HMICFRS

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

An inspection of vetting, misconduct, and misogyny in the police service

Contents

Foreword

Following the murder of Sarah Everard by a serving police officer, the then Home Secretary commissioned us to inspect the police's vetting and counter-corruption arrangements. This was to include assessing forces' abilities to detect and deal with misogynistic and predatory behaviour by police officers and staff.

Forces need effective systems to prevent unsuitable applicants from joining. No system is watertight so, inevitably, unsuitable applicants will slip through from time to time. And some who are assessed as suitable when they join may become unsuitable later in their career. When this happens, forces also need effective systems to identify these individuals and, if necessary, dismiss them.

Over the last decade, there have been many warning signs that these systems aren't working well enough. Some police officers have used their unique position to commit appalling crimes, especially against women. Some forces have repeatedly failed to implement recommendations – from us and other bodies – that were designed to prevent and detect such behaviour. We explain these more fully in Chapter 2 of this report.

Identifying unsuitable applicants should start during the recruitment process. Too often, this process is not rigorous enough. Some forces appoint applicants without seeking references from previous employers or checking their educational qualifications. Several forces have recently reintroduced final interviews into their recruitment process. But others still select applicants without assessing them in person first. Whether this will adversely affect standards remains to be seen, but initial indications are not reassuring.

The next opportunity to identify unsuitable applicants is the vetting process. This too needs to be more stringent. We examined 725 vetting files. In most cases, we agreed with forces' decisions to grant clearance. But we also found 131 cases where the decision was questionable at best. In these, we found officers and staff with criminal records, or suspicions that they had committed crime (including some serious crime), substantial undischarged debt, or family members linked to organised crime. In other cases, officers and staff had given false or incomplete information to the vetting unit. We also found officers who, despite a history of attracting complaints or allegations of misconduct, successfully transferred between police forces. This is wholly unsatisfactory.

In all these cases, forces had overlooked or downplayed the matter and cleared the applicants, often without any rational explanation for doing so. There were occasions when sound vetting rejections had been overruled, with dubious justification. We have concluded that many aspects of police vetting need to be clarified and strengthened.

As well as focus groups and interviews, we carried out an online survey of officers and staff. We received over 11,000 responses – the largest we have ever received to one of our surveys.

An alarming number of female officers and staff who responded to our survey alleged appalling behaviour by male colleagues. Their allegations included sexual harassment and serious sexual assault. We concluded that far too many women had, at some stage in their career, experienced unwanted sexual behaviour towards them.

Even worse, in many cases the perpetrator was someone who had previously been reported for similar behaviour, which the force either didn't take seriously or investigate thoroughly.

Some forces have failed to consider the link between misogynistic behaviour towards colleagues and similar behaviour towards members of the public. And some are not responding robustly enough when presented with misogynistic behaviour in the workplace. We examined 264 complaint and misconduct investigations. In almost one in five cases, we were unimpressed by the force's decision-making.

In this report, we describe 5 areas for improvement and make 43 recommendations – an unusually high number for one of our reports. Our recommendations are designed to strengthen the systems by:

- introducing more thorough pre-employment checks;
- establishing better processes for assessing, analysing, and managing risks relating to vetting decisions, corruption investigations and information security;
- improving the quality and consistency of vetting decision-making, and improving the recording of the rationale for some decisions;
- extending the scope of the law relating to police complaint and misconduct procedures;
- strengthening guidance for forces in respect of vetting processes, relationships, and behaviours in the workplace;
- understanding and defining what constitutes misogynistic and predatory behaviour in a policing context;
- improving the way the police collect corruption-related intelligence; and
- improving the way police assess and investigate allegations of misconduct.

At the moment, it is too easy for the wrong people both to join and to stay in the police. Too many recent events prove this. If public confidence in the police is to be improved, chief constables, among others, need to be less complacent. Standards need to be consistent, and higher.

Matt Parr CB

His Majesty's Inspector of Constabulary

Summary

Background

In March 2021, Sarah Everard was murdered by a Metropolitan Police Service (MPS) officer. His actions involved abuse of authority, kidnap and rape. The case raised substantial questions about police recruitment and vetting arrangements, and the standards of behaviour in the workplace. It has prompted several reviews into the MPS and policing more widely.

The standards of behaviour of police officers and staff, towards the public and towards each other, both on and off duty, must be of the highest order. It is vital that arrangements for their recruitment and vetting are robust.

On 18 October 2021, the then Home Secretary commissioned us to carry out a thematic inspection to assess current vetting and counter-corruption arrangements in policing across England and Wales. The inspection was to include assessing forces' abilities to detect and deal with misogynistic and predatory behaviour.

Failure to learn lessons

The majority of police officers and staff meet – and often exceed – the standards of behaviour the public have a right to expect. But an examination of police misconduct-related matters in the years prior to Sarah Everard's murder points to some systemic failings, missed opportunities, and a generally inadequate approach to the setting and maintenance of standards in the police service. Following our terms of reference, this report will concentrate on misogyny and sexualised misconduct; but its observations also apply to wider forms of wrongdoing.

Too many warnings have been ignored

In the decade leading up to our inspection, there have been several appalling offences against women and girls by serving police officers and staff. Some of these have led to lengthy custodial sentences for the perpetrators, ranging from 19 years to life imprisonment.

Over the same period, a series of reports should have alerted forces that some of them were not properly equipped to prevent and investigate misogynistic and predatory behaviour. We could draw similar conclusions about racism, dishonesty, and other forms of corruption. In our inspections, we found that some forces

consistently and repeatedly failed to implement recommendations contained in these reports. A UNISON survey of its police staff members also raised concerns about the internal culture of the police service, with evidence of sexual harassment in the workplace.

The police service has had ample warning that behaviours, cultures and processes need to change.

The recruitment process

Police recruitment through the Government's Police Uplift Programme (PUP) is underway on a massive scale. The size and speed of this programme carry risks that, if standards of recruitment practice (including vetting) are not high enough, some applicants who are unfit to serve as police officers may be recruited.

The College of Policing guidance sets the standard required for the entire recruitment process. The first stage of the process is an online application form that applicants submit to the force they want to join. Forces check each applicant's eligibility to become a police officer against the force's chosen criteria. These may include a minimum age, restrictions concerning the nature of any tattoos the applicant may have, and whether they hold a licence to drive.

In most forces, those who complete the form properly and meet the eligibility criteria move on to the College of Policing's national sift. The national sift consists of an online situational judgment test and a behavioural-style questionnaire. Six forces haven't adopted the national sift. These forces either don't sift applicants at all or carry out their own sift.

The next stage is the national assessment centre (NAC). Both the national sift and NAC are designed to test applicants against the competencies and values required of officers. Since the start of the pandemic, the NAC has been an online process.

Following the NAC, most forces now hold post-assessment interviews for successful applicants, but some still don't. According to the College of Policing's standards, this isn't a mandatory part of the recruitment process.

Successful applicants then undergo a series of pre-employment checks, including some mandatory checks to establish their identity and right to live and work in the UK. Applicants for forces that don't hold post-assessment interviews could proceed to this stage without ever having any personal contact with a representative from the force.

Most forces told us they also carry out checks on an applicant's employment history and obtain employment and character references. But there is no legal requirement on forces to carry out these checks and some have stopped doing them. These forces told us that employment references often give little more than confirmation of periods of employment so in their opinion don't add value. But applicants aren't always

truthful, and we heard some anecdotal evidence of unsuitable applicants managing to join.

It is unacceptable that some police applicants are appointed without any checks to confirm the accuracy of some of the important information they have provided on their application form. Recruitment processes in many other organisations are far more thorough.

At the very least, references can confirm that stated employment timelines are correct and identify gaps in employment history. Forces should do more to check the accuracy of information given by applicants.

The initial vetting stage

In explaining why vetting is necessary, the Vetting Code of Practice (Vetting CoP) refers to information security and the protection of police assets. The Vetting Authorised Professional Practice (Vetting APP) also refers to public safety and public confidence. As well as having access to a wealth of police information, police officers enforce the law, exercising intrusive powers over other citizens. This will often be in relation to people who are vulnerable at that time. It is therefore vital that, as well as considering information security, vetting decision-makers take full account of any factors relating to the safety of the public, particularly those who are vulnerable.

Police refer to the reasoning behind their decisions as the 'rationale'.
Vetting decision-makers should treat each case on its own merits and record the rationale for their decision. Forces should comply with the Vetting APP, although they are not legally obliged to do so.

Even the most thorough and complete vetting regime could never guarantee that an applicant would not go on to become corrupt or become a risk to the police service.

Our review of force vetting decisions

Vetting units sometimes grant clearance to applicants with criminal convictions, or whose family or friends have convictions, or where other concerning information is held. There can be valid reasons for this.

We formed a review team, including current vetting experts from police forces.
This team reviewed 725 vetting files relating to new recruits and transferees.
We asked forces to give us vetting clearance files from the preceding three years, relating to police officers and staff who had previously committed criminal offences and those the force had other concerns about.

In the majority of cases, the review team agreed with forces' decisions to grant vetting clearance. But there were 68 cases where they disagreed. There were also 63 cases where the review team believed they may have agreed with the decision, had the rationale contained greater detail or potential risk mitigation measures been

properly considered. Although we found many examples of good decision-making, our vetting file review revealed some disturbing results.

In many of the cases, the review team found no evidence that forces had fully assessed the risks or taken steps to mitigate them (through closer supervision, for example). Some forces didn't have enough people within their counter-corruption unit (CCU) or vetting unit to mitigate the risks. The failure to adequately deal with such risks represents a significant corruption threat for forces. Often, forces hadn't properly considered the effect that granting clearance may have had on public safety, public confidence, or the reputation of the police service.

Forces are increasingly doing social media research as a form of vetting enquiry. Our vetting file review showed that forces had found language and comments on social media, attributable to vetting applicants, that were potentially discriminatory, inflammatory, or extremist. Worryingly, the cases we examined didn't result in rejection. Instead, forces were addressing this through advice to applicants regarding their future use of social media.

Given the frequency with which our review team disagreed with vetting clearance decisions, there is a clear case for introducing more extensive and routine quality assurance processes.

The College of Policing Vetting APP gives guidance to forces in relation to vetting processes. We found many areas of the Vetting APP that need to be amended to make the guidance more robust. These areas include:

- decision-making, particularly in respect of factors relating to public protection;
- risk mitigation;
- recording of rationales;
- appeals;
- vetting reviews; and
- transferees.

Disproportionality in vetting decisions

The Vetting CoP states that forces should monitor their vetting clearances and refusals to make sure that people with protected characteristics aren't unfairly treated. If decisions are found to disproportionately affect certain groups, for example people with disabilities or minority ethnic groups, then forces should take steps to understand the reasons for this. Vetting is a complex issue which, for various reasons, has the potential to work against people from diverse backgrounds in different ways. We found that most of the forces we inspected have very little understanding of disproportionality in their vetting decisions. Without any analysis to help forces understand the reasons for disproportionality in their decision-making, forces can't take informed action to address it.

Vetting appeals processes

Some forces have nominated an individual to act as an appeal body – usually a senior officer within the professional standards department (PSD). In other forces, for example where supervisors within the vetting unit make the vetting decision, we found that the vetting manager handles any appeals.

Two forces we inspected have introduced vetting panels. In the absence of any national guidance, these operate differently to each other. We found several examples of these vetting panels overturning sound decisions, overlooking risks, and not recording their rationale in sufficient detail.

Vetting interviews

We found that forces used vetting interviews infrequently. There were numerous cases where vetting enquiries revealed concerning information, but forces hadn't interviewed applicants to clarify the issues. In borderline cases, it would be of value for decision-makers to interview the applicants before deciding whether they are suitable.

Reviews of vetting after misconduct proceedings

The Vetting APP states that, at the conclusion of misconduct proceedings where the officer, special constable or member of staff is issued with a written warning or a final written warning, forces should review the individual's vetting clearance. Inexplicably, not all the forces we inspected do this. Under the Police (Conduct) Regulations 2020, there is an additional disciplinary action of 'reduction in rank', which is deemed more serious than a final written warning. But the Vetting APP makes no reference to this. We believe it should.

Forces determine their own risk appetite, some more liberally than others

When making vetting decisions, there is a level of risk forces are willing to tolerate, which some refer to as their 'risk appetite'. We believe that sometimes this may be influenced by the need to meet certain recruitment targets. As a consequence, some forces had too great a risk appetite, which led them to grant vetting clearance despite knowing disturbing information about applicants.

When forces grant vetting clearance to such applicants, and fail to put sufficient mitigation measures in place, the risks to the force and the public become unacceptable.

Designated posts and management vetting

Police officers and staff working in more sensitive posts generally need a higher level of police vetting known as management vetting (MV). We found disparities across forces as to which posts they had designated for MV. There are limitations in how effectively the MV process assesses suitability to work with vulnerable people. But we do recognise the benefits of re-vetting someone before they move into such posts. The Vetting APP should provide clearer guidance on the criteria for designating MV posts and those roles which involve working with vulnerable people.

Forces' understanding of who occupies designated posts is sometimes amateurish. None of the forces we inspected had linked their HR and vetting IT systems. As a result, there are occasions when forces have police officers and staff in these posts who aren't vetted to the right level.

Vetting renewal intervals

A person's vetting must be renewed periodically to make sure they are still suitable to work in the police. For MV, this is every seven years and for recruitment vetting (RV), this is every ten years. (The checks needed for each type of vetting are listed at Annex A). Numerous interviewees, including some with national policing responsibilities, expressed the view that these intervals are too long. We agree.

Reporting changes in circumstances

Both the Vetting CoP and the Vetting APP require police officers and staff with current vetting clearance to report changes in their personal circumstances. We found many officers and staff weren't fully aware of what changes they should report.

Using the Police National Database to identify unreported changes in circumstances

Staff in vetting units weren't confident that all information potentially affecting an individual's vetting clearance was being given to them. A force may not be aware that an officer or staff member has come to police notice (for example, by being arrested or issued with a fixed penalty notice) outside their home force area, unless the person reports this themself.

