerable [victims](#) and members of [organised crime groups](#), data breaches and computer misuse. We saw examples of this during our corruption file review, which we highlight in [the 'Sources of corruption-related intelligence' section](#). But, frustratingly, the gaps in IT monitoring coverage greatly hamper the DET's work to detect misuse.

The ACAC uses the DET's IT monitoring capability to support its anti-corruption investigations. And the force monitors police personnel when intelligence shows that they may pose a higher risk. The ACAC intelligence bureau identifies them by analysing intelligence reports and information from public complaints and misconduct reports.

The integrity assurance unit (IAU) maintains a register of police personnel who present sexual misconduct-related corruption risks. It assesses the corruption risk they pose and records the action the force takes to manage and mitigate the risks. We comment further on how the force manages sexual misconduct-related corruption intelligence in [the 'Risk management' section](#).

The ACAC works with the force's ICT department in the procurement of new IT systems. The detective superintendent from the ACAC intelligence bureau attends a monthly technical board chaired by the [deputy assistant commissioner](#) (professionalism, trust, legitimacy). And the force has also designed a minimum requirements guide that makes sure that any new or updated IT systems it develops or procures meet ACAC needs. For example, it makes sure that any new system can be covertly audited.

Overall, it is encouraging, after several years, to see such a marked improvement in the force's capability and capacity to monitor and audit its IT systems routinely and proactively. But the force still has further work to do before its IT monitoring arrangements can be assessed as fully effective.

IT monitoring policy

The Metropolitan Police Service has a lawful business monitoring policy for monitoring and recording workforce communications. The policy allows the DET to audit data for all mobile phones issued by the force. In addition, it allows for proactive monitoring of IT systems to identify and tackle corruption.

The policy provides the workforce with clear guidance regarding any expectation of privacy they may have when using force-owned handheld and other mobile systems.

But the force's policy requires the DET to get additional authorisation for some IT monitoring. DET personnel told us that this delayed the progress of some intelligence development and corruption investigations. We don't believe this extra authorisation is necessary and encourage the force to remove it.

The DET proactively monitors activity on mobile and desktop devices. DET personnel use a variety of techniques to do this. But the gaps in the force's IT monitoring coverage, mentioned in [the 'Use of IT monitoring software to tackle corruption' section](#), limit the overall effectiveness of this activity.

Digital device management

To protect sensitive information, it is important that the police manage their mobile devices. It is essential that a force has accurate records of who has each device so that it can hold the person accountable for its use. Police personnel must also understand the restrictions on the use of force-supplied devices. This is intended to make sure personnel aren't using them for unauthorised purposes.

The ACAC can identify which members of the workforce are accessing different IT systems. It achieves this through a combination of methods. An app installed on force mobile devices makes sure that the device syncs with IT systems. And the IT systems record the unique login details of users each time they access their device. We found that the ACAC intelligence bureau was able to successfully attribute devices to the relevant users.

But as we explained in [the 'Use of IT monitoring software to tackle corruption' section](#), there are mobile phones, SIM cards, laptops and tablets being used by personnel in their roles that aren't linked to force IT systems. Until the force has completed its review of these devices, it can't attribute each one to its individual user.

Social media

If forces allow the use of [encrypted apps](#) on force-issue mobile phones, it is very difficult to monitor what police personnel are sharing on these devices. The force allows the use of encrypted apps on its devices.

The Metropolitan Police Service has a comprehensive social media (standards) policy. It provides guidance to the workforce. It states that officers and [staff](#) should meet the standards of professional behaviour when using or accessing social media and online platforms for policing purposes or when off duty. It clearly explains the consequences of breaching the policy.

The [directorate of professional standards \(DPS\)](#) and the ACAC provide training and guidance to the workforce about the risks associated with social media use. This includes the standards of behaviour expected when using encrypted apps on either personal or force-issued devices. Most officers and staff we spoke to had a good awareness of the force's policy and expectations.

Artificial intelligence

Artificial intelligence (AI) offers an opportunity to improve police performance and productivity. But its use is contentious. The [National Police Chiefs' Council](#) is addressing concerns by taking part in [a research project, PROBabLE Futures](#), to make sure its use is responsible and transparent.

Some forces are exploring how AI can create efficiencies. This includes trialling AI in [contact centres](#) to help manage calls from the public, to develop transcription and translation tools and to examine large datasets to identify suspected [child](#) exploitation offences.

But there are risks associated with using AI in policing. For example, some forces have identified officers and staff using external AI-powered apps to help them write reports and witness statements. This increases the risk of non-compliance with security policies and legislation. Accessing these apps could also result in officers and staff sending sensitive data from police IT systems to their personal email addresses.

To prevent misuse of AI, forces should recognise the emerging risks and give guidance on appropriate use to their officers and staff.

The Metropolitan Police Service recognises the data security risks associated with misuse of AI. For example, its ACAC analysts recorded it as an emerging risk in the force's corruption [strategic threat assessment \(STA\)](#), which we describe in [the 'Identifying corruption threats' section](#). The ICT department has arranged for external online AI apps to no longer be accessible on force devices.

But the force has detected that some personnel are breaching data security by emailing information to their personal email accounts and using an AI app to create police reports. At the time of our inspection, the counter-corruption executive steering group, chaired by the ACAC commander, had recently approved a recommendation to update policies to address AI misuse.

The force has published a framework for the responsible use of AI. It outlines ethical and legal standards when using AI. But it doesn't include specific guidance to help personnel avoid breaching data security when using AI in their roles. And we found that officers and staff had only limited awareness of the data security risks associated with the misuse of AI.

Having identified the corruption risks associated with AI, the force should take immediate steps to raise awareness among its workforce. And it should update any relevant force policies without delay.

Tackling potential corruption

Area for improvement: The force needs to improve how it uses intelligence to help it prevent corruption

The force should make sure that:

- it carries out regular and intrusive reviews of its gifts and hospitality register so that the corruption compliance team (CCT) can make sure that no aspect creates a corruption risk; and
- it strengthens its business interest arrangements so that corruption-related [intelligence](#) informs all business interest authorisation decisions.

When a gift or hospitality is accepted by a member of the workforce, they must record a rationale. This has to be approved by either their line manager, the local professional standards unit or their [basic command unit](#) or operational command unit commander.