Automated Police National Database (PND) checks would tell forces if any new information was added to the PND in relation to their police officers and staff. This would allow forces to address potentially serious issues at the earliest opportunity and identify personnel who fail to self-report relevant matters. In one force, a pilot study to use the PND for automated checks was underway.

Capacity within vetting units

The PUP gave each force an annual recruitment target and funding to help it meet the target. The funding is allocated not only to support the initial recruitment and pay the wages of new police officers and staff, but also to provide the extra infrastructure forces need to recruit and train them. Some forces have chosen to use the funding to recruit more staff to work in vetting units.

But not all the forces we inspected had enough staff within their vetting units to cope with current demands. Personnel in some vetting units told us that increasing vetting demand from the PUP was creating pressure and that their workload was no longer manageable.

Training for those involved in vetting

Our vetting file review identified significant skills gaps in some vetting units. It is clear that vetting training needs to be improved. There were limited training resources and opportunities available to vetting officers. The PUP has provided funding for additional training, prompting the development of a new course. When it is introduced, this course should improve vetting processes across the service.

Vetting of police officers and staff transferring between forces

The Vetting APP states that forces must make sure the integrity of a police officer wishing to transfer into the force (or to re-join the police service) is beyond question.

Forces are consistently sharing information and choosing to re-vet all transferees

In some circumstances, APP allows forces to accept a transferee's current vetting clearance. But in each of the forces we inspected, we found that vetting units were carrying out their own vetting enquiries on applicants to transfer or re-join. We also found that forces routinely requested and received such applicants' professional standards history and any corruption-related intelligence. This is encouraging. But we found that forces aren't always using this information effectively to support their vetting decisions.

Inconsistencies between forces

We found examples of vetting refusal decisions based wholly or in part on the PSD history or corruption-related intelligence shared between forces. But we also found some transferee application cases where the receiving force refused to grant vetting clearance, even though the originating force had previously granted clearance based on the same information. This brings into question the originating force's rigour in vetting standards.

Some forces grant vetting clearance to transferees with unresolved complaints or misconduct matters

The Vetting APP states that when a police officer is subject to a complaint or conduct investigation that hasn't yet been finalised, they shouldn't be allowed to transfer between forces. The Vetting APP makes clear that this condition can be waived with the agreement of both forces. We found occasions when forces allowed the transfer to proceed, without any record of the required agreement or explanation for the decision.

A vetting refusal for a transferee should trigger a review of their current vetting status

Some force vetting managers (FVMs) told us that, when another force refuses to grant vetting clearance on a transferee application, this triggers them to carry out their own review of the applicant's vetting status. This is not a requirement of the Vetting APP but seems to us to be a sensible approach. We take the view that, in every case where a transferee applicant is refused clearance, the originating force should carry out its own review of the applicant's vetting status.

Detecting and dealing with misogynistic and predatory behaviour

Defining misogynistic and predatory behaviour in a policing context

The then Home Secretary asked us to examine forces' ability to detect and deal with "misogynistic and predatory behaviour". To identify more precisely the types of behaviour in question, we had to define what they were, as we found no nationally agreed definition.

We defined 'prejudicial and improper behaviour' as:

> Any attitude and/or behaviour demonstrated by a police officer or police staff that could be reasonably considered to reveal misogyny, sexism, antipathy towards women or be an indication of, or precursor to, abuse of position for a sexual purpose (AoPSP).
>
> During the inspection, we heard numerous examples, mainly from female police officers and staff, of such attitudes and behaviour towards them. This was usually, but not exclusively, from their male colleagues. When police officers and staff don't treat colleagues with respect and courtesy, it suggests that they may be more likely to behave in a similar way towards the public, and towards vulnerable women.

An improving police culture, but with persistent problems

Many of the officers we interviewed – particularly those who were more senior – told us that although these types of attitudes and behaviour in policing have reduced over the last five years or so, they persist. The view that there had been an improvement in culture and behaviour was largely reflected in our survey results.

Nevertheless, we were left in no doubt that, in too many places, a culture of misogyny, sexism and predatory behaviour towards members of the public and female police officers and staff still exists. Female officers and staff we spoke to – in alarmingly high numbers – described the profoundly negative effect such behaviour has had on them.

We carried out an online survey, which 11,277 police officers, staff and volunteers responded to. This was the highest ever response to one of our surveys. Additionally, 668 of the respondents volunteered for follow-up interviews. We interviewed 42 of these. In the interviews, all the respondents recounted examples of misogynistic and predatory behaviour. Their accounts included sensitive detail, some of which amounted to allegations of criminal offences. These included female officers and staff alleging sexual assault by male colleagues in the workplace and at social events.

The interviewees also told us that, in many cases, the perpetrator was someone who had previously been reported for similar behaviour, which either hadn't been taken seriously or wasn't thoroughly investigated.

We believe that the poor behaviour towards women we were told about is prevalent in many – if not all – forces. Much of the behaviour interviewees described was outside our terms of reference. For example, women told us about misogynistic and sexist behaviour that fell short of being predatory.

Challenging and reporting prejudicial and improper behaviour

Most police officers and staff told us they would recognise prejudicial and improper behaviour and knew how to report it. Conversely, some officers and staff who had personally experienced such behaviour told us it was often witnessed by colleagues, including supervisors. But they said that these colleagues rarely challenged it.

Many women told us they were used to tolerating a degree of such behaviour before reporting it. And many told us they were worried about the repercussions if they did make a report. They were concerned that they would be viewed as a troublemaker or be ostracised.

When (usually female) police officers and staff did report this behaviour, in most cases they were dissatisfied with the outcome.

The rights of dissatisfied police officer victims need to be strengthened

Unlike members of the public, police officers who are victims of crime and dissatisfied with the service they received from colleagues in their own force do not have a right to make a formal complaint. They should have similar rights to members of the public in these circumstances.

Policies and procedures relating to prejudicial and improper behaviour

All forces have a range of policies and procedures aimed at preventing corruption. But very few of these relate to the type of behaviour that falls within our definition of prejudicial and improper behaviour. Our inspection revealed a prevalence of this behaviour, which suggests that forces should have policies to support officers and staff to identify, deal with and investigate it.

The Standards of Professional Behaviour set out a clear framework of what type of conduct by a police officer is or is not acceptable. All aspects of prejudicial and improper behaviour would generally be covered by these standards. There is a specific duty for police officers and staff to report, challenge or act if they witness it, or become aware of such behaviour exhibited by a colleague.

But, in their records, forces are unable to easily identify conduct matters involving prejudicial and improper behaviour. They find it difficult to differentiate such cases from other conduct matters. There is no single category that can be used to identify them, or other means of flagging cases. Forces need to have a standardised definition of prejudicial and improper behaviour, to help them accurately assess its prevalence.

Forces need to do more to collect intelligence relating to prejudicial and improper behaviour

Most of the prejudicial and improper behaviour cases we reviewed originated from reports from the public or from colleagues. During this inspection, we reviewed 236 complaint and misconduct cases that we considered fell under our definition of prejudicial and improper behaviour. Of these, only 15 resulted from proactive intelligence collection. Forces should routinely widen their inquiries to establish whether the matter under investigation is part of a wider pattern of behaviour. During our investigation file review, we found that forces didn't usually carry out these wider inquiries.

There is too much tolerance of prejudicial and improper behaviour

Reports of prejudicial and improper behaviour should be dealt with consistently. Initially, forces must consider the seriousness of the allegation and whether it is a crime or conduct matter. In most of the cases we examined, we found the standard of the decision-making to be good. But some initial assessments reveal leniency, apathy and too much tolerance of prejudicial and improper behaviour. There were examples of cases which we believe should have been assessed as potential gross misconduct, that were assessed as 'misconduct only' or not treated as misconduct at all.

Overly lenient assessments undermine staff confidence, discourage the reporting of wrongdoing and harm the police service's reputation. None of the forces we inspected operated any kind of quality assurance process for these assessments. Improvements in the quality and consistency of these assessments are needed.

The standard of investigations

In general, forces have the skills they need to effectively investigate prejudicial and improper behaviour. We found PSDs had officers from a range of policing backgrounds. Most had detective experience. In the preceding two years, forces had increased officer numbers in these departments and recruited officers with experience in vulnerability and sexual offence investigation.

Of the 236 investigations we reviewed, most were effective and carried out in a timely way. In most cases, investigators followed relevant lines of inquiry.

But in 46 cases (almost 20 percent of the total), we found shortcomings in the investigation. Often, officers had not investigated as thoroughly as they should have done before closing the case. In most of these cases, there was no investigation plan and a lack of supervisory oversight.

In some of the cases we reviewed, investigators focused only on the circumstances of that specific case. They failed to consider that the alleged misconduct may well be an indicator of a wider pattern of behaviour. Investigators frequently missed opportunities to identify further misconduct or even criminal behaviour, potentially towards members of the public.

We also found ten occasions where the investigating officer recommended there was a case to answer for gross misconduct, only for a senior officer to disagree. These included cases being reduced from 'gross misconduct' to 'misconduct only', or even 'no further action'. We strongly disagreed with some of these decisions. We provide examples of this in Chapter 7.

Discharging unsuitable student officers

Regulation 13 of the Police Regulations 2003

Regulation 13 of the Police Regulations 2003 provides a relatively straightforward way to discharge an officer while they are within their probationary period, if they are not likely to become an efficient or well-conducted officer.

We were told during our inspection that, when it comes to misconduct, Regulation 13 can work well. It is a simple and effective tool. However, some forces are reluctant to use it.

The introduction of new ways to join the police, including via the Police Education Qualification Framework, means Regulation 13 may need to be updated to include academic ability as a factor when determining whether to discharge an unsuitable student officer.

Managing corruption-related intelligence

Awareness of abuse of position for a sexual purpose among officers and staff is good

AoPSP involves the sexual abuse, or attempted sexual abuse, of members of the public by police officers or staff. We examined how well forces attempted to prevent and detect AoPSP by police officers and staff. Most of the officers and staff we spoke to understood what AoPSP was and recognised it as police corruption.

Some improvement in the management of the risk of AoPSP is needed

Where a force identifies a potential perpetrator of AoPSP, they should assess the risk posed by that police officer or member of staff. Those who forces assess as a higher risk should receive additional oversight, such as monitoring of their IT use. We found that some forces were good at providing this additional oversight, but others weren't.

Not all forces record AoPSP correctly. Some cases included allegations that related to sexual misconduct toward colleagues as opposed to members of the public. The mis-recording of AoPSP has consequences for force and national-level analysis of the risks.

We found that most, but not all, force counter-corruption units (CCUs) have developed links with organisations that support vulnerable people. Forces told us that, due to the pandemic, the contact with these organisations had, for obvious reasons, reduced in frequency. These links need to be reinvigorated and maintained as they can be a valuable source of AoPSP intelligence.

Forces aren't doing enough to actively search for intelligence

Most forces respond well when they receive corruption-related intelligence. But almost all the intelligence files we reviewed involved CCUs reacting to unsolicited intelligence rather than intelligence they had actively sought.

Lawful business monitoring (LBM)

LBM helps forces make sure that access to police systems and use of communication devices is for a lawful policing purpose.

One form of LBM is using specialist software to monitor the use of IT systems. While most forces have invested in this software, we found some that still lacked this essential capability. We also found little evidence of any force using IT monitoring proactively.

Management of mobile devices is important when protecting information. Some forces told us they couldn't attribute all their mobile devices to named police officers or staff. We find this extraordinary.

Opportunities are being missed to identify officers and staff who pose a corruption risk

One method of identifying police officers and staff who pose a corruption risk is a people intelligence meeting. We found only one force we inspected regularly held such meetings.

Another way forces identify corrupt officers and staff is through reports from their colleagues. All police officers and staff we spoke to were aware of their responsibility to report wrongdoing. Most of them were aware of their force's confidential reporting system and how to access it.

Counter-corruption strategic threat assessments

All forces should produce an annual counter-corruption strategic threat assessment, detailing the corruption threats they face. We found that most forces had a comprehensive assessment. Some forces didn't make sure their police officers and staff were made aware of the corruption threats they faced. These forces are missing opportunities to involve their whole workforce in efforts to prevent corruption.

The Counter-Corruption (Intelligence) APP (unpublished) lists 12 categories of corruption-related intelligence, such as infiltration (by organised crime groups), theft, and drug misuse. Use of these categories is essential if forces are to play a meaningful part in the production of a national counter-corruption strategic threat assessment. Some forces we inspected were, without good reason, still not routinely using the national categories.

Developing corruption-related intelligence

We examined forces' intelligence development processes – the ways in which they try to find out more about what is happening in relation to specific items of intelligence, usually by interviewing witnesses, checking records, etc. In most of the 616 cases we examined, the forces had asked the right questions. However, in 53 cases, they hadn't.

Capability and capacity to tackle corruption

Most forces we inspected had increased the number of officers and staff working in counter-corruption roles over the preceding two years. Personnel working in CCUs told us their workloads were manageable.

We have recommended that forces should do more to look for corruption-related intelligence. Should they do this, it is likely that the current levels of resources in CCUs will be insufficient to deal with additional demand. CCUs need to plan for this.

Similar to PSDs, we found that most CCUs have the rights skills and equipment. And in most cases, CCUs carried out their investigations effectively and in a timely way.

Counter-corruption policies

Most forces follow Counter-Corruption (Prevention) APP guidance in relation to their counter-corruption policies

The Counter-Corruption (Prevention) APP sets out what policies forces should have and gives guidance on their content. These policies include gifts and hospitality, business interests and notifiable associations. We found that, in most forces, the content of their counter-corruption policies and oversight of these reflected the Counter-Corruption (Prevention) APP guidance. Some forces need to make sure that supervisors are fully aware of their officers and staff who have business interests or notifiable associations.

The knowledge and understanding of the counter-corruption policies in the forces we inspected was mostly good. Most people told us that, even if they didn't have detailed knowledge of the actual policy, they knew how to find it on their force's intranet and had confidence that their supervisors could give them advice if needed.

All forces should introduce annual integrity reviews

Integrity reviews are where supervisors discuss with members of their teams risks such as: AoPSP, notifiable associations, business interests, gifts and hospitality, and changes in circumstances. These are often done alongside performance reviews and can play an important role in reinforcing and maintaining the standards of a force. Not all forces have adopted annual integrity reviews. And some of those which have (in theory) adopted integrity reviews don't always make sure that supervisors complete them.

Recommendations

We have made 43 recommendations. They fall into the following categories:

- updating minimum standards for pre-employment checks; (see recommendation 1);
- establishing better processes for assessing, analysing, and managing risks relating to vetting decisions, corruption investigations and information security; (see recommendations 2, 3, 11, 13, 15, 16, 29, 31, 36, 37, 38, 39, 41, 42 and 43);
- improving the quality and consistency of vetting decision-making, and improving the recording of the rationale for some decisions; (see recommendations 4, 7 and 8);
- extending the scope of the law relating to police complaint and misconduct procedures; (see recommendations 19 and 30);
- strengthening guidance for forces in respect of vetting processes, relationships, and behaviours in the workplace; (see recommendations 5, 6, 9, 10, 12, 14, 17 and 21);

- understanding and defining what constitutes misogynistic and predatory behaviour in a policing context; (see recommendations 20, 22, 23 and 24);
- improving the way the police collect corruption-related intelligence; (see recommendations 32, 33, 34 and 35); and
- improving the way police assess and investigate allegations of misconduct. (see recommendations 18, 25, 26, 27, 28 and 40).

Recommendation 1

By 31 October 2023, the College of Policing should update its guidance on the minimum standard of pre-employment checks that forces must carry out before appointing an officer or member of staff. Every chief constable should make sure their force complies with the guidance. As a minimum, pre-employment checks should:

- obtain and verify previous employment history for at least the previous five years (including dates of employment, roles carried out and reason for leaving); and
- verify the qualifications the applicant claims to have.

Recommendation 2

By 30 April 2023, chief constables should establish and begin operation of a process to identify, within their vetting IT systems, vetting clearance records where:

- applicants have committed criminal offences; and/or
- the record contains other types of concerning adverse information.

Recommendation 3

By 30 April 2023, chief constables should take steps to make sure that, when granting vetting clearance to applicants with concerning adverse information about them:

- vetting units, counter-corruption units, professional standards departments, and HR departments (working together where necessary) create and implement effective risk mitigation strategies;
- these units have enough capacity and capability for this purpose;
- responsibilities for implementing specific elements of the risk mitigation strategy are clearly defined; and
- there is robust oversight.

Recommendation 4

By 30 April 2023, chief constables should make sure that, when concerning adverse information has been identified during the vetting process, all vetting decisions (refusals, clearances and appeals) are supported with a sufficiently detailed written rationale that:

- follows the National Decision Model;
- includes the identification of all relevant risks; and
- takes full account of the relevant risk factors described in the Vetting Authorised Professional Practice.

Recommendation 5

By 31 October 2023, the College of Policing, working with the lead for vetting, should change the Vetting Authorised Professional Practice, to give improved clarity in relation to:

- a greater focus on protecting the public;
- mitigation factors that may be employed;
- the weight to be applied to adverse information found on social media; and
- an obligation to record sufficiently detailed rationale, noting all identified risks and taking full account of all relevant factors, when coming to a vetting decision.

Recommendation 6

By 31 October 2023, the College of Policing, working with the National Police Chiefs' Council lead for vetting, should include a vetting decision-making template within the Vetting Authorised Professional Practice, to standardise decision-making.

Recommendation 7

By 31 October 2023, chief constables should introduce an effective quality assurance process to review vetting decisions, including routine dip sampling of:

- rejections; and
- clearances where the vetting process revealed concerning adverse information.

Recommendation 8

By 30 April 2023, chief constables should make sure they comply with the Vetting Authorised Professional Practice by analysing vetting data to identify, understand and respond to any disproportionality.

Recommendation 9

By 31 October 2023, the College of Policing, working with the National Police Chiefs' Council lead for vetting, should change the Vetting Authorised Professional Practice to include guidance for dealing with vetting appeals. This should include specific guidance concerning the composition and role of vetting panels.

The guidance should be consistent with the Vetting Code of Practice, particularly in relation to decision-making responsibilities and the involvement of HR professionals.

Recommendation 10

By 31 October 2023, the College of Policing, working with the National Police Chiefs' Council lead for vetting, should change the Vetting Authorised Professional Practice to make it clear that, if an officer is reduced in rank following misconduct proceedings, forces should review their suitability to keep their current level of vetting clearance.

Recommendation 11

By 30 April 2023, chief constables who have not already done so should establish and begin operation of a policy requiring that, at the conclusion of misconduct proceedings where an officer, special constable or member of staff has been issued with a written warning or a final written warning, or been reduced in rank, their vetting status is reviewed.

Recommendation 12

By 31 October 2023, the College of Policing, working with the National Police Chiefs' Council lead for vetting, should change the Vetting Authorised Professional Practice to be more prescriptive about what types of roles require management vetting, and give guidance on how people working with vulnerable individuals are vetted. This should include an emphasis on roles that specifically involve working closely with vulnerable people.

Recommendation 13

By 31 October 2023, chief constables who have not already done so should establish and begin operation of a process to:

- identify the required vetting level for all posts within the force, including designated posts requiring management vetting; and
- determine the vetting status of all police officers and staff in designated posts.

As soon as possible after this, these chief constables should:

- make sure that all designated postholders are vetted to the enhanced (management vetting) level using all the minimum checks listed in the Vetting Authorised Professional Practice; and
- give continued assurance that designated postholders always have the requisite level of vetting.

Recommendation 14

By 31 October 2023, the College of Policing, in consultation with the National Police Chiefs' Council lead for vetting, should change the Vetting Authorised Professional Practice to prescribe intervals substantially shorter than ten and seven years for the renewal of recruitment vetting and management vetting respectively.

Recommendation 15

By 30 April 2023, chief constables should:

- make sure that all police officers and staff are made aware of the requirement to report any changes to their personal circumstances;
- establish a process through which all parts of the organisation that need to know about reported changes, particularly the force vetting unit, are always made aware of them; and
- make sure that where a change of circumstances creates additional risks, these are fully documented and assessed. If necessary, additional risks should lead to a review of the individual's vetting status.

Recommendation 16

By 31 December 2023, chief constables should make routine use of the Police National Database (PND) as a tool for revealing any unreported adverse information about officers and staff. To help this, the College of Policing should:

- working with the National Police Chiefs' Council lead for counter-corruption, change the Counter-Corruption (Intelligence) APP to include a requirement for the PND to be used in this way; and
- change the PND Code of Practice (and any subsequent code of practice concerning the Law Enforcement Data System) to include a specific provision that allows for the PND to be used in this way.

Recommendation 17

By 31 October 2023, the College of Policing, working with the National Police Chiefs' Council lead for vetting, should change the Vetting Authorised Professional Practice to give guidance that:

- in every case where a transferee is refused vetting clearance, the originating force should carry out its own review of the individual's vetting status; and
- the two forces involved exchange relevant information about the reasons for the refusal decision.

Recommendation 18

By 30 April 2023, chief constables should make sure that there is a robust response to any criminal allegation made by one member of their force against another. This should include:

- consistent recording of allegations;
- improved investigation standards; and
- sufficient support for victims and compliance with the Code of Practice for Victims of Crime in England and Wales.

Recommendation 19

By 31 October 2023, the Home Office, working with the National Police Chiefs' Council lead for complaints and misconduct, and the Independent Office for Police Conduct, should make sure that police officers who make criminal allegations against other members of their own force are afforded rights similar to those held by members of the public who make criminal allegations. These should include:

- the right to complain about the conduct of officers concerned with the handling of the allegation, including its recording and investigation; and
- the right to appeal against the outcome of such a complaint.

Recommendation 20

By 30 April 2023, chief constables should adopt the National Police Chiefs' Council sexual harassment policy.

Recommendation 21

By 30 April 2023, the College of Policing, working with the National Police Chiefs' Council lead for ethics and integrity, should extend the scope of the *Appropriate personal relationships and behaviours in the workplace* guidance. An amended version should include guidance in relation to non-consensual behaviours as well as consensual relationships.

Recommendation 22

By 30 April 2023, the National Police Chiefs' Council and the College of Policing, in consultation with the Independent Office for Police Conduct, should define prejudicial and improper behaviour, using the definition contained in this report or a suitable alternative.

Recommendation 23

By 31 October 2023, the National Police Chiefs' Council lead for complaints and misconduct, in consultation with the relevant IT provider and the Independent Office for Police Conduct, should arrange to add a prejudicial and improper behaviour identifier flag to the professional standards database used to record complaints and misconduct.

Recommendation 24

By 31 October 2023, chief constables should make sure their professional standards departments attach a prejudicial and improper behaviour flag to all newly recorded relevant cases.

Recommendation 25

By 30 April 2023, chief constables should make sure their professional standards departments and counter-corruption units routinely carry out all reasonable wider inquiries when dealing with reports of prejudicial and improper behaviour. These inquiries should ordinarily include (but not be limited to) sampling the following, in relation to the officer under investigation:

- their use of IT systems;
- incidents they attended, and incidents they are otherwise connected to;
- their use of work mobile devices;
- their body-worn video recordings;
- radio location checks; and
- misconduct history.

Recommendation 26

By 30 April 2023, chief constables should make sure their professional standards departments:

- produce and follow an investigation plan, endorsed by a supervisor, for all misconduct investigations; and
- check all reasonable lines of inquiry in the investigation plan have been concluded before finalising the investigation.

Recommendation 27

By 30 April 2023, the National Police Chiefs' Council lead for complaints and misconduct should design a sampling regime for appropriate authorities' decisions. This is to quality assure the decisions and identify any learning. The sampling should make sure that appropriate authorities' decisions:

- are consistent;
- maintain public confidence in, and the reputation of, the police service;
- uphold high standards in policing and deter misconduct; and
- protect the public.

Recommendation 28

By 30 April 2023, in the forces where we have not carried out fieldwork during this inspection, chief constables who have not already carried out a review of all allegations relating to prejudicial and improper behaviour, should do so. The review should be of cases from the last three years where the alleged perpetrator was a serving police officer or member of staff. The review should establish whether:

- victims and witnesses were properly supported;
- all appropriate authority assessments, including assessments which didn't result in a complaint or misconduct investigation, were correct;
- investigations were comprehensive; and
- any necessary steps are taken to improve the quality of future investigations.

These reviews will be subject to examination during our next round of inspections of professional standards departments.

Recommendation 29

With immediate effect, chief constables must make sure that forces use Regulation 13 of the Police Regulations 2003 for underperforming officers during their probationary period, rather than the Police (Performance) Regulations 2020.

Recommendation 30

By 31 December 2023, the Home Office, working with the National Police Chiefs' Council lead for complaints and misconduct and the College of Policing, should make sure that forces can use Regulation 13 of the Police Regulations 2003 effectively to discharge probationers who don't achieve the required educational or academic standard during their probationary period.

Recommendation 31

By 31 October 2023, the Home Office, working with the College of Policing and the National Police Chiefs' Council lead for complaints and misconduct, should make sure that, during pre-employment or vetting checks, police forces can identify any applicants previously discharged under Regulation 13 of the Police Regulations 2003.

Recommendation 32

By 30 April 2023, chief constables should make sure that:

- all intelligence concerning possible sexual misconduct by officers or staff (including abuse of position for a sexual purpose and internal sexual misconduct) is subject to a risk assessment process, with action taken to minimise any risk identified; and
- rigorous additional oversight arrangements are in place to monitor the behaviour of officers subject to the risk assessment process, especially in cases assessed as high risk.

Recommendation 33

By 31 March 2023, chief constables should make sure that counter-corruption units (CCUs) have established relationships with external bodies that support vulnerable people who may be at risk of abuse of position for a sexual purpose, such as sex-worker support services, drug and alcohol and mental health charities. This is to:

- encourage the disclosure by such bodies, to the force's CCU, of corruption-related intelligence relating to the sexual abuse of vulnerable people by police officers and staff;
- help the staff from these bodies to understand the warning signs to look for; and
- make sure they are made aware of how such information should be disclosed to the CCU.

Recommendation 34

By 30 April 2023, chief constables should make sure that their counter-corruption units actively seek corruption-related intelligence as a matter of routine.

Recommendation 35

By 31 March 2023, to protect the information contained within their systems and help them to identify potentially corrupt officers and staff, chief constables should make sure that:

- their force has the ability to monitor all use of its IT systems; and
- the force uses this for counter-corruption purposes, to enhance its investigative and proactive intelligence gathering capabilities.

Recommendation 36

By 30 April 2023, chief constables should establish and begin operation of an improved system of mobile device management, with accurate record keeping concerning:

- the identity of the officer or staff member each device is allocated to; and
- what each device has been used for.

Recommendation 37

By 30 April 2023, chief constables should:

- convene, and hold on a regular and continuing basis, people intelligence meetings; or
- establish and begin operation of an alternative process to support the presentation and exchange of corruption-related intelligence, to identify officers and staff who may present a corruption risk.

Recommendation 38

By 30 April 2023, chief constables should make sure that all corruption-related intelligence is categorised in accordance with the National Police Chiefs' Council counter-corruption categories (and any revised version of these).

Recommendation 39

By 30 April 2023, chief constables should make sure they have a current counter-corruption strategic threat assessment, in accordance with the Counter-Corruption (Intelligence) Authorised Professional Practice.

Recommendation 40

By 30 April 2023, chief constables should make sure their counter-corruption units:

- produce and follow an investigation plan, endorsed by a supervisor, for all counter-corruption investigations; and
- check all reasonable lines of inquiry in the investigation plan have been concluded before finalising the investigation.