But none of these have access to any corruption-related intelligence held by the [anti-corruption and abuse command](#) to help inform their decision.

CCT [personnel](#) examine entries on the gifts and hospitality register to look for obvious anomalies and risks. But they don't analyse patterns of gifts or hospitality offered or given to any person or team. And the force doesn't consider whether there may be any concerns about the intentions of any donors. It doesn't, for example, check if there is any intelligence to suggest that they may be external corruptors.

The CCT authorises business interests with or without conditions or refuses the application. The CCT passes any applications it considers contentious to the anti-corruption and abuse command commander for a decision. But the force doesn't routinely check for any corruption-related intelligence held on an applicant before authorising a business interest. This is a surprising omission and a significant corruption risk. Corruption-related intelligence should inform every business interest authorisation decision.

Intelligence

Sources of corruption-related intelligence

The Metropolitan Police Service records its corruption-related intelligence on a confidential IT system managed by the ACAC intelligence bureau. Between 19 July 2024 and 18 July 2025, the force recorded between 100 and 150 items of corruption-related intelligence on average per month. However, there are numerous other IT systems across the force and within the ACAC itself that also hold information relevant to corruption investigations. This means that the corruption-related material about a person can be fragmented across numerous systems. These systems aren't integrated, and the vast majority of personnel have limited or no access to some of them. We describe the steps the force is taking to overcome these difficulties in [the 'Lack of integration of IT systems' section](#).

The force proactively looks for corruption-related intelligence as a matter of routine. The intelligence bureau uses a variety of tactics and systems to carry out this work. As we explained in [the 'Use of IT monitoring software to tackle corruption' section](#), the DET has developed numerous methods of using its IT monitoring capability to look proactively for corruption.

We examined 150 items of corruption-related intelligence. We found 19 items that were the result of proactive intelligence work. These included data protection offences, inappropriate and racist language shared on a force-issued mobile phone and suspected [abuse of position for a sexual purpose](#). This latter case resulted in the force dismissing the officer without notice and placing them on the [barred list](#).

[When we inspected the force's anti-corruption arrangements in 2022](#), we said that its lack of proactive work to gather corruption-related intelligence was a [cause of concern](#). We later closed the cause of concern, and it is encouraging to see that the force is continuing to develop well in this area.

Members of the workforce have several channels to anonymously report corruption or wrongdoing. These are:

- Right Line, an internal phone line direct to [on-call](#) intelligence bureau personnel;
- Integrity, a phone and online system managed by [Crimestoppers](#);
- [Hotline](#), a further phone and online system managed by Crimestoppers; and
- Signa, an internal intranet system for personnel to report cultural issues and behaviours that fall short of misconduct or corruption.

Hotline is primarily for use by members of the public, but sometimes police personnel use it. The Metropolitan Police Service was the first force to provide an anti-corruption hotline for the public. And Crimestoppers has now extended it nationally.

The force told us that between 1 January and 31 December 2023, it received 518 reports through Right Line. It received 633 reports through Integrity and 450 reports through Hotline. This is a total of 1,601 reports.

Between 1 January and 31 December 2024, the force received 168 reports through Right Line. It received 605 reports through Integrity and 600 reports through Hotline. This is a total of 1,373 reports.

And between 1 January and 20 October 2025, the force received 126 reports through Right Line. It received 477 reports through Integrity and 334 reports through Hotline. This is a total of 937 reports.

The force told us that its IT monitoring software automatically deactivated when police personnel used confidential reporting channels. This should reassure those making the report that they can't be identified. Officers and staff that we spoke to had a good understanding of the different channels available, which is reflected in the high volume of reports received.

The force gathers corruption-related intelligence from a variety of sources. In 39 of the 150 corruption-related intelligence cases we reviewed, we found that police personnel reported the intelligence using a confidential reporting channel. In 41 cases, personnel directly reported the corruption intelligence to the intelligence bureau. And in 12 cases, members of the public made the reports. Further sources of corruption-related intelligence included external agencies, self-referrals, [covert human intelligence sources](#) and other forces or law enforcement agencies.

The force also told us about Operation Sentinel, its continuous integrity screening programme. This has been in place since June 2025. Every 24 hours, the force carries out an automated scan of all of its crime records, criminal intelligence, reported incidents and custody records. It compares the results against HR data for its entire workforce.

The intelligence bureau is alerted if any officers or staff come to police attention or if there has been an incident at their home in the force area. The force told us of a recent example when Operation Sentinel identified a member of police staff who had been given a drug-related warning at a music festival in London but hadn't reported the matter. The person resigned immediately after the force questioned them about the incident.

Random drug testing

The force has a substance misuse and testing policy. The policy allows it to randomly drug test all police officers and staff members in certain drug-related and safety-critical roles. These include roles such as those involving contact with the public or driving vehicles.

The force told us that in the three years before our inspection, it carried out 2,935 random drug tests. Of these, eight were positive, and in every case the person either resigned or was dismissed. This extensive drug testing sends a clear message to the workforce that the force won't tolerate misuse of drugs.

Police corruption categorisation

The counter-corruption (intelligence) APP lists 12 categories of corruption-related intelligence. Forces should all use these categories when recording intelligence. This will help them identify their biggest corruption threats. It will also provide more accurate data to better inform regional and national analysis of police corruption.

Forces should make sure they accurately categorise all items of sexual misconduct intelligence. For example, forces should only record a sexual misconduct case as abuse of position for a sexual purpose if it involves a member of the public.

We found that the Metropolitan Police Service didn't always correctly categorise corruption-related intelligence in line with the APP. Of the 150 intelligence files we examined, intelligence bureau personnel wrongly categorised 11 items of intelligence. They should take more care.

Identifying corruption threats

Counter-corruption strategic threat assessment

The counter-corruption (intelligence) APP states that all forces should produce an annual counter-corruption STA detailing the corruption threats they face.

At the time of our inspection, the Metropolitan Police Service had produced a counter-corruption STA using data from 1 April 2024 to 31 March 2025. It analyses the corruption risks that the force faces, including some emerging risks.

But the STA isn't clear enough about what risks the force has assessed as its highest priorities. The STA would also benefit from further analysis to identify locations where different types of corruption activity are more prevalent.