Recommendation 41

By 30 April 2023, chief constables should strengthen their business interest monitoring procedures to make sure that:

- records are managed in accordance with policy and include cases where authorisation has been refused;
- the force actively monitors compliance with conditions that are attached to the approval, or where the application is refused;
- regular reviews of each approval are carried out; and
- all supervisors are properly briefed about business interests held by members of their teams.

Recommendation 42

By 30 April 2023, chief constables should strengthen their notifiable association procedures to make sure that:

- they are compliant with the Counter-Corruption (Prevention) Authorised Professional Practice (APP) and that the obligation to disclose all associations listed in the APP is explicit;
- there is an effective monitoring process to make sure that any conditions imposed are being complied with; and
- all supervisors are correctly briefed on the notifiable associations declared by members of their teams.

Recommendation 43

By 30 April 2023, chief constables should make sure that a robust process is in place for completing annual integrity reviews for all officers and staff.

Areas for improvement

The areas for improvement listed below are in addition to other relevant areas for improvement raised in previous inspections and referred to in this report.

Area for improvement 1

Forces' use of vetting interviews is an area for improvement. In more cases, forces should interview applicants to explore adverse information of relevance to the case. This should help with assessing risk. When they carry out such interviews, forces should maintain accurate records and give copies of these to interviewees.

Area for improvement 2

Automated links between force vetting and HR IT systems are an area for improvement. When specifying and procuring new IT systems for these purposes, or developing existing ones, forces should seek to establish automated links between them.

Area for improvement 3

Forces' understanding of the scale of misogynistic and improper behaviour towards female officers and staff is an area for improvement. Forces should seek to understand the nature and scale of this behaviour (like the work carried out by Devon and Cornwall Police) and take any necessary action to address their findings.

Area for improvement 4

Forces' data quality is an area for improvement. Forces should make sure they accurately categorise all items of sexual misconduct intelligence. Sexual misconduct cases that don't meet the definition of AoPSP (because they don't involve the public) shouldn't be recorded as AoPSP.

Area for improvement 5

Workforce awareness of corruption-related threats is an area for improvement. Forces should routinely brief police officers and staff on the pertinent and sanitised content of their annual counter-corruption strategic threat assessment.

1. Introduction

Background

In March 2021, Sarah Everard was murdered by a Metropolitan Police Service (MPS) officer. His actions involved abuse of authority, kidnap, and rape. The case raised substantial questions about police recruitment and vetting arrangements, and standards of behaviour in the workplace. It has prompted several reviews into the MPS and policing more widely. They include:

- a Home Office-sponsored independent inquiry, by the Rt Hon Dame Elish Angiolini DBE KC;
- an MPS-sponsored review of the force's culture and standards of behaviour, led by Baroness Casey of Blackstock DBE CB;
- several misconduct investigations by the IOPC; and
- this thematic inspection of police vetting and counter-corruption arrangements.

Our inspection comes at a time when the police are carrying out a major recruitment campaign, bringing in tens of thousands of new officers. If the police are to restore public confidence in the service, and the support they lost in the wake of Sarah Everard's murder, it is vital that their recruitment and vetting arrangements are robust. And it is imperative that their standards of behaviour, in and out of the workplace, towards the public and towards each other, are of the highest order.

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

Our commission

On 18 October 2021, using her powers under section 54(2B) of the Police Act 1996, the then Home Secretary commissioned us to carry out a thematic inspection to provide an assessment of current vetting and counter-corruption arrangements in policing across England and Wales – to include forces' ability to detect and deal with misogynistic and predatory behaviour.

The Home Secretary wrote:

> "That such a brutal crime was carried out by a serving police officer has shocked this country and will have damaged confidence in policing. It is critical that the public, and particularly women and girls, can be assured that police forces are doing everything they can to prevent individuals who are unsuitable to serve the public from joining policing, and that forces are ever vigilant for signs of behaviour that indicate that individuals are not fit to serve."

Terms of reference

Our terms of reference were to address the following questions:

1. How effective and rigorous are current vetting standards, and how well do forces identify the correct vetting levels of officers and staff and vet and re-vet them in accordance with the requirements for their roles?
2. How effective are the vetting arrangements for police officers and staff who intend to transfer from one force to another?
3. How effectively do forces prevent, manage, understand, and investigate potential corruption among their police officers and staff?
4. How effectively do forces identify, prevent, detect and deal with prejudicial and improper behaviour based on gender by their police officers and staff?

Methodology

Our inspection took place between November 2021 and May 2022. We carried out fieldwork in eight police forces in England and Wales. We did:

- a **document review**, in which we examined 667 documents, which included policies, procedures and other material;
- an **intelligence file review**, in which we examined 616 items of corruption-related intelligence, including 158 items relating to sexual misconduct;
- an **investigation file review**, in which we examined 236 misconduct and complaint investigations;
- a **vetting file review**, in which we examined 725 vetting files, using a panel of subject matter experts;
- a total of 94 interviews and 182 focus groups with police officers and staff;
- reality testing across each force area by speaking with individual police officers and staff; and
- a review of forces' progress against relevant recommendations and areas for improvement, which we identified in previous inspections.

Survey

We carried out an online survey of police officers, staff, and volunteers across forces in England and Wales. The survey was voluntary and anonymous and covered a range of areas relating to misogyny and sexual misconduct in the workplace, including:

- access to training and guidance;
- reporting of wrongdoing by colleagues;
- knowledge of vetting;
- views on the culture in police forces;
- use of social media; and
- experience of misogyny, sexual misconduct, improper behaviours and attitudes in the workplace.

The survey allowed respondents to miss out questions if they wished. We received 11,277 responses to the survey, with 7,523 respondents completing it in full. We also asked respondents if they would be willing to be interviewed to discuss their experiences in more detail. A total of 668 respondents volunteered to be interviewed by us. We interviewed 42 of them.

Terminology in this report

Our report contains references to ‘national’ bodies, strategies, policies, systems, responsibilities, processes and data. In some instances, ‘national’ means applying to England and Wales. In others, it means applying to England and Wales and Scotland, or the whole of the United Kingdom.

2. Failure to learn lessons

Since Sarah Everard's murder in 2021, there have been increasing concerns about the extent of misogynistic and predatory behaviour committed by police officers. Much of this behaviour attracted adverse media reporting. Several officers have been convicted of serious offences. Others were dismissed for gross misconduct.

The scale and nature of these cases makes them worrying in their own right. The murder of Sarah Everard did substantial damage to public trust and confidence in policing, especially among women and girls.

Unfortunately, these recent cases are an indication of longer-standing problems. An examination of police misconduct-related matters in the last decade points to some systemic failings, missed opportunities and a generally inadequate approach to the setting and maintenance of standards in parts of the police service.

2011

Northumbria officer jailed for life

In 2011, a Northumbria Police officer was jailed for life for carrying out sex attacks on vulnerable women he met while on duty in Newcastle. He was convicted of two charges of rape, three indecent assaults and six counts of misconduct in public office.

The officer targeted vulnerable women, including heroin addicts and shoplifters, by offering to help them while they were in police custody and then asking for sexual favours.

It also emerged that he had been accused of a serious sexual offence while he was in the army. But this wasn't revealed as part of the vetting process when he applied to join Northumbria Police.

During sentencing, the trial judge said the officer presented such a danger to women that he might never be released from prison, and that the officer had broken the bond of trust that existed between the public and the police. He was described as a sexual predator who "ruthlessly exploited" his victims for his own pleasure and "degraded them repeatedly". This behaviour lasted over a period of months, and in some cases, years.

2012

Forces urged to act

In 2012, because of this case, the Independent Police Complaints Commission (IPCC), now the Independent Office for Police Conduct (IOPC), and the Association of Chief Police Officers (ACPO), now the National Police Chiefs' Council (NPCC), commissioned a joint report relating to the abuse of police powers to perpetrate sexual violence. Among other findings, the report concluded that forces should actively look for intelligence about any officers and staff acting inappropriately. It said they should properly assess and thoroughly follow up any such intelligence.

The IPCC and ACPO checklist provided guidance for forces

The report included a checklist of 32 questions forces were asked to examine and assure themselves they had everything in place "for the prevention, prediction, and investigation of this kind of case". The questions covered the following topics:

- effective supervision of staff;
- effective vetting;
- sharing information on transferees;
- effective designation of posts that require a higher level of vetting;
- robust links between HR and vetting;
- reviews of unproven sexual allegations;
- monitoring patterns of work to look for an interest in vulnerable people;
- making sure sexual misconduct allegations (internal or external) trigger reviews of work and IT use;
- IT monitoring;
- effective links with outside agencies that support vulnerable people;
- adequate procedures for staff to report concerns regarding colleagues;
- analysis of corruption-related intelligence; and
- adequate counter-corruption resources.

2013

Another officer imprisoned

Another distressing case went before the crown court in December 2013, when a former Cleveland Police officer was jailed for 19 years. He was convicted of ten rapes, two offences of inciting a child to engage in sexual activity, one offence of sexual touching and two common assaults. There were several victims and not all the cases against him went to court.

An investigation by the force, under IPCC supervision, led to findings that some of his offending could have been avoided if other colleagues had tackled his 'red flag' behaviour. The red flags included:

- allegations of sexual assault on colleagues and members of the public;
- the receipt of love letters from ten-year-old girls he met through his work;
- inappropriate sexual language in front of colleagues;
- talking to colleagues about his sex life, including talking about sexual fantasies;
- misuse of force computer systems to search for the details of vulnerable women;
- possession of a phone that he kept at work and used on duty to contact women (referred to by colleagues as his "shagging phone"); and
- bullying and humiliating behaviour towards colleagues, particularly women, such as handcuffing them to a chair against their will.

The investigation also found that the officer's behaviour was "allowed to flourish" throughout his career. One reason for this was "indifference" by some colleagues. Other colleagues, some of whom were victims, found him manipulative and intimidating. This made them reluctant to challenge him or notify supervisors.

2014–2015

Other reports provided ample warning

Since 2014, we, the NPCC and the College of Policing have also published a series of other reports. These reports, outlined below, have individually provided forces with ample warning of the risks posed by police officers who are sexual predators. The cumulative effect of these reports should have been to set off alarm bells. But as the following pages explain, some forces have not taken adequate note of their findings.

Police integrity and corruption inspection

In 2014, we carried out a national inspection of police integrity and corruption. In our report *Integrity matters*, published in January 2015, we found that approximately a fifth of forces were still failing to sufficiently develop corruption-related intelligence and that more than half of forces didn't monitor their IT systems regularly.

We also raised concerns about the capability and capacity of counter-corruption units (CCUs) and reported that almost a third of forces didn't have enough resources to deal effectively with the amount of intelligence they were receiving. This lack of resources was also limiting the amount of proactive intelligence gathering forces could do.

We concluded that forces needed to make sure that CCUs have the necessary capability and capacity to develop and assess corruption-related intelligence. We also concluded that all police officers and staff involved in investigating corruption, including senior investigating officers, should be trained in how to investigate corruption and have the skills needed to carry out the role.

2016

PEEL: police legitimacy

During our 2016 PEEL inspections, we examined how forces were tackling the problem of officers and staff who abused their authority for sexual gain, as it was then known.

We reported that forces were generally good at assessing and developing intelligence once they received it. But many needed to improve their ability to seek out intelligence, particularly in relation to the problem of abuse of authority for sexual gain. We found that, two years on from our previous inspection, almost half of forces still didn't have the capability to monitor the use of their IT systems. About a fifth were failing to develop corruption-related intelligence. And almost a third of CCUs didn't have enough resources.

We recommended:

> "Within six months, all forces should have started to implement a plan to achieve the capability and capacity required to seek intelligence on potential abuse of authority for sexual gain. These plans should include consideration of the technology and resources required to monitor IT systems actively and to build relationships with the individuals and organisations that support vulnerable people."

Response to our 2016 PEEL report

In response to our 2016 PEEL report, the Home Secretary and the Policing Minister required the police service to develop a national strategy to address this issue. This work was led by the National Policing Counter Corruption Advisory Group (NPCCAG).

2017

New national strategy

In April 2017, the NPCC published a *National strategy to address the issue of police officers and staff who abuse their position for a sexual purpose (AoPSP)*. The strategy and an accompanying plan set out numerous things for the police to do, under the following headings: prevention, intelligence, enforcement, and engagement.

Forces still had work to do

In 2017, we reviewed the progress of forces' plans in response to our PEEL legitimacy national recommendation. We published our report in October 2017. Regrettably, we found that only two forces had all elements of our recommendation in place. Eleven force plans contained insufficient information. The remaining 30 forces had plans in place, but only 15 had started to implement these. We gave each force an individual letter setting out our views on their progress. We noted that a significant number of forces still had work to do to address this critical issue.

2018

College of Policing guidance on maintaining professional boundaries

In accordance with the national strategy for abuse of position for sexual purposes (AoPSP), in 2018 the College of Policing and NPCCAG produced national guidance for forces called *Maintaining a professional boundary between police and members of the public*. This guidance standardised advice throughout the whole service and was written to complement the College of Policing's work on its Code of Ethics, which it produced in 2014. Before this, some forces had produced documents specifying how their police officers and staff should behave with members of the public they met during the course of their duties.

The national guidance provides broad principles to support decision-making and professionalism for police officers and staff. In general, it states that they should not instigate any form of sexual relationship with someone involved in a current incident or investigation, and whom they meet in the course of their duties. It states that police officers and staff who display sexualised behaviour towards a member of the public they meet through their police duties undermine the profession, breach trust, exploit a power imbalance, act unprofessionally and potentially commit a criminal act.

UNISON sexual harassment survey raised significant concerns

In 2018, UNISON, a trade union that represents 33,700 police staff members across most police forces in England and Wales, published the findings of a survey of its police staff members, carried out in 2016. The survey, which 1,776 members responded to, sought data about sexual harassment experienced by police staff in the workplace. The findings were concerning.

Almost a fifth of the respondents said they had received a sexually explicit email or text from a colleague. Almost one in ten said that colleagues had suggested to them that sexual favours could lead to preferential treatment. Almost one in 20 disclosed that they had been pressurised into having sex with a colleague.

Over a third revealed that they weren't confident that if they complained it would be dealt with properly.

Following the publication, UNISON called for a zero-tolerance policy towards all sexual harassment in the police service. The NPCC acknowledged that the UNISON report highlighted some "outdated and unacceptable behaviour that must be rooted out".

A further warning from another significant case

In 2018, a Cheshire Constabulary officer was described in court as someone who had joined the police service "to gain the keys to a sweetshop" through access to potential victims. He met a 13-year-old girl at her home after answering a call to a domestic incident. He later contacted her on social media and started sending sexual messages and photos, returning to her home three days after the incident. While her mother was out, he drove the child to a secluded country lane and raped her, filming the offence on his mobile phone. At Liverpool Crown Court, he was convicted of a series of sex offences. This included rape, four charges of attempting to arrange the commission of a child sex offence, and one charge of arranging a child sex offence. These related to 5 different victims, aged between 12 and 15.

This officer had passed the vetting process in October 2016. Before his appointment as a police officer, the force received information that a complaint of rape had been made against him in early 2017 in another force area. Cheshire Constabulary put his recruitment on hold until the sexual offence allegation had been fully investigated. When no further action was taken against him, they resumed his recruitment application but didn't re-vet him. If they had, they would have been made aware of two further complaints about him: one of sexual activity with a child and one of persistently asking a young girl out on social media. These were being investigated by neighbouring forces that didn't know that he had applied to join the police. Further vetting checks would have revealed this.

In April 2017, the officer eventually joined Cheshire Constabulary. It was while on duty in October 2017 that he met his victim. He was jailed for 25 years.

2019

Guidance on personal relationships and behaviours in the workplace

In response to the UNISON survey, the College of Policing produced its guidance *Appropriate personal relationships and behaviours in the workplace*. The guidance relates to "intimate or sexual relationships, rather than any other 'social' relationship". It provided forces with advice on consensual workplace relationships, avoiding conflicts of interest and preventing relationships negatively affecting service delivery and public confidence.

PEEL spotlight report *Shining a light on betrayal: Abuse of position for a sexual purpose*

Also in 2019, we published *Shining a light on betrayal: Abuse of position for a sexual purpose*.

In our report, we pointed out that, for some years, forces had been urged to act to address the problem of officers and staff abusing their position for a sexual purpose. We acknowledged that many forces had listened and were already making changes. But others had been far too slow and lagged behind.

We had previously urged CCUs to develop effective relationships with agencies that support vulnerable people. This was also an action recommended in the national strategy from 2017. By 2019, regrettably, 13 CCUs still hadn't forged these links. A total of 31 forces hadn't achieved full monitoring of their IT systems. And yet again, we found that many forces still didn't have enough capacity in their CCUs. Advances in technology have made the monitoring of IT more challenging. Of the 43 forces in England and Wales, we judged that 32 didn't have enough staff to monitor their IT effectively. We found that 31 of these 32 forces weren't actively looking for corruption-related intelligence. They were simply reacting to information they were told.

We made further national recommendations, including the following:

> "By September 2020, the National Police Chiefs' Council should also work with forces to establish a standardised approach to using the information that ICT monitoring software provides."

and

> "By April 2020, all forces that haven't yet done so should:
>
> - record corruption using the national corruption categories;
> - produce a comprehensive annual counter-corruption strategic threat assessment, in line with the authorised professional practice; and
> - establish regular links between their counter-corruption units and those agencies and organisations that support vulnerable people.
>
> Where forces are yet to implement an effective ICT monitoring system that allows them to monitor desktop and handheld devices, they should do so as soon as reasonably practicable.
>
> By September 2020, all forces should have completed a review of their use of encrypted apps on police ICT systems to understand the risk they pose and to take any necessary steps to mitigate that risk."

2021

Sarah Everard murder

The officer who killed Sarah Everard had a long history of involvement with the police service. In 2002, he became a special constable in Kent. In 2011, he joined the Civil Nuclear Constabulary. In 2018, he transferred to the Metropolitan Police Service (MPS). At the time of the murder, he worked in the Parliamentary and Diplomatic Protection Command as an authorised firearms officer. He had access to the Parliamentary estate and diplomatic premises in and around central London.

In July 2021, he pleaded guilty to Ms Everard's murder. In September 2021, sentencing him to a whole-life term of imprisonment, Lord Justice Fulford said there had been "significant planning and premeditation". The police officer had "long planned to carry out a violent sexual assault on a yet-to-be-selected victim" who he intended to coerce into his custody.

The prosecution said that after finishing his police shift, the officer went out "hunting" for a lone, young woman to kidnap and rape. He apparently selected Ms Everard at random after she had left her friend's house in Clapham, south London. The court heard how he used the knowledge he had gained from his work policing COVID-19 restrictions and his MPS-issue warrant card to trick his victim under the guise of a fake arrest for breaching these restrictions. He handcuffed her and drove her away in his car. He then drove to Kent where he murdered Ms Everard.

After his conviction for murder, he was charged with six further offences of indecent exposure, alleged to have taken place between 2015 and 2021. We understand that, at the time of this report's publication, there were separate IOPC investigations and reviews in relation to possible failures by forces to investigate three of these offences. In September 2022, one officer and one former officer were convicted of sharing "grossly racist, sexist and misogynistic" messages in a social media group of which Sarah Everard's murderer was a member. In Chapter 7 and Chapter 9, we present several examples that show the inadequate ways in which some forces have dealt with some potential 'red flag' cases. These demonstrate the importance of not taking lightly what may appear to some to be relatively trivial allegations.

2022

Independent Office for Police Conduct report – Operation Hotton

In February 2022, the IOPC published a highly critical report about police officers at Charing Cross Police Station sharing racist, misogynistic, and homophobic messages.

Counter-corruption inspection of the Metropolitan Police Service

In our inspection report of March 2022, *An inspection of the Metropolitan Police Service's counter-corruption arrangements and other matters related to the Daniel Morgan Independent Panel*, (referred to later in this report as 'the DMIP report'), we raised significant concerns over the MPS's ability to tackle corruption within its ranks.

Too many warnings have been ignored

The various inspections and other reports outlined above should have alerted forces that some of them were not properly equipped to prevent and investigate misogyny and predatory behaviour, including AoPSP – a form of police corruption. But some forces consistently and repeatedly failed to implement recommendations which were designed to bring about the required improvements. Similar recommendations were included in the NPCC national strategy, but some forces still didn't act on them.

While it didn't include police officers, the UNISON survey of police staff painted a picture of a police service with a very unhealthy internal culture. This should have served as a further reminder to those forces that were falling behind in their efforts to address corruption. But this and other warnings, in some cases, have been ignored.

If forces had responded to the recommendations in the various HMICFRS reports between 2014 and 2019 and implemented all the recommended actions within the NPCC's national strategy, it is possible that a healthier police culture may have emerged. If forces used more effective vetting and counter-corruption practices, it is possible that the police officers who committed horrific offences may have been deterred from joining the service in the first place. If they did join, colleagues may have been more likely to report concerns, intelligence gathering may have alerted the force to the risk they posed and they may not have been given vetting clearance to transfer across forces. If forces had operated effectively in this way, a culture of misogyny and predatory behaviour would have been less likely to develop and thrive.

The police service has had ample warning that behaviours, cultures, and processes need to change.

3. The recruitment process

Recruitment through the Government's Police Uplift Programme (PUP) is underway on a massive scale. The programme commenced in 2019 and was designed to recruit 20,000 police officers in England and Wales by the end of March 2023. This is in addition to the recruitment required to cover the number of officers who leave for reasons such as retirement.

Taking this into account, the service will need to recruit and train over 50,000 people over a three-year period. The scale and speed of this level of recruitment carries risks that, if standards of recruitment practice (including vetting) are not high enough, some applicants who are unfit to serve as police officers may be recruited. By 31 March 2022, 13,576 officers were recruited through funding from the PUP.

We reviewed the entire process of police recruitment, from the point of advertisement to people joining the police.

The importance of realistic police advertisements

The PUP has responsibility for national recruitment advertisements and decides on their content. The Home Office communications team has developed the advertising campaign, which features real officers and case studies from a range of forces. Some forces also run their own advertising campaigns. The PUP gives guidance on the content of advertisements for forces to consider.

To recruit and retain officers, there is a need to make sure the role, and range of opportunities within policing, specifically in the early years of a career, are both accurately reflected in advertisements and recruitment information. During our inspection, there was some media criticism that one force's local adverts didn't accurately reflect the reality of day-to-day policing for most new recruits. There have also been some examples of applicants joining the service with unrealistic expectations, such as thinking they wouldn't have to work night shifts or weekends.

The results of a survey conducted by the PUP for the first year's cohort show that fewer than 80 percent of officers thought their job as a police officer had met or exceeded their expectations.

The College of Policing sets the national standards for officer recruitment

Previously, the College of Policing produced guidance to forces on some specific aspects of the recruitment process: eligibility, assessment, and pre-employment. The College has now expanded these standards to include the entire recruitment process. The stages of officer selection are:

- application;
- eligibility checks;
- national sift (situational judgment test and behavioural styles questionnaire);
- online assessment process (structured interview, written and briefing exercises);
- post-assessment interview conducted locally (optional); and
- pre-employment checks (fitness, biometrics, vetting, medical, references).

Applicants complete an online application form for the force they want to join. Forces then check the eligibility of the applicant against the standards established in the College of Policing's *Eligibility criteria for the role of police constable 2020*. This includes requirements in respect of:

- age;
- education;
- nationality;
- residency;
- physical and mental health and fitness;
- the nature of any tattoos; and
- holding a driving licence.

Forces apply this guidance in different ways. For example, forces can use their discretion as to whether the ability to drive is an essential requirement for becoming an officer.

The PUP analyses attrition rates at each stage of the selection process to help with local and national recruitment planning. In England and Wales, approximately 47 percent of applicants are successful at this stage.

In most forces, those who are successful move on to the College of Policing's national sift. The national sift consists of an online situational judgment test and a behavioural-style questionnaire that assess candidates against the behaviours required of an officer. These are explained more fully in the College of Policing's *Competency and values framework* (CVF). A senior officer told us that six forces haven't adopted the College of Policing's national sift. These forces either carry out their own assessments or don't carry out a sift at all.

In England and Wales, approximately 20 percent of the applicants who were successful at the first stage are sifted out at this stage. Successful applicants progress to the College of Policing National Assessment Centre (NAC).

Since the start of the pandemic, this has been an online process. The online assessment centre involves applicants being video-recorded as they carry out three exercises:

- a written exercise;
- an interview; and
- an oral briefing based on police-related scenarios.

These are marked remotely by assessors who are selected and trained by the College of Policing. The exercises test candidates against the CVF, with each value and competency being tested at least twice. The pass mark is set by the College.

At the time of our fieldwork, the pass rate for the online assessment was 73 percent, compared to a pass rate at the previous face-to-face assessment of 71 percent. College of Policing data shows that people from some under-represented groups are more likely to pass the online assessment centre than they were previously.

Following the online assessment, some forces hold final interviews. These take place online or face-to-face. This isn't a mandatory part of the College of Policing standards. For those forces wishing to hold final interviews, the College of Policing provides online training for interviewers and a bank of questions that are aligned to the CVF.

Successful applicants then undergo a series of pre-employment checks. In those forces that don't hold final interviews, these applicants could proceed to this stage without ever having any personal contact with a representative from the force.

Pre-employment checks include:

- biometric – DNA samples and fingerprints are taken from applicants and the samples are checked against the national databases;
- fitness – tested locally and assessed against national standards set by the College of Policing;
- medical – carried out by a medical officer locally to the national standards established by the College of Policing; and
- vetting – carried out locally, for which there is a statutory Vetting Code of Practice (Vetting CoP) and associated Vetting Authorised Professional Practice (Vetting APP), established by the College of Policing.

Data for forces in England and Wales shows that approximately 10 percent of the original field of applicants are finally recruited as student officers.

We heard some anecdotal evidence of wholly unsuitable applicants managing to join, and of unease among some senior leaders about the impersonal nature of the online process. But, at the time of our fieldwork, the vast majority of applicants recruited in this way were still in their student officer period (usually a two or three-year period from the day of joining). No national data was available on the length of service of officers facing misconduct proceedings. A senior officer subsequently told us that this data is now being collected nationally. We understand that, at a local level, some forces held such data.

We found some concerning evidence that suggests that, in one force we inspected, the suitability of some new recruits was questionable. In a 12-month period in that force, half of all the force's misconduct proceedings against police officers (14 out of 28) involved an officer in their first 2 years of service.

Further psychometric testing may improve the national recruitment process in the future

The national recruitment process includes some psychometric testing of applicants' behaviours, values, and competencies against those required by police officers. Researchers at Bournemouth University are carrying out some research to see if other psychometric tests can be used to predict future sexual misconduct.

The university has planned a pilot psychometric study with Warwickshire Police, whose chief constable is the NPCC lead for vetting. First, this study will establish a UK-based control sample of well-performing police officers, and then begin comparison-testing with new officers joining the service.

The aim of the pilot study is to establish whether lower conscientiousness could be an indicator of sexual misconduct in a UK policing context. This is a long-term study to help establish whether there is a case to implement psychometric testing as part of the police recruitment process. In due course, this study could provide findings of value to the police service. The College of Policing informed us that it is aware of the study and will review any potential learning from it.

Forces should do more to check the accuracy of applicants' previous employment and academic information

Before carrying out vetting enquiries, HR departments should carry out some pre-employment screening checks such as proof of identification and residency. But there is no legal obligation on a police force to carry out other checks or to obtain references from previous employers.

Some forces told us they carry out checks on an applicant's employment history. Others have stopped doing so. This is because they often find that references provide little more than confirmation of periods of employment, so apparently, they add little value. While we understand this view, references can at the very least confirm that stated employment timelines are correct and identify gaps in employment history.