In addition to the annual STA, ACAC intelligence bureau analysts prepare a quarterly report. They analyse trends in corruption-related intelligence and compare them to data in previous quarters. They give each corruption theme a 'risk prioritisation' score, based on the volume of intelligence reports received and the nature of that intelligence. The highest risks are sexual misconduct and theft/fraud. The report includes analysis of data on each corruption type by BCU and OCU area. This is an important feature due to the size and complexity of the force area.

But the STA and the quarterly report contain very little analysis of the threat from external corruptors. This is surprising as the force assesses the threat of infiltration and inappropriate associations as medium risk.

The force would greatly improve its STA by including the quarterly report's in-depth analysis. It could provide the force with a far richer picture of its corruption risks and trends. We encourage the force to incorporate this additional analysis when it produces its next STA.

During our inspection, we found that the ACAC hadn't briefed the [force vetting unit](#) on the risks in the latest STA. Briefing the force vetting unit is important so that its personnel consider the main corruption threats facing the force when making vetting decisions. The force told us that it hadn't published a redacted version of the STA on its intranet. It should do so to raise awareness across the workforce of the current corruption threats.

The force told us that every two years, it supplies a copy of its STA to the South East [Regional Organised Crime Unit](#). This helps to inform the national analysis of police corruption.

Counter-corruption control strategy

The Metropolitan Police Service doesn't have an effective counter-corruption [control strategy](#).

The force showed us its one-page counter-corruption control strategy. The threats listed on the control strategy are the same as those identified in the STA. But the control strategy lacks detail. It merely lists and briefly describes each corruption threat.

Implementation plan

The force's counter-corruption implementation plan is more detailed. It comprises a spreadsheet covering each of the corruption threats identified in the STA. For each threat, the plan lists a series of control measures under the headings 'intelligence', 'prevention', 'enforcement' and 'communication'.

But surprisingly, there are very few control measures within the plan aimed at addressing the threat from organised crime. And neither the control strategy nor implementation plan make any reference to plans to collect intelligence in respect of any of the emerging corruption risks identified in the STA.

The implementation plan records the designated lead for each threat. They are responsible for overseeing the control measures. And each separate action in the plan has a named person responsible for completing it. The counter-corruption executive steering group, chaired by the ACAC commander, monitors progress against the plan on a quarterly basis. But we found that not all actions had a completion date. This makes it more difficult to hold the named leads to account. We noted action updates were often merely recorded as 'ongoing'. And some had no updates recorded against them.

The force should make more effective use of the STA, control strategy, implementation plan and its quarterly analysis reports to prioritise activity against the main corruption threats it faces.

We found weaknesses in some of the force's arrangements to tackle the main corruption risk that it has identified in its STA – sexual misconduct. We comment further on this in the rest of this chapter. For example, we comment on the force's arrangements for managing some sexual misconduct-related intelligence, widening investigations of [prejudicial and improper behaviour](#) cases and making sure that all officers and staff complete training on abuse of position for a sexual purpose. The force may be missing opportunities to effectively tackle corruption. This could put the public at risk.

We identified effective use of the STA as an area for improvement in our 2018/19 PEEL inspection. And it was a recommendation in our 2022 national report on vetting, misconduct and misogyny.

Exchanging information on people who may be a concern

Where forces have [people intelligence meetings](#), they can help to identify officers and staff who may pose a corruption threat. The meetings bring together representatives from different parts of the force to exchange information on those who may be of concern. This can include, but isn't limited to, information relating to:

- management of unsatisfactory performance;
- sickness management and absenteeism;

- public complaints;
- corruption-related intelligence;
- internal misconduct cases;
- internet use;
- unusually high overtime and expenses;
- business interests;
- debt management problems;
- inappropriate use of force-issue credit cards; and
- excessive use of force phones, including text messages.

Police personnel discussed in these meetings can often appear in more than one category. Because several departments often hold relevant information, forces can easily miss corruption risks.

The Metropolitan Police Service doesn't have an established force-wide people intelligence meeting. This is entirely understandable due to the size of the force and the number of people it would need to discuss each month.

Instead, the force has alternative processes to support the presentation and exchange of information on those who may be of concern. This helps the force to identify individual officers and staff or teams who may present a corruption risk.

The force requires every BCU and OCU to hold a monthly professional standards review meeting (PSRM), chaired by the chief inspector (professionalism). Attendees at PSRMs include members of the local professional standards unit (PSU), line managers, HR and representatives from the Police Federation and staff trade unions.

The force holds PSRMs to exchange relevant information on people who may pose a misconduct or corruption risk. In line with the force's 'public health' prevention approach to misconduct, PSRMs aim to agree on early interventions to mitigate any risk.

Misconduct and complaint data from [Centurion](#), as well as some lower-level corruption-related intelligence, informs the PSRM. And the results of each meeting are communicated to the ACAC intelligence bureau and discussed at the ACAC daily intelligence tasking meeting. At the time of our inspection, the intelligence bureau had recently started to maintain a central PSRM database for the force.

Representatives from the DPS, ACAC and the force vetting unit don't attend PSRMs. There is also no representation from the directorate of legal services or the learning and development department. And the force told us that HR representatives often didn't attend. In our view, the limited attendance at PSRMs may restrict their effectiveness.

ACAC senior leaders also brief BCU and OCU commanders on any emerging corruption themes or patterns. Intelligence bureau analysts produce [problem profiles](#) that raise awareness of any specific corruption risks in a BCU or OCU. This allows local commanders to introduce control measures, such as additional bespoke training or guidance for teams, or line manager interventions to reduce the risk.

The DPS holds a daily management meeting. Representatives from across the DPS, including ACAC senior managers, attend. They discuss complaints and conduct cases that have been reported in the previous 24 hours. And they share time-critical information, such as arrests of members of the workforce, disciplinary proceedings, court proceedings and media interest.

Partnership working to identify potential corruption

In our 2018/19 PEEL inspection, we identified that the Metropolitan Police Service needed to improve how it built effective relationships with individuals and organisations that supported and worked with vulnerable people. And in [our 2022 national report 'An inspection of the Metropolitan Police Service's counter-corruption arrangements and other matters related to the Daniel Morgan Independent Panel'](#), we said that the force's lack of concerted effort to establish relationships between the DPS and organisations that support vulnerable people was a cause of concern.