Anecdotally, we were told about an officer who faced misconduct proceedings. Apparently, when joining the police, the officer disclosed on her application form that she had had a series of very short periods of employment. She didn't disclose that she had been repeatedly dismissed, and the force didn't investigate her employment history before deciding to grant vetting clearance.

We have examined the British Standards Institution (BSI) publication BS7858:2019, *Screening of individuals working in a secure environment*. This is a code of practice for the screening of individuals working in organisations where the security and/or safety of people, goods and services, data or property is a requirement. For some occupations, such screening may also be in the public interest. The code of practice gives guidance for organisations to verify, in writing, details of education, employment, periods of self-employment and unemployment from current and former employers, government departments, educational authorities, etc.

The College of Policing gives guidance to forces on obtaining employment history and character references. A senior officer told us that six forces don't comply with the guidance on employment history and that some do more than just the minimum set out in the guidance. Some interviewees told us that many employers only provide limited data on previous employment, such as to and from employment dates and sickness absence. Not all forces request a character reference.

The same code of practice advises that organisations obtain either five or ten years of employment history. The guidance for police forces advises only a minimum of three years' history should be obtained. An applicant's dismissal from employment four years prior would come to the attention of a security industry recruiter: it wouldn't come to the attention of a police recruiter. It is surprising that people who apply to work in the security industry would appear, in some respects, to receive closer scrutiny than people who apply to become police officers and staff. It is wholly unsatisfactory that some police applicants are appointed without any checks to confirm the accuracy of some important information they have provided on their application form. As many employers know, some applicants will lie on their forms. Applicants shouldn't proceed to the vetting stage until forces are as confident as they can reasonably be that they have provided accurate information.

Recommendation 1

By 31 October 2023, the College of Policing should update its guidance on the minimum standards of pre-employment checks that forces must carry out before appointing an officer or member of staff. Every chief constable should make sure their force complies with the guidance. As a minimum, pre-employment checks should:

- obtain and verify previous employment history for at least the previous five years (including dates of employment, roles carried out and reason for leaving); and
- verify the qualifications the applicant claims to have.

4. The initial vetting stage

In this and later chapters, we have taken account of various sources including the statutory Vetting Code of Practice (Vetting CoP), the current Vetting Authorised Professional Practice (Vetting APP), Government guidance on national security vetting and relevant case law.

An explanation of vetting regimes and processes

Police forces operate under two different vetting regimes: national security vetting and police vetting. National security vetting is 'owned' by the Cabinet Office and carried out by the United Kingdom Vetting Service. Police vetting is owned by the College of Policing and carried out by individual forces. There is some overlap between these regimes, but they assess different risks and have different decision-making criteria.

National security vetting focuses heavily on information security. Police vetting assesses an applicant's suitability based on their honesty and integrity and any vulnerability they may have to corruption and coercion.

Forces vet officers and staff to different levels depending on their role. The minimum level of force vetting required before they can join the police service is called recruitment vetting (RV). Some roles need a higher level of vetting due to the postholders' access to more sensitive information or due to the extent that the role involves working with vulnerable people. This is called management vetting (MV). In Chapter 5, we comment on our concerns about how effectively forces use MV to assess the suitability of police officers and staff to work with vulnerable people.

The Vetting CoP refers to the role of police vetting in terms of information security. The Vetting APP explains the role of vetting in assessing suitability to serve in the police service, either as a police officer, special constable, or member of police staff.

The Vetting CoP states that vetting is an integral part of a police force's framework of ethics and professional standards. Vetting is designed to identify individuals who are unsuitable to work within the police service because of:

- a criminal activity or association;
- a demonstrable lack of honesty;
- previous behaviour inconsistent with the Code of Ethics; and/or
- financial vulnerability.

The importance of integrity

The importance of integrity in police officers is self-evident. Decisions to grant vetting clearance must be made on all known information to allow for informed and balanced recruitment decisions.

That is why an applicant to become a police officer or police cadet is exempt from the protections established in the Rehabilitation of Offenders Act 1974 (ROA). They must disclose, no matter how minor or long ago they were received, all convictions, cautions and reprimands. The consideration of an applicant's criminal record is a critically important part of any vetting procedure.

If a police officer is involved in criminal proceedings against someone, then in accordance with Chapter 18 of the Crown Prosecution Service (CPS) *Disclosure Manual*, they must disclose their full criminal record to the CPS. This allows the CPS to consider what information regarding the officer should be disclosed to the defence solicitors. If a police officer has a criminal record, they could become a 'tainted witness', and in this way jeopardise any investigation they are involved in. This could severely limit the ways in which their force could deploy them.

Vetting has its limitations

When vetting enquiries reveal information about an applicant or their friends and family which may present a risk, such as involvement in criminal activity or financial concerns, this is known as adverse information. Some types of adverse information present greater risks and are therefore of greater concern than others.

Even the most thorough and complete vetting regime could never guarantee that an applicant wouldn't go on to become corrupt or become a risk to the police service. Equally, it would be wrong to assume that all applicants with concerning adverse information about their past would necessarily go on to commit acts of criminality or misconduct.

When serving police officers do go on to commit serious criminal offences, it is entirely reasonable to scrutinise their vetting. But vetting may not identify deeply hidden character traits. Vetting can be viewed as a safety net, but an imperfect one. There will always be a danger of unsuitable applicants 'slipping through'. Of course, the risk of this is greater if the vetting safety net has holes that are of the police service's own making.

The vetting process

The Vetting APP goes on to say that vetting aims to identify, assess, and manage risk relating to areas including, but not limited to:

- the protection of police assets;
- national security;
- public safety;
- public confidence;
- operational safety;
- leadership;
- corruption and coercion; and
- integrity.

The role vetting plays in public safety is of particular interest to our inspection. In explaining why vetting is necessary, the Vetting APP refers to public safety and public confidence. As well as having access to a wealth of police information, police officers enforce the law, exercising intrusive powers over other citizens. This will often be in relation to people who are vulnerable at that time. So it is vital that, as well as information security considerations, vetting decision-makers take full account of any factors relating to the safety of the public, particularly vulnerable people.

Following the initial vetting process, officers and staff granted clearance are subject to an 'aftercare' process under which they must, for example, declare any relevant changes in circumstances.

The Vetting APP gives guidance for forces to assess information and intelligence gathered during the vetting process by applying a two-stage test:

1. Are there reasonable grounds for suspecting that the applicant, a family member or other relevant associate:
    - is or has been involved in criminal activity;
    - has financial vulnerabilities (applicant only); or
    - is, or has been, the subject of any concerning adverse information?
2. If so, is it appropriate, in all the circumstances, to refuse vetting clearance?

When applying this test, we believe forces should have public protection as their primary consideration, but this is not clear in the Vetting APP. In Chapter 5, we say that the Vetting APP needs to be strengthened in order to give protection of the public, particularly vulnerable people, greater prominence.

Vetting Code of Practice

In the statutory Vetting CoP, the College of Policing establishes principles that, it says, should underpin all vetting decision-making. These include:

- treating each case on its merits;
- compliance with the standards laid out in the Vetting APP;
- the independence of vetting decisions;
- use of the National Decision Model (NDM); and
- the recording of the rationale for vetting decisions made.

The Vetting CoP also deals specifically with the factors to consider when assessing applications from individuals who have previously committed criminal offences.

Vetting Authorised Professional Practice

In March 2021, the College of Policing published the current Vetting APP, which replaced a previous version from 2017.

It sets out the minimum standards that should be applied for each clearance level and lists the minimum vetting checks that should be carried out on the applicant, their family, and associates. There is a large section dedicated to decision-making, which gives advice on how forces should assess information. This is to make sure decisions are balanced and proportionate when determining whether to grant vetting clearance. It includes decisions relating to the suitability of applicants with previous convictions and cautions, criminal associations, or financial vulnerabilities. In assessing risk and vulnerability, forces should consider all possible threats.

The College of Policing, its vetting documents, and their legal status

The College of Policing is the professional policing body whose purpose is to provide police forces with the skills and knowledge necessary for effective policing. Its principal responsibilities include setting standards and developing guidance and policy. The College of Policing has a statutory power (under section 39A of the Police Act 1996) to issue codes of practice relating to the discharge of their functions by chief officers of police. A chief officer of police must have regard to the code when discharging any function which such a code of practice relates to.

In October 2017, the College of Policing issued the Vetting CoP under this statutory power.

The Vetting CoP sets out standards expected of police forces in England and Wales in relation to vetting. Chief officers of police forces must have regard to what the code says but they are not bound by its terms; the code is not the law. That said, established principles of law require that they should follow it unless there are strong reasons for not doing so. They must be able to justify any departure from it.

The College of Policing produces APP following a detailed, evidence-based process, in consultation with other policing bodies. Most APP documents are published on the College of Policing's website. The college does not issue an APP document under any statutory power.

The Vetting APP sets out detailed guidance to the police forces of England and Wales. It is 240 pages long, compared to the Vetting CoP's 18 pages. As a result, it is more prescriptive. Because it isn't issued under any statutory power, there is no requirement in legislation that chief officers have regard to the APP. But where guidance such as the APP has been issued, there is a general expectation that forces will only depart from it with good reason.

In practice, it is unlikely that a chief officer would wish or need to depart from the terms of the Vetting CoP. The principles it sets out won't usually be controversial and don't generally prescribe any particular outcome or process. It is much more likely that a police force may not always wish to follow the precise terms of the Vetting APP, which is much more prescriptive. A court, or a body with regulatory or oversight powers such as the IOPC or HMICFRS, can scrutinise the justification for any such departure.

Vetting decision-makers must consider case law

A particular case which forces must be aware of in the context of making vetting decisions is the Court of Appeal case of R (RD) v Secretary of State for Justice & Ors [2020] EWCA Civ 1346; [2021] 1 WLR 262. In that case, a 13-year-old girl stole an item of clothing worth £20 from a high street store. She was arrested and admitted the offence. The police decided not to prosecute her and instead issued a reprimand.

After completing her schooling, the young woman went to university and obtained a degree in criminology. She decided to pursue a career in the police service and applied to South Wales Police for a police staff job. Her intention was to gain experience and then apply to become a police officer. The force rejected her application at an early stage in the recruitment process, purely because of her previous reprimand.

The court criticised the force's decision to reject in that specific case as it appeared to have a blanket rule against recruitment of any applicant with any criminal record. This case, although it pre-dates both the Vetting CoP and Vetting APP, shows how important it is for forces to make risk-based proportionate decisions and to decide each individual case on its own merits.

However, the case also contains powerful support for the importance of the principle that forces should be aware of an applicant's full criminal record so they can take informed and balanced decisions.

5. Our review of force vetting decisions

In our previous inspections of force vetting arrangements, we have focused on forces' compliance with various aspects of the Vetting Authorised Professional Practice (Vetting APP). For example, we have previously inspected whether all personnel had the right level of vetting for their role, and that forces were carrying out the minimum required vetting checks. A list of the minimum vetting checks required by the Vetting APP can be found in Annex A of this report.

Vetting units sometimes grant clearance to applicants with criminal convictions, or whose family or friends have convictions, or where other concerning adverse information is held. In principle, these may be appropriate decisions when all the circumstances of a particular case have been considered. For this inspection, we wanted to understand how effectively forces make these vetting decisions, for new recruits and for transferees.

In the DMIP report, we said that the vetting decision-making guidance in the Vetting APP appeared to give forces considerable latitude. This was in relation to the level of risk they are willing to accept when deciding on the suitability of applicants. We were concerned that this would lead to inconsistent vetting decisions being made by forces. So in this inspection, we wanted to assess how well the Vetting APP supports forces in making consistent and effective vetting decisions. And, if there is any evidence of inconsistency, whether the Vetting APP itself may be a contributory factor.

To do this, we drew together a review team comprised of a number of our regular inspectors as well as seven peer inspectors who were either leading national figures in police vetting, a current vetting manager in a police force, or both.

We contacted the forces being inspected in advance and explained our intentions to them. We asked them to identify police officers and staff who had been recruited to the police service or transferred from one force to another during the three-year period from October 2018 to September 2021. We asked forces to identify police officers and staff to whom they had granted vetting clearance during this period, who had previously committed criminal offences. We also asked the forces to identify any police officers and staff granted clearance over this same period, for whom the vetting process had revealed other types of concerning adverse information.

Vetting units could not readily access data to identify police officers and staff with concerning adverse information

Most, but not all, of the forces we inspected gave us details of individuals they had vetted who had committed criminal offences before joining the service. But none of the forces could give us details of cleared police officers and staff with other types of concerning adverse information, such as financial risks or having family or friends with criminal backgrounds. They had no means of producing these details other than by manually trawling through all their vetting cases.

We would have expected that every force would have had a process to flag such cases within their vetting IT systems and would therefore have this information readily available. This would help them to effectively monitor these cases. But worryingly, forces could not even tell us how many of these cases they had cleared though vetting. Despite this, by working with forces and using the limited data that some of them did have, we were able to identify many relevant cases. And during our inspection fieldwork, we identified some further cases to review.

Recommendation 2

By 30 April 2023, chief constables should establish and begin operation of a process to identify, within their vetting IT systems, vetting clearance records where:

- applicants have committed criminal offences; and/or
- the record contains other types of concerning adverse information.

Our vetting file review disagreed with many vetting decisions

We recorded details of all the vetting decisions we reviewed. The review team then discussed the cases where they had concerns about the vetting decision.

Although we found many examples of good decision-making, our vetting file review revealed some disturbing results, including numerous examples where we disagreed with the force's decision to grant vetting clearance. These examples included decisions about recruitment vetting (RV), transferees and appeals.

In total we reviewed 725 vetting files, consisting of 548 RV files and 177 transferee or re-joiner files. Of the 725 files reviewed, we chose 315 due to the type of adverse information the vetting process revealed. We chose the remaining 410 at random.

The review team unanimously disagreed with the decision to grant vetting clearance in a total of 68 cases, some of which are presented in this chapter. These occurred across all the forces being inspected. Due to the small sample size and the way we carried out the vetting file review, it would not be appropriate to presume any statistical significance from these figures.