The force has responded well. It now works with a variety of different external agencies and organisations that support vulnerable people who may be at risk of abuse of position for a sexual purpose. And it uses several methods to do so.

Many cases of sexual misconduct, including allegations of abuse of position for a sexual purpose, are investigated by [domestic abuse](#) and sexual offence team (DASO) officers. Dedicated DASO victim support officers support victims directly. And they work alongside organisations such as [Solace Women's Aid](#), a London-based charity that supports victims of domestic and [sexual abuse](#), as well as [independent sexual violence advisers](#) and [Rape Crisis](#) centres.

The force told us that DASO team officers had given presentations to organisations such as the violence against women and girls [independent advisory group](#), NHS services and the [London's Victims' Commissioner's](#) Victim Voice Forum. These presentations help staff in the organisations to recognise the warning signs of abuse of position for a sexual purpose and understand how to report corruption-related intelligence.

The ACAC commander holds a quarterly external scrutiny panel for agencies to review a selection of investigations. The panel includes agencies that provide support for domestic abuse victims and a charity that provides support for sex workers.

During our file review of 150 items of corruption-related intelligence, we found two examples of intelligence reports relating to suspected abuse of position for a sexual purpose from agencies the force works with. In one case, the officer was arrested. This is encouraging and demonstrates the value of the force continuing to build trust with these agencies.

Managing corruption threats

Developing corruption-related intelligence and investigations

The ACAC intelligence bureau collates all corruption-related intelligence for the Metropolitan Police Service. The force holds a daily intelligence tasking meeting to review the intelligence collated in the preceding 24 hours. Most ACAC teams have representatives at the meeting.

Each item of corruption-related intelligence is discussed, assessed and then allocated for action to one or more of the following teams:

- the intelligence bureau core desk;
- the complaint resolution unit;
- the DASO team;
- the specialist investigation unit;
- the tactical team; or
- one of the four [covert](#) investigation teams in the ACAC.

During our review of 150 items of corruption-related intelligence, we found 20 examples of ACAC investigators not carrying out all appropriate actions to develop that intelligence effectively. These included instances of failing to carry out sufficiently intrusive IT audits, overlooking a possible witness and not enquiring further into a possible unregistered business interest.

Of the 150 corruption intelligence files we reviewed, 64 cases led to an anti-corruption investigation. Investigators mostly completed all reasonable lines of enquiry before the case was finalised. But we found that the force missed investigative opportunities in four cases. These included:

- a lack of IT auditing of internet use at work in relation to a business interest;
- not giving enough consideration to a forensic examination of a victim's bag following a workplace theft; and
- failing to carry out [automatic number plate recognition](#) or [CCTV](#) enquiries in a [stalking](#) case.

In cases that involve [prejudicial and improper behaviour](#), investigators should consider whether the intelligence may be an indicator of a wider pattern of behaviour. But we found 21 prejudicial and improper behaviour cases where investigators hadn't extended the scope of their investigation enough to look for patterns. The cases included allegations of workplace bullying and misogynistic behaviour, abuse of position for a sexual purpose, sexualised domestic abuse and sexual touching of colleagues. The investigators may have missed opportunities to identify additional victims or further offences.

This is disappointing. The force has identified sexual misconduct as its highest corruption threat. And since 2023, as part of Operation Onyx, it has invested significant resources in reviewing historical domestic abuse and sexual offence investigations into officers. This makes it all the more surprising that the force hadn't investigated these more recent sexual misconduct cases more thoroughly.

Some, but not all, ACAC investigators use investigation plans. If every ACAC investigator and intelligence personnel consistently used structured, bespoke plans for all intelligence developments and investigations, it would help supervisors check that they are following all reasonable lines of enquiry. And supervisors would be less likely to finalise cases before investigators have completed all enquiries.

Overall, it was disappointing to find that the force hadn't taken all the appropriate steps to fully develop the intelligence or thoroughly investigate these cases. This is a higher proportion of cases than we see in most other forces. The force could have avoided this with better use of investigation plans and more effective supervisory oversight of these cases.

Effective use of investigation plans to improve the quality of counter-corruption investigations was part of a recommendation in our 2022 national report on vetting, misconduct and misogyny. And carrying out all reasonable wider inquiries when dealing with reports of prejudicial and improper behaviour was also a recommendation in that report.

The force consistently refers potential corruption cases to the [Independent Office for Police Conduct](#), in line with [statutory guidance](#). During our review, we found just two cases that the force should have referred but hadn't. These were an allegation of sexual harassment in the workplace and a suspected abuse of position for a sexual purpose case. We consulted with the Independent Office for Police Conduct. It confirmed that the force should have referred these two cases or there should at least have been a pre-referral discussion.

Lack of integration of IT systems

In addition to the ACAC intelligence bureau's database, there are numerous systems across the force and within the ACAC itself that hold information relevant to corruption investigations. The force manages different types of intelligence development or investigation on a variety of different IT systems. And ACAC teams manage some individual intelligence developments and corruption investigations simultaneously across two or more unconnected systems. None of these systems are integrated.

The force also told us that the overall lack of integration created difficulties when researching and analysing corruption-related intelligence and other professional standards data. As mentioned in [the 'Considering relevant information' section](#), to overcome this, the integrity screening unit developed an IT solution known as the Combo Checker.

Researchers and investigators can use this Microsoft SharePoint-based tool to search 25 different force IT systems at the same time. They can identify if there is any information held about people in relation to:

- complaints and conduct history on Centurion;
- live conduct matters, complaints and other matters on Centurion;
- live [written warnings](#) and [final written warnings](#) on Centurion;
- restrictions and suspensions on Centurion;
- IAU risk management conditions, including high-risk declarable associations;
- 'learning through reflection' and [reflective practice review process](#) history;
- vetting data held on the HR system;
- unsatisfactory performance information;
- business interests;
- cadet management; and
- firearms authorisations.

They can also use the Combo Checker to search some, but not all, of the ACAC's corruption databases. It can't be used to search external IT systems, such as the [Police National Database](#) and [Police National Computer](#).

At the time of our inspection, the force was also trialling an AI-based system supplied by a company based in the USA. The force told us that this system was "ingesting data from across multiple systems". Due to its sensitive nature, some of the ACAC's corruption information was excluded.

We assessed the force's use of this system. It presents a good opportunity for the force to improve the management and analysis of its data. We look forward to reviewing the force's progress.

These IT initiatives help the force to search for information across a range of systems. But significant gaps remain.

The force's approach to managing corruption records is fragmented. In our view, this is a direct consequence of the numerous teams across the DPS and ACAC using such a convoluted arrangement of disparate and non-integrated IT systems.

Of the 150 corruption intelligence files we reviewed, we found 18 cases where investigators didn't adequately record all aspects of the force's response. This included very limited rationale for a decision to treat a case involving racism through the reflective practice review process. Investigators also recorded a poor rationale for a decision not to continue with gross misconduct proceedings after someone had resigned. We also found that there was a lack of follow-up and outcome information recorded when the ACAC intelligence bureau passed cases outside the DPS or allocated them to local PSUs to deal with.

'With cause' drug testing

Where the force has intelligence about drugs misuse, the substance misuse and testing policy allows it to carry out 'with cause' drug testing of all police officers and staff. The force told us that over the three years before our inspection, it carried out 132 'with cause' drug tests, of which 27 were positive. In each case the person either resigned or was dismissed.

During our file review, we found four examples where the force had used 'with cause' drugs testing in appropriate cases.

Ethical interviews

There may be circumstances where forces have lawfully obtained intelligence, but they can't use it in criminal or misconduct proceedings. If the force can disclose the intelligence to the person involved, it may carry out an [ethical interview](#) with them. This gives the person an opportunity to clarify matters. It may also allow the force to implement measures to address any risk or vulnerability to corruption.

The force told us that it regularly used ethical interviews to address unresolved corruption-related concerns. But during our corruption file review, we saw four examples where ACAC investigators hadn't held ethical interviews when it would have been appropriate to do so. Three of these were sexual harassment cases and one was inappropriate messaging on social media.

Service confidence

Sometimes forces can't disclose intelligence to the person concerned. This is because disclosure of the intelligence or information is prohibited by law and/or would put investigations, police tactics or people at risk.

A service confidence policy can give forces a framework to manage these situations sensitively and impose restrictions on the person. A force may prevent an officer from having contact with the public while on duty, for example. The policy should create an appropriate balance between the needs of the force and the rights of the person. It should include regular reviews and a right of appeal to the chief constable against any restrictions that the force may impose.

Rather than a service confidence policy, the force has a well-established integrity assurance policy. It applies to any officer or member of staff who:

- becomes subject to an adverse judicial finding following a criminal trial, civil trial or other judicial proceedings;
- is evidentially tainted because of receiving a criminal conviction or an [out-of-court disposal](#), relevant court finding or misconduct finding; or
- is the subject of other [adverse information](#) or intelligence.

At the time of our inspection, the force told us that the IAU was actively managing 324 members of the workforce in line with this policy. IAU personnel had assessed 161 of these as high risk and 163 as medium risk. In each case, the force had held a formal integrity assurance meeting to determine appropriate risk-management measures, such as restriction of duties or role.

In the three years before our inspection, the IAU held 271 such meetings for personnel assessed as high risk. The force told us that it held 103 of these meetings during 2025. But at the time our inspection in November 2025, the IAU had 45 cases waiting for an integrity assurance meeting. The force said lack of resources had caused this delay.

Risk management

If forces suspect that a police officer or member of staff may abuse their position for a sexual purpose, they should assess the risk that individual poses. Forces tend to do this using a risk matrix. This prompts the assessor to consider all the circumstances and record the findings. Counter-corruption units then categorise each case as low, medium or high risk.

The types of behaviour that would trigger a force to assess someone against the risk matrix include:

- inappropriate behaviour with or towards colleagues;
- inappropriate sexual comments to colleagues or to the public in general;
- making a large number of calls or sending a large number of texts, instant messages or emails to vulnerable people;
- sending emails or any messages of a sexual nature; and
- intelligence or information about inappropriate sexual behaviour off duty.

If a force has assessed an individual as being medium or high risk, they should receive additional monitoring.

The Metropolitan Police Service doesn't use separate risk registers to monitor members of the workforce who may pose a corruption risk.

The IAU proactively identifies these people through intelligence reports, analytical work, reports of misconduct and information from public complaints. The unit [flags](#) personnel on either the DPS database, Centurion or the ACAC intelligence bureau database, depending on the corruption type and assigned risk level. It does this for personnel suspected of posing a threat of sexual misconduct. It also does this for personnel who may pose other types of corruption risk, including, for example, someone with financial vulnerabilities due to a gambling addiction.

The IAU carries out a [risk assessment](#) against each person. Rather than using a formal scoring matrix, it bases this assessment on research into any known corruption-related intelligence and on professional judgment. It categorises the level of risk that each person poses. The IAU records any action the force takes to mitigate the risks.

But we found that the force's process to manage personnel who come to notice for any sexual misconduct-related matters wasn't effective in several critical areas.

The IAU doesn't carry out a risk assessment or set control measures until an investigation has concluded. This process is flawed. It may prevent the force from identifying corruption risks early enough to intervene effectively. This approach is only justified if it is clear from the outset that the suspect will be suspended without delay and remain so until they are dismissed.

Of the 150 corruption intelligence files we reviewed, we found 13 cases where the force hadn't taken the action we would expect. It hadn't assessed the level of sexual corruption risk the person posed, and the IAU hadn't flagged or actively managed them.

In 8 of the 13 cases, members of the workforce had flagged the person using the force's confidential reporting lines. The cases were finalised without any criminal or misconduct proceedings. But as the IAU hadn't flagged the cases or risk assessed them, the force wasn't doing anything to mitigate the risks posed. The cases included personnel reported for the sexual assault of junior colleagues, sexualised domestic abuse and harassing female personnel.

The force told us that it had 123 cases awaiting assessment by the IAU. It didn't know how many of these were sexual misconduct-related cases that it had finalised following a criminal or misconduct investigation. This is surprising and concerning. We encourage the force to consider putting in place a flagging system so that it can better track sexual misconduct-related cases.

The force should review the way that it manages this type of intelligence. It told us that the IAU was notified of all people who come to notice for any sexual misconduct-related matters. But the IAU should then make sure that it carries out its risk assessment at the outset so that it can apply any control measures deemed necessary without delay.