There were a further 63 cases where the review team believed they may have agreed with the decision had the rationale contained greater detail, or potential risk mitigation measures been properly considered. That said, there were also many cases where we fully agreed with the decision and the supporting rationale to grant clearance. We found that the vetting unit in Nottinghamshire Police recorded the vast majority of their vetting decisions well, with a good level of detail, reference to relevant Vetting APP risk factors and effective use of the NDM.

The Vetting APP gives advice regarding convictions and cautions

The Vetting APP states that the existence of a criminal record would clearly indicate reasonable grounds for concluding that an individual is, or has been, involved in criminal activity. It also states that it is not appropriate to identify a prescriptive list of convictions and cautions that should lead to a vetting rejection. Instead, decision-makers should consider each case on its own individual merits in relation to the role being carried out and the assets being accessed.

Both the Vetting CoP and Vetting APP state that a vetting application is to be rejected in all cases if:

- any type of custodial sentence was imposed, or
- the applicant is (or has been) a registered sex offender.

For all other convictions or cautions, except where the exceptions of the ROA apply for police staff and non-police personnel, there is a “rebuttable presumption” that applications should be rejected. This means the applicant with the convictions or cautions is presumed not to be suitable and should be rejected, unless there is other information to suggest they should be given clearance.

In particular, the Vetting APP states that the following should result in rejection:

- offences where vulnerable people were targeted;
- offences motivated by hate or discrimination; and
- offences of domestic abuse.

The Vetting APP further states that particular care must be taken with offences of dishonesty, corrupt practice, or violence. Although the rebuttable presumption is that these should lead to rejection, there will be cases where vetting clearance may be justified. For instance, it could be justified if the offence was committed as a juvenile, it was not serious, and the applicant has demonstrated a commitment to help individuals or communities in the subsequent years.

Convictions and cautions should be subject to a proportionate risk-based assessment. Forces should consider both the circumstances of the offence and the potential effect that those circumstances may have on the applicant's role within the police service. This includes their suitability to have access to police assets and vulnerable people. The Vetting APP gives a comprehensive list of factors for forces to consider when making the assessment. It states that the emphasis should be on making a balanced and proportionate decision, taking account of the:

- seriousness of the offence;
- level of involvement of the applicant in the criminal behaviour;
- motivation of the applicant in committing the offence;
- openness of the applicant;
- level of clearance required;
- length of time that has passed since any convictions have been obtained;
- evidence of repeat offending;
- impact on public confidence in the force or police service;
- relevance of the information to the post for which clearance is required, including unsupervised and unrestricted access to assets and premises;
- nature of the role applied for, including any involvement in investigations or as a potential witness in a prosecution; and
- the applicant's behaviour in the period since the conviction or caution.

The Vetting APP advises forces to take particular care in relation to cautions, reprimands and warnings issued to juveniles. These are designed as a form of early intervention and intended to help prevent crime, rehabilitate offenders, and promote welfare. The APP states that the potential effect of youth matters on suitability for vetting clearance will diminish over time.

Vetting APP gives advice on mitigating risks

The Vetting APP gives advice for forces on using risk mitigation strategies. The APP says that where a decision is made to grant clearance following assessment of identified risks, forces must consider whether there are reasonable, proportionate, and manageable mitigations that can be put in place. It gives examples such as geographical posting restrictions, additional aftercare and reporting requirements, and engagement with supervisors and welfare departments.

Some forces granted vetting clearance to applicants with a history of criminal offending

Our vetting file review revealed cases in many forces involving applicants who had committed criminal offences, where we disagreed with the decision to grant vetting clearance. Our main concern related to vetting decision-makers not taking full account of all the relevant Vetting APP factors when assessing the risk. In several cases, we found that the decision relied too heavily on the passing of time and the fact that applicants had openly revealed the information.

We found applicants who had received vetting clearance after committing offences such as robbery, indecent exposure, possession of controlled drugs, drink-driving and domestic abuse-related assaults. We found no evidence that decision-makers in these cases had considered relevant factors, such as: the seriousness of offences; offences that were domestic abuse-related; repeat offences; and offences against vulnerable people. In such cases, there was also no evidence to show that forces had adequately considered the potential effect on public confidence or the reputation of the police service.

During our vetting file review, we found that forces often referred to criminal acts as being “one-off”, that is, isolated examples of criminal activity.

Case studies

All of the case studies in this report relate to the period between October 2018 and September 2021.

Case study 1

An applicant for the Special Constabulary was granted vetting clearance. In the mid-1990s, he received an adult caution for making threats to commit criminal damage. Six years earlier, when he was a juvenile, he was convicted of indecent exposure and received a 12-month supervision order plus £25 costs.

Over a 13-year period, he applied 3 times to the same force but was rejected on each occasion. On the final occasion he appealed, and the vetting manager granted clearance.

The rationale for this clearance included the passing of time since the applicant had last come to notice and the fact that he was a juvenile when he was convicted of indecent exposure. The rationale stated that there was “minimal risk” to the force.

We examined the detail of the indecent exposure offence, which was available in the vetting file. This showed that over a two-week period, the applicant had indecently exposed himself to the same woman on seven separate occasions. On each occasion he stood at his bedroom window, coughed to attract her attention, and then masturbated.

The rationale didn't make any reference to these circumstances or any assessment of his motivation in committing the offence. Nor did it give any evidence that the decision-maker considered the risk posed to members of the public. There was no consideration of any risk mitigation measures or the potential for this appointment to negatively affect public confidence in the force or the police service.

Anyone behaving this way after the introduction of the Sexual Offences Act 2003 and receiving a similar sentence from a court would have been placed on the sex offenders' register and been subject to notification requirements. This reflects Parliament's view of the seriousness of such offending. It is also a highly relevant indication as to the likely effect on public confidence in the police when a person with a history of sexual offending is recruited. In accordance with the Vetting APP, this would have been an automatic rejection.

Case study 2

An applicant for a police community support officer (PCSO) post was granted vetting clearance. Seven years earlier, he had received an adult caution for a common assault. This was a domestic abuse case during which he slapped his partner across the face.

The rationale focused solely on the length of time that had passed since the offence was committed. There was no evidence the force had considered the fact that the offence consisted of domestic-related violence and was committed as a mature adult. There was no consideration of any risk mitigation measures, in line with the advice in the Vetting APP, or the potential for this appointment to negatively affect public confidence.

Case study 3

An applicant for a police officer post was granted vetting clearance. Nearly two decades earlier, as a juvenile, he received a final warning for an offence of robbery. This offence was committed against an 80-year-old woman. During the crime two offenders, one of whom was the applicant, knocked the victim to the ground and stole her handbag. The applicant had not come to police attention in the intervening period. Initially, the vetting unit decided to refuse clearance. At this point, the rationale identified relevant factors including the passing of time, the fact that the offence was committed by a juvenile and noting that the victim was a vulnerable elderly woman.

Following the refusal decision, the applicant appealed. An appeal panel, chaired by a senior police officer, recommended clearance. Other than noting that the applicant had shown his honesty and integrity by declaring the matter, the panel didn't record any further information to justify their recommendation. The force vetting manager (FVM) then granted vetting clearance without recording any rationale for their decision whatsoever.

We found no evidence that the force, in reaching its vetting clearance final decision, considered the serious nature of the offence and the fact that it was targeted against a vulnerable person. The force didn't consider any risk mitigation or the potential for this appointment to negatively affect public confidence.

Some types of adverse information can be challenging for vetting decision makers

Some vetting decisions are complex and require careful assessment of a range of different types of information. This can be particularly difficult when cases are borderline.

Frequently, adverse information relates to an applicant's previous convictions or cautions. But vetting may also reveal information about their family or friends who themselves may have previous convictions. This also counts as adverse information.

Some types of adverse information can be particularly challenging: intelligence about criminal activity; being named as a suspect but where there is no formal outcome, such as a conviction; and any such information about a family member or close associate. Forces need to consider all adverse information on a case-by-case basis.

Vetting units must also consider other factors, such as applicants' financial status and, for applicants with previous police service, their police disciplinary record. Forces must also carry out a military or MoD service history check on all applicants who have previously served in the armed forces.

The Vetting APP gives guidance for forces on how to assess these different types of information. It states a range of factors for forces to consider. The Vetting APP recommends the use of the NDM. There is national online training for vetting managers in its use.

We found vetting clearance was granted to applicants with other concerning adverse information held about them

As well as cases where applicants had a criminal record, our review team also examined several cases with various other types of concerning adverse information.

We examined several examples where applicants had come to police attention as suspects in criminal investigations. Often, these investigations had been concluded as 'no further action' and the case didn't lead to a prosecution or other formal outcome such as a caution or reprimand.

The Vetting APP advises forces that intelligence and other non-conviction information may lead to reasonable grounds for suspecting an applicant's involvement in criminal activity. In considering the weight to be applied to untested allegations, forces should take the grading of the intelligence into consideration. But the Vetting APP gives no further guidance for forces in how to assess applicants' suitability based on such intelligence.

Case study 4

A police officer applicant was granted vetting clearance. Five years earlier, he had come to police attention for speeding and other driving-related matters. He also declared that he had been convicted abroad of an attempted theft in that same year. He was fined for this offence. There was also police intelligence, from around the same period, relating to the applicant's possible link to drug supply. And in recent intelligence, a man was seen with a firearm and involved in a police pursuit. The vehicle in question was a hire vehicle and the address for the hire was the home address of the applicant. There was also recent intelligence linking a separate vehicle, registered to the applicant, to an offence of aggravated burglary. In that offence, five offenders had threatened the occupants with a metal bar before stealing jewellery.

When granting vetting clearance, the force didn't fully assess the risks associated with this applicant. When we expressed our concerns about this decision to the force, it was clear from its response that the force had dismissed both the attempted theft conviction abroad and the intelligence picture. The force put no risk mitigation measures in place at the time of the vetting clearance and appeared not to do so after our vetting file review.

In this case, the mutually corroborative nature of the intelligence and other information caused us substantial concern.

Forces aren't giving enough weight to non-conviction information relating to applicants

Where an applicant has previously come to adverse police attention – for example, been arrested, a subject of a criminal allegation, or a subject of investigation – but this has not led to a criminal conviction, the Vetting APP advises forces to make a case-by-case assessment. A force's assessment should include consideration of the:

- number of allegations;
- severity of the allegation(s);
- credibility of the allegation(s), including whether there is irrefutable evidence to show these are false or malicious;
- reasons for the matters not being taken forward;
- amount of time that has passed since the matters being considered; and
- age of the applicant at the time.

We found that some forces were not giving enough weight to occasions when applicants had been arrested but no action resulted. We disagreed with vetting decisions in several forces where we found them making decisions with no evidence that they had fully considered all the risk factors above. For instance, some forces didn't enquire deeply enough into the circumstances to understand the reasons for no further action being taken.

In some of these cases, it seemed to us that forces felt constrained in their ability to use non-conviction information to inform their decision. In one force the vetting decision-maker stated that the non-conviction information could not have a bearing on their decision. This is simply wrong. As a result, the force granted vetting clearance, without sufficient justification in the rationale, to people who had come to attention as suspects in crimes such as domestic-related assaults, racially aggravated damage, sexual touching, serious violence, and rape.

Case study 5

A police officer applicant was given vetting clearance. The applicant had a conviction for drink-driving and driving with no insurance, 18 years prior to his application. Four years later, he was arrested, but not prosecuted, for intimidating a witness. In the same year, he was also arrested for a domestic-related assault. A woman was left with marks to her neck. There was no evidence on the vetting file to confirm or refute whether these two arrests were linked. Five years before his application, the applicant was again arrested for a domestic-related assault. In this case too, a woman allegedly suffered injury marks to her neck.
The rationale focused on the passing of time, stating that the "traces on applicant are significantly aged". There was no evidence that the force had considered the full circumstances of the offences, including the reasons for no further action being taken, for any of the arrests. The rationale didn't make any comment on the fact that two separate domestic-related incidents had occurred, where two women were both allegedly left with marks to their neck.

Case study 6

A police officer applicant was granted vetting clearance. He declared that he had been cautioned for shoplifting as a juvenile, although vetting enquiries could not confirm this. He also declared that 20 years prior to his application, as a teenager, he had been accused of rape. He was charged, but a senior prosecutor subsequently withdrew the charge. The issue was one of consent, as the applicant had claimed that the actions were consensual.

The vetting unit interviewed the applicant about the incident and consulted officers who had been involved in presenting the case to the CPS. The head of the professional standards department (PSD) countersigned the decision to grant clearance. But the recorded rationale for granting clearance didn't contain enough detail to explain the decision. The force didn't introduce any risk mitigation measures.

Case study 7

A police officer applicant was granted vetting clearance. A Police National Database (PND) check revealed that the applicant had been investigated five years earlier for a sexual assault offence at a nightclub. The recorded rationale for granting clearance contained scant detail. There was no reference to the specific circumstances of the alleged offence. There was no apparent consideration of the relevant factors required in the Vetting APP (which include the severity of the offence and the likelihood of the alleged offence having taken place).
The applicant was not given a vetting interview. The PND revealed that the victim's initial account included criminal allegations of non-consensual kissing, and touching of her breasts and vaginal area, while in a nightclub. She later withdrew her criminal allegation and didn't support any further police action.

A senior manager expressed the view that this was a case of one person's word against another. They told us: "Innocent until [proven] guilty when there is no evidence – just because … [there is a current] spotlight on these types of offences, we cannot presume someone's guilt with no evidence." We believe it is wrong to equate a vetting decision with a finding or assumption of guilt. The Vetting APP is clear that forces should take account of non-conviction information. We can't say categorically that this case should have resulted in a rejection, but the force appeared to simply disregard the information. There was no evidence of the force considering why the woman withdrew her allegation, or any risk mitigation measures.

Case study 8

A police officer applicant was granted vetting clearance. Over 20 years prior to his application he had received a conviction for drink-driving and an adult caution for theft from an employer, as well as more recent minor traffic offences. Ten years ago, he was investigated for offences of racially aggravated criminal damage and public order. He was linked to these offences via his vehicle.