Assessing all intelligence relating to sexual misconduct and taking action to minimise risk was a recommendation in our 2022 national report on vetting, misconduct and misogyny.

Training on abuse of position for a sexual purpose

The force told us that it recognised abuse of position for a sexual purpose as serious corruption.

The force told us that the prevention and engagement team regularly gave training sessions to its officers and staff. The training has a specific section on abuse of position for a sexual purpose and includes the warning signs to look out for.

The force has made the [College Learn](#) abuse of position for a sexual purpose training mandatory. At the time of our inspection on 1 November 2025, force data showed that only 61 percent of all police personnel had completed it. This is disappointing.

The force told us about other training that it provided to the workforce that covered abuse of position for a sexual purpose. And, generally, we found that members of the workforce had an adequate understanding of it. But some officers and staff we spoke to were unclear whether it referred to both internal and external improper relationships. The force should do more to make sure that its officers and staff comply with this mandatory training requirement.

Sexual harassment

The Metropolitan Police Service has adopted the National Police Chiefs' Council sexual harassment policy in line with our national recommendation.

In line with the [Equality Act 2010](#) and the [Worker Protection \(Amendment of Equality Act 2010\) Act 2023](#), all employers, including police forces, have a legal duty to take 'reasonable steps' to prevent sexual harassment and create a safe working environment.

In October 2025, to comply with this legal obligation, the force completed a risk assessment relating to sexual harassment. The force-wide assessment includes guidance for BCUs and OCUs to complete their own local risk assessments.

Capacity and capability to investigate corruption

The Metropolitan Police Service's ACAC is by far the largest counter-corruption unit in England and Wales. Its size reflects the scale and complexity of the challenges faced by the force.

The ACAC comprises a number of highly specialised teams. These teams work well together to provide a comprehensive force capability to tackle all aspects of police corruption. Different ACAC teams manage corruption-related intelligence, proactively monitor individuals suspected of posing corruption risks, investigate sexual misconduct and use a range of covert methods to address very high-level and serious corruption.

The ACAC intelligence bureau is led by a detective superintendent and has about 140 officers and staff. It comprises a number of sub-units, which are:

- a core desk;
- a confidential reporting team;
- a research and analysis team;
- the IAU;
- an intelligence management unit;
- a tactical team;
- the DET; and
- an electronic-discovery unit.

The investigative arm of the ACAC comprises the anti-corruption command (ACC) and the DASO team.

A detective superintendent leads the ACC. It has three detective inspectors, each with teams comprising two detective sergeants and ten detective constables. The ACC carries out covert investigations to address high-level corruption, which includes firearms offences, drugs supply and other serious criminality.

A team of experienced misconduct investigators supports the ACC. This team, comprising a sergeant and four constables, provides expertise in managing misconduct matters. It has an important role when the force is pursuing gross misconduct proceedings, particularly in complex criminal cases where the ACC may have deployed covert techniques.

The ACC's investigations are also supported by a number of smaller units that provide specialist capabilities.

The DASO team is led by a detective superintendent and a detective chief inspector. It consists of four teams, each comprising a detective inspector, two detective sergeants, ten detective constables and two police officers. And the DASO team has six dedicated victim support officers, led by a sergeant. The force formed the DASO team several years ago to focus on all alleged sexual misconduct-related cases, including criminal offences, such as rape and police-perpetrated domestic abuse.

Most of these teams told us that they had sufficient personnel to meet demand and carry out their work effectively. The exceptions were the DASO team and the IAU.

The force told us that the DASO team was struggling to meet demand. At the time of our inspection, it was operating at about 70 percent capacity. The higher-than-normal number of prejudicial and improper behaviour ‘missed investigative opportunities’ that we found during our corruption file review may be due to this lack of resources. We explain this in more detail in [the ‘Developing corruption-related intelligence and investigations’ section](#).

The IAU is responsible for assessing the risks posed by people in the force and implementing control measures to mitigate these risks. It consists of a detective inspector, 2.5 full-time equivalent detective sergeants and 11 constables. This level of resourcing appeared to be insufficient to match demand. We found that the IAU was significantly behind with its risk assessments for sexual misconduct-related intelligence and its assurance of declarable association risk assessments completed by BCU/OCU professionalism leads. We explain this further in the sections on ‘[Risk management](#)’ and ‘[Declarable associations](#)’.

Police officers and staff in the various units have an impressive range of experience and specialist skills. They have backgrounds in protecting vulnerable people, [serious and organised crime](#) investigation, counter-terrorism and intelligence.

Officers in both the ACC and the DASO team are experienced investigators. All ACC investigators and the majority of DASO team investigators are [professionalising investigations programme](#) level 2 accredited. But none of the investigators in either unit have attended the [College of Policing](#)’s corruption investigator development programme. The force has supported some of its detective sergeants and detective inspectors to complete the lead corruption investigator programme. But it relies on corruption investigators learning from colleagues and locally provided training. The force told us that this was because of the cost.

Some, but not all, members of the ACAC intelligence bureau have gained accreditation under the College of Policing’s [intelligence professionalisation programme](#). And some, but again not all, of the remainder are working towards this accreditation. The force should review its training provision for intelligence bureau personnel to make its approach more consistent.

During our inspection, the force told us that it was planning to restructure the DPS, including the ACAC, as part of its professionalism transformation programme. The planned restructure aims to improve the force’s ability to move resources across reactive and proactive functions to better meet changing demand. The force also aims to reduce the number of vacancies in the DASO team.

The force’s rotation policy aims to improve the experience of frontline officers. About 60 percent of the ACAC’s corruption investigators will soon be eligible to move to more mainstream detective duties as they will have spent ten or more years working in a specialist department. A management board outside the DPS will decide how many will be rotated.

During our inspection, we heard from ACAC personnel who were concerned about the application of the force's rotation policy. They were worried that the policy would result in a loss of experience. We share some of their concerns. We noted there wasn't a training budget to upskill new corruption investigators to equip them for the role. And the force acknowledged the likely difficulty in securing applications from suitably experienced investigators. People with experience are likely to be rotated themselves or are unlikely to be released from specialist units that are suffering a similar loss of experience.

We understand the rationale for the force's rotation policy. And we support it. But a note of caution is warranted. The force should take great care that applying the rotation policy doesn't reduce the ACAC's impressive specialist capabilities and capacity to tackle and root out corruption.

Specialist resources

ACC officers, including the senior management team, are experienced in covert law enforcement. The ACC has good working relationships with the National Crime Agency and can access additional support or specialist equipment if required.

The ACAC has its own trained operational security advisors. And the ACC has trained three of its investigators as operational security liaison officers. This informs the ACC's assessment of the police corruption and operational security risks associated with organised crime groups.

The ACC frequently uses [intelligence-led integrity tests](#) as a covert tactic. The force has a dedicated unit that helps manage the tests. During our corruption file review, we saw an example of the ACC and the intelligence-led integrity test team working together to carry out a test. And they were planning another one at the time of our inspection.

Policies designed to prevent corruption

Clear and concise corruption prevention policies help forces to protect themselves from corrupt activity. But they can't guarantee to prevent corruption or, in themselves, stop corrupt practice. They provide guidance on how police officers and staff should behave. Policies should clearly state what is expected of personnel and what actions they should take to protect themselves and the force from corruption.

The counter-corruption (prevention) APP sets out what policies forces should have and gives guidance on their content. We examined policies on:

- declarable associations;
- business interests; and
- gifts and hospitality.

Declarable associations policies cover how the force should manage the risks related to people who officers and staff may associate with, for example, criminals, private investigators or members of extremist groups. The policies should require officers and staff to disclose such associations.

Business interests policies should state when the force allows or doesn't allow officers and staff to have other jobs, interests or activities. Policies should explain how the force will manage any associated risks.

Gifts and hospitality policies should cover the circumstances in which police officers and staff should accept or reject offers of gifts or hospitality.

The force's corruption prevention policies generally reflect APP guidance. However, we found shortcomings in the way it applied some aspects of these policies.

Declarable associations

The Metropolitan Police Service has a generally effective process to manage declarable associations. But we found that there were issues of timeliness in relation to the risk assessment assurance process.

The declarable association policy, published in May 2024, applies to all officers and staff and non-police personnel. It requires them to report any associations with, for example, criminals or private investigators. Since we inspected the force in 2022, the force has extended its declarable association policy to include members of extremist groups and people who work as journalists.

At the time of our inspection, the force had completed a survey of its workforce about a possible change to the policy. This would require officers and staff to report their membership of any organisation that is hierarchical and requires members to support and protect each other, which raises questions about the impartiality of officers who are members.

The force told us that it received broad support for its proposal and intended to implement the change in policy in early December 2025. We applaud the Metropolitan Police Service for this initiative. We recognise that the force is making this change to improve transparency and address perceptions of unfairness.

The ACAC intelligence bureau manages the register for low and medium-risk declarable associations. The IAU manages those that are high risk. The force requires officers and staff to notify their local PSU via email of any declarable associations using a templated form. Additionally, some new applicants may disclose such associations during the vetting process. The force may also identify declarable associations when personnel notify it of changes in circumstance or through ACAC intelligence gathering.

The local PSU carries out intelligence research on the declared associate. It doesn't research corruption-related intelligence held by the intelligence bureau. The chief inspector (professionalism) then uses a tool to assess the risks posed by the declarable association. The tool considers a range of aggravating and mitigating factors in relation to the associate and the relationship the member of the workforce has with them. Using the tool, the chief inspector assesses the association as high, medium or low risk. Use of the tool relies on professional judgment of the risk factors rather than use of a scoring system.

The PSU sends the completed risk assessment to the intelligence bureau. Depending on the level of risk, either the IAU or the intelligence bureau carries out further research on the intelligence bureau's database. This includes research on any corruption-related intelligence held about either party. This allows supervisors in those units to make an informed assessment on the final level of risk.

The force told us that between 1 January and 31 December 2023, it recorded 2,752 declarable associations. Of these, it assessed 39 as high risk, 164 as medium risk and 2,549 as low risk.

Between 1 January and 31 December 2024, it recorded 2,561 declarable associations. Of these, it assessed 51 as high risk, 207 as medium risk and 2,303 as low risk.

Between 1 January and 6 December 2025, it recorded 2,092 declarable associations. Of these, it assessed 59 as high risk, 184 as medium risk and 1,849 as low risk.

Depending on the level of risk, the IAU or the local PSU may hold a risk management meeting and impose appropriate bespoke risk management measures, such as restrictions on postings, home working and use of IT.

The declarable association policy doesn't routinely require the IAU to inform the officer's or staff member's line manager about the declared association. However, it does state that personnel can inform their own line manager if they wish to do so. Where risk management measures are in place, the IAU will inform the line manager of the association and the measures imposed. This helps the line manager to monitor compliance with the measures.

At the time of our inspection, the force told us that the IAU didn't have enough resources to meet demand. As a result, there were 200 low and medium-risk cases yet to be researched. And there were 120 high-risk cases awaiting final risk assessment. The force has put some early risk management measures in place in these cases.

As a proactive check in support of the IAU, the DET monitors IT systems to identify any potential misuse in all cases relating to a declarable association. But as we mentioned in [the 'Use of IT monitoring software to tackle corruption' section](#), there are gaps in IT monitoring coverage that reduce the effectiveness of this as a reliable control measure.

We spoke to officers and staff about the force's declarable association policy. We found that they generally had an adequate understanding of the requirement to declare any associations linked to criminality. But most had only limited knowledge of the other types of associations that the policy requires them to declare.

Business interests

The force has a business interests policy. But its processes to manage business interests aren't effective.

The force requires members of the workforce who are seeking approval for a business interest to complete a digital online application form. This includes a description of the proposed activity, estimated time commitment, income and any potential conflicts or incompatibility with their role in the force.

The applicant's line manager can endorse the application, or otherwise, based on considerations such as sickness, absences, performance and any current conduct or complaint cases. The local PSU then considers the application. It adds any additional relevant information, which includes any records relating to the applicant on Centurion. The PSU then forwards the application to the ACAC corruption compliance team (CCT).

The CCT is responsible for managing the business interests register for the whole of the Metropolitan Police Service. It comprises a sergeant and three police officers.

The CCT can authorise business interests, either with or without conditions. It passes any applications that are contentious to the DPS OCU commander for a decision. The CCT informs the applicant and their line manager of the decision. It records all approved business interests on the force's integrated HR, payroll and finance system.

Despite it being part of the ACAC, the CCT doesn't routinely consider any corruption-related intelligence that is held on an applicant before authorising a business interest. This is a surprising omission and a significant corruption risk. Corruption-related intelligence should inform every business interest authorisation decision.

The force's business interests policy doesn't require officers and staff, other than chief officers, to obtain CCT authorisation to carry out unpaid voluntary work. Instead, personnel must seek approval from their line manager only. But line managers don't have access to the corruption intelligence held by the ACAC.

In our view, a force's business interests policy should extend to all voluntary work, particularly to roles that involve [safeguarding](#) responsibilities. And the decision to approve such work must also be informed by any corruption intelligence held by the force. It isn't appropriate for line managers to make these decisions.

The CCT maintains a database of all contentious approved business interests, those with conditions attached and any refused business interests. The CCT carries out checks to monitor compliance with any conditions imposed or refusal decisions. These checks are primarily led by intelligence.

It carries out some proactive compliance checks, but this is limited to desktop enquiries, such as social media checks.

When approving the business interest, the CCT advises successful applicants that they must reapply for approval after 12 months. This period is extended to three years when the business interest relates only to property rental. At the time of our inspection, the force told us that 39 renewal applications were with the CCT waiting for a decision. But, on checking the business interests register, we found that 953 approved business interests were overdue for renewal. And several had been overdue for a number of years. Some of the oldest cases went back as far as 2016.

The CCT was unaware of these cases. The team suggested that there may be data quality issues on the business interests register. But the force couldn't say with any certainty how many of these overdue renewals were still active business interests or how many of them should no longer be approved. This is a corruption risk.

The force subsequently reviewed the cases and found, as suggested, that many were the result of administrative errors. Nevertheless, the force told us that it found 350 renewals that were outstanding, which was still far too many.

The force told us that in 2023, it granted 69 business interests and declined 104 applications. In 2024, it granted 791 business interests and declined 134 applications. And between 1 January and 11 October 2025, it granted 1,359 business interests and declined 74 applications.

The force suggested that the increase in the number of business interest applications was due to a process it introduced in 2023. At that time, it introduced measures to improve workforce awareness.

During our inspection, we found that some officers and staff didn't have a full understanding of the force's business interests policy. We found that some were confused in relation to seeking approval for voluntary work.

Strengthening business interest monitoring procedures was recommendation 41 in our 2022 national report on vetting, misconduct and misogyny.

Gifts and hospitality

The force needs to improve some aspects of its process to manage gifts and hospitality.

Members of the workforce must submit notifications about gifts and hospitality using an online form. This applies to any gift or hospitality offered, whether accepted or declined. The notification creates an entry on a centrally held register. This includes:

- details of the gift or hospitality;
- its value;
- details of the person or organisation offering the gift or hospitality;
- whether it was refused or accepted; and
- a rationale if it was accepted.

Members of the workforce submit the form to their line manager, who decides whether or not they can accept the gift. In the more contentious cases, the force refers this decision to a chief inspector in the local PSU or to the BCU/OCU commander. But none of these have access to corruption-related intelligence held by the ACAC intelligence bureau to help inform their decision.

During our inspection, we examined a selection of entries on the gifts and hospitality register. We found that the register was comprehensive and up to date and that it had a healthy mix of acceptances and refusals. Acceptances had sufficiently detailed and bespoke rationale recorded against them. The register included entries from senior officers. The force told us that it published the register monthly on its public-facing website.

The CCT manages the register for the whole force. But individual PSUs can examine the register entries for their own specific BCU or OCU. And part of their role is to examine entries on the register to check that they are timely and comply with force policy. CCT members examine entries to look for obvious anomalies and risks. But there is no work to analyse patterns of gifts offered or given to any individual person or team. And neither the local PSUs nor the CCTs scrutinise whether the force has any concerns about the intentions of any donors of any gifts or hospitality. This includes, for example, if there was any intelligence to suggest that they may be external corruptors.

In 2023, the force recorded 496 gifts and hospitality applications, of which it declined 77. In 2024, it recorded 1,065 applications, of which it declined 128. And during 2025 up to the time of our inspection in November, it had recorded 657, of which it declined 67.

During our inspection, we spoke to officers and staff and found that they had an adequate understanding of the force's gifts and hospitality policy.

We examined some of the register entries relating to gifts accepted by the Royalty and Specialist Protection (RaSP) OCU. The RaSP OCU is often offered high-value gifts by visiting heads of state and other dignitaries. Therefore, it has produced additional guidance for its officers and staff. This guidance reminds RaSP officers that they must comply with the force's gifts and hospitality policy. We found that the local PSU regularly examined entries in the RaSP OCU's gifts and hospitality register.

But during our inspection, we found that RaSP officers sometimes accepted gifts with the intention that they would be later disposed of by the force. For example, the CCT told us about a cash gift of £17,500 that a RaSP officer accepted and recorded on the register. This is in direct contravention of the force's policy on gifts. The policy states that personnel must never accept cash gifts under any circumstances. Entries on the register indicated that the force intended to donate the full amount to charity.

At our request, the force demonstrated that it had disposed of the cash appropriately. But we found that the RaSP OCU's processes for managing such gifts weren't robust enough to prevent corruption risks. And records on the gifts and hospitality register about the eventual disposal of such gifts weren't detailed enough.

[Annual integrity review](#)

The force has a process in place for completing [annual integrity reviews](#) with all officers and staff. The process runs in parallel with annual performance development reviews. It serves as a reminder for personnel to report any change in circumstances, including any declarable associations or business interests.

The force told us that 81 percent of the workforce had completed a review. As we mentioned in [the 'Vetting reviews' section](#), at the time of our inspection, the force told us that it was planning to introduce a more comprehensive annual integrity and vetting review process in April 2026.

Operation Sentinel, the force's continuous integrity screening programme, which we mentioned in [the 'Sources of corruption-related intelligence' section](#), provides further assurance in relation to the workforce's integrity.

July 2026 | © HMICFRS 2026

hmicfrs.justiceinspectorates.gov.uk