There was no evidence of the force enquiring into the details of this racially aggravated offence. This was despite there being an opportunity to do so, as the victim in that case had been an off-duty member of the Special Constabulary. There was also minimal assessment of the Vetting APP factors relating to the applicant's history of offending.

A conviction, caution or other formal outcome gives more compelling evidence than criminal intelligence or other non-conviction information, such as being a suspect in a crime. But, as we said above, we do not consider that taking a view of "innocent until [proven] guilty", as we heard from one force, is the right approach. The threshold is not 'beyond all reasonable doubt' as it would be for a criminal case. A refusal of vetting clearance isn't a finding of guilt to the criminal standard. In the Vetting APP's two-stage test, the threshold is much lower than the criminal standard. It is set at 'reasonable grounds to suspect involvement in criminal activity'. Forces should be carrying out a full and careful analysis of non-conviction information and police intelligence cases. But sometimes they are overlooking such information with minimal rationale and no mitigations in place.

Forces sometimes overlook other risks

As well as applicants suspected of committing crime, we identified occasions when vetting decision-makers overlooked other significant risks. These included: applicants with financial risks; applicants whose family had concerning criminal traces; and applicants who provided deliberately false, incomplete, or misleading information as part of the vetting process.

We found vetting clearance granted to some individuals with financial risks and vulnerabilities

Vetting enquiries include financial checks to assess whether applicants could become vulnerable to financial inducement. This could be due to being in financial difficulty or showing signs of financial irresponsibility.

The Vetting APP lists several factors to help forces assess applicants' financial vulnerability, including credit cards, overdraft arrangements and use of payday loans. Applicants who can show their commitment to debt management arrangements over several months may be considered for clearance. But the Vetting APP advises that it is unlikely clearance will be granted if the applicant has existing county court judgments (CCJs) against them or they have been registered bankrupt.

During our vetting file review, we found that some forces closely monitored applicants they had cleared who carried financial risks. We found examples in several forces of applicants with debt management plans that they were following. The rationale specified that these applicants' continued clearance was dependent on them continuing to show financial responsibility.

But in some forces, we also found examples of applicants with financial vulnerabilities who had been granted clearance without enough rationale recorded to justify the decision, and without any financial aftercare in place. This included applicants with outstanding CCJs, undischarged debts from defaulted loans and debt management plans that had only been entered into just as vetting was taking place.

We found one force that had a vetting officer with specific responsibility for this type of financial aftercare. Having someone within the vetting unit with responsibility for this type of financial risk mitigation allows the force to accept applicants with financial risks who may otherwise have been refused clearance.

Case study 9

Vetting clearance was granted to a police officer applicant following appeal. The applicant had revealed one previous CCJ, which they had settled. But financial vetting enquiries revealed six further live CCJs, totalling over £11,000, linked to the applicant. The force refused vetting. The applicant then appealed.

The rationale for the refusal decision was not available. The only document we could inspect was the letter to the applicant with the result of the appeal. This document indicated that the force granted clearance subject to regular financial checks, but there was no evidence that it had carried these out. There was also no evidence that the force had scrutinised the possibly deliberate omission of the information relating to the additional CCJs.

Case study 10

A police officer applicant was granted clearance by an appeals panel. Initially, the FVM rejected him for failing to declare a caution for possession of cannabis from over 20 years earlier and a more recent traffic conviction. The applicant had also failed to disclose five defaulted accounts with debts totalling over £5,000.

The vetting unit had recorded detailed and structured rationale regarding the applicant's rejection for non-declaration of the caution and traffic offence. But these records didn't include the applicant's financial situation. The appeals panel upheld the appeal after the applicant submitted a letter, explaining that he thought he had been "told off" rather than getting a caution.

The vetting panel held a vote and unanimously determined that it would be disproportionate to refuse clearance. There was no evidence that the vetting panel explored the applicant's financial situation, and the force didn't interview him.

Making vetting decisions when adverse information relates to family or friends

The Vetting APP states that where adverse information relating to relatives or associates is revealed, the force should consider the risk that these people pose. Forces should consider such things as convictions or cautions for recordable offences, or intelligence suggesting involvement in criminal activity, along with:

- the likelihood that the applicant's performance may be negatively affected, for example, through adverse pressure or a conflict of interests;
- the nature, number and seriousness of the offences or involvement in criminal activity, as well as the time over which these took place;
- the likelihood of damage to the force's operational capability;
- the potential for information leaks; and
- whether the circumstances are likely to bring discredit to, or embarrass, the police service or police force.

Risk mitigation should be used more effectively

We referred earlier to the advice contained in the Vetting APP about putting risk mitigations in place, following assessment of identified risk. A key factor for forces to consider in relation to this is the nature of the relationship between the applicant and the third party. We found examples of forces accepting applicants whose family members had extensive criminal records.

Some forces put geographical posting restrictions in place to make sure these applicants couldn't work in the area where such a family member was based. But we also found examples where the officer still lived in the same household. Some forces can mitigate the risk of such vetting clearances by carrying out routine IT monitoring to look for potential information leaks. Others cannot use such measures, due to a lack of IT monitoring capability or staff to carry this out (we expand on this later in this report).

Clearance granted to some applicants with links to organised crime

A failure to adequately mitigate risks may represent a significant corruption threat for forces. This is particularly true where the applicant's family have links to serious and organised crime. In such cases, there is a heightened risk of compromise to operations and information leaks.

We found a small number of cases where forces granted vetting clearance despite family members being involved in drug supply offences or being part of organised crime groups. In these cases, the relevant forces didn't provide adequate rationale for their decision. Despite the obvious risks in recruiting officers in such circumstances, there was also no evidence of risk mitigation measures being put into place.

Forces should not grant vetting clearance if they cannot mitigate against the risks involved

Some forces have adopted 'risk appetite' as a phrase to describe their level of tolerance to risks posed by applicants. Too great a risk appetite means forces may be recruiting applicants who are not suitable to join the police service.

A force vetting unit on its own cannot successfully put mitigations in place. The capability of force counter-corruption units (CCUs) varies greatly. Some forces have limited means to monitor their IT systems, and others have limited staff numbers to do such work even if they have the capability. So before accepting applicants with known risks, forces should think very carefully about their ability to mitigate the risks.

If a force is not able to carry out any proposed mitigation, this fact should be considered in the vetting decision and should, in our view, lead to a rejection. But the vetting unit alone should not determine, or be responsible for implementing, any required risk mitigation measures. The risks and the associated mitigation measures should be managed by professional standards units, CCUs and/or HR departments. This should be made clear in any documented rationale where a force decides to grant vetting clearance to an applicant with an identified risk.

We asked some vetting managers what knowledge they had of the capability and capacity of force CCU and HR departments to put mitigations in place. We found they had limited, if any, knowledge. We also asked who decided what, if any, mitigations were put in place. Almost universally, the answer was the force vetting unit.

There were limited examples of vetting decision-makers considering the force's capability and capacity to monitor mitigations when granting clearances.

Recording a mitigation strategy that cannot then be put into practice is of no value. Indeed, it could be worse than that, as the decision-maker may decide to grant vetting clearance with a false sense of security that the applicant's work and behaviour will be monitored.

Placing restrictions on postings relies on effective HR processes

As we discussed earlier, some risk mitigation strategies are designed to restrict applicants from being posted to certain parts of the force area. In setting this condition, vetting units are reliant on HR departments maintaining records of this (potentially for a long period of time) and on HR personnel being vigilant to prevent it happening.

Additional 'use of force' scrutiny could be used as a risk mitigation

Occasionally, forces grant vetting clearance to applicants with convictions, cautions or other formal outcomes for offences of violence, or where a transferee's PSD history indicates possible excessive use of force. In such cases, it might be sensible for forces to introduce a process in which any use of force by these officers or staff in connection with their duties receives additional scrutiny. But we have not found any force introducing such risk mitigation strategies.

Case study 11

An applicant for the Special Constabulary was granted vetting clearance. He had an adult caution for a public order offence, and there was extensive criminality within his family. His brother was actively involved in organised crime, with convictions for violence and drugs. According to the papers we examined, the brother had been "of interest" in murder and kidnap investigations. Several police forces across England and Wales held intelligence in relation to the brother.

The force had interviewed the applicant and concluded that the risks were mitigated "as there is clear distance between the applicant and the family". This was after the applicant told the force he was estranged from his family. The force didn't take any action to verify the applicant's claim that he no longer had links with other family members. The force granted vetting clearance.

The force didn't consider the potential risk of infiltration and the wider risk of public confidence being affected. There was no consideration of any risk mitigation strategy – for instance, carrying out routine IT monitoring for any access to information or intelligence relating to the organised crime group.

Vetting decisions in such cases should always take account of the force's capacity and capability to implement any required risk mitigation strategy.

Recommendation 3

By 30 April 2023, chief constables should take steps to make sure that, when granting vetting clearance to applicants with concerning adverse information about them:

- vetting units, counter-corruption units, professional standards departments, and HR departments (working together where necessary) create and implement effective risk mitigation strategies;
- these units have enough capacity and capability for this purpose;
- responsibilities for implementing specific elements of the risk mitigation strategy are clearly defined; and
- there is robust oversight.

Forces sometimes grant vetting clearance to applicants who have been dishonest in their applications

For all police officers and staff, honesty should be the most basic of requirements. It is reasonable to expect that an applicant will honestly answer any question that is put to them, such as a request to disclose any criminal record they may have.

The Vetting APP lists several factors for particular scrutiny. In most cases, the presence of any of these factors should lead to a vetting rejection. One such factor is when an applicant provides false or deliberately misleading information in their vetting application form.

Our vetting file review revealed occasions when forces had granted clearances to applicants who had provided false or deliberately misleading information on their vetting application forms. The cases concerned a failure to disclose information that related to criminal offences involving drugs and offensive weapons, associations with criminals, convictions, and financial problems.

In some cases, vetting decision-makers interviewed applicants and investigated the reason for non-disclosure. But we also found examples where they didn't investigate thoroughly enough and granted vetting clearance without giving the apparent non-disclosures sufficient scrutiny.

Forces should make more effective use of vetting interviews

We found that forces used vetting interviews infrequently. We found numerous cases where vetting enquiries revealed concerning adverse information, but forces had not interviewed applicants to clarify the issues. Or, when forces had interviewed the applicant, in many cases they hadn't made a record of the interview or retained a copy. The Vetting APP contains a large amount of guidance for forces on how to carry out such interviews. In many borderline cases, interviewing applicants would help decision-makers assess their suitability.

Area for improvement 1

Forces' use of vetting interviews is an area for improvement. In more cases, forces should interview applicants to explore adverse information of relevance to the case. This should help with assessing risk. When they carry out such interviews, forces should keep accurate records and give copies of these to interviewees.

Case study 12

A force vetting unit rejected a police officer applicant who had family members, including his brother, with extensive criminal backgrounds. Following an appeal, the force granted vetting clearance.

In his vetting application form the applicant stated that he only had minimal contact with his brother. The applicant claimed that they only communicated a couple of times a month via social media. Later enquiries by the vetting unit found that the applicant and his brother lived at the same address. The rationale for the initial refusal stated that the applicant had been "economical with [the] truth".

Following an appeal, a vetting officer interviewed the applicant. The applicant said he had taken the difficult decision to distance himself from his family. The force noted the discrepancy between the low level of contact with his brother which the applicant claimed and the fact that they lived together. But the force stated in the rationale for granting clearance that this was "not significant enough to deny vetting to a young man [who] has wanted to fulfil his dream of joining the police".

The force was able to use routine IT monitoring to mitigate against the risk of information leaks and the applicant was required to submit notifiable association forms. The notes of the interview where the force challenged the applicant about the deliberately misleading information, and the reasons he gave for supplying this, were not available on the vetting file.

Case study 13

Having served as a PCSO, an applicant applied to transfer to another force. The applicant was granted vetting clearance. Various members of the applicant's family, who lived in different parts of the country, were linked to criminal behaviour. Two years before he became a PCSO, the applicant had been involved in a domestic incident with a partner in which he hit them. The applicant admitted the offence, but the victim told police they didn't want to pursue matters and the case resulted in no further action. The applicant didn't declare this incident on his application form. The vetting officer suggested the applicant may "not have considered it an investigation based on the nature of the incident" and that it would be "harsh to decline" vetting clearance. The vetting manager endorsed this approach, stating in relation to his non-disclosure, that he would "give him the benefit of the doubt". The force didn't carry out a vetting interview to determine why the applicant failed to disclose or to establish the level of contact he had with his various family members. The force granted clearance without any mitigation measures.

Some phrases we found used within the vetting units in case studies 12 and 13 didn't reassure us that the protection of the public, police information or operations was at the forefront of the decision-makers' minds. (These were "give him the benefit of the doubt"; "harsh to decline"; and "not significant enough to deny vetting to a young man [who] has wanted to fulfil his dream of joining the police"). If such attitudes are widespread, and our evidence suggests they may be, the police have their priorities wrong.

Vetting decision-makers should use information from applicants' social media accounts more effectively

The forces we visited were all examining applicants' publicly available social media profiles. For some forces, this is a relatively new practice, and it was clear that some forces are more adept at this than others. We found examples of forces apparently disregarding concerning material revealed in their examination when making vetting decisions.

The Police Uplift Programme (PUP) has granted funding to the national vetting portfolio to carry out a pilot scheme using a commercially available social media analytical tool. This is aimed at automating scrutiny of applicants' social media profiles and is expected to improve efficiency.

We found forces making increasing use of social media research as a vetting enquiry. We discovered language and comments, attributable to vetting applicants, that were potentially discriminatory, inflammatory, or extremist. Forces were generally addressing this through words of advice to applicants regarding their future use of

social media. Worryingly, none of the files we reviewed containing concerning information about an applicant's use of social media resulted in their vetting application being rejected. Sometimes forces didn't include any reference to this social media content within decision rationales.

The Vetting APP provides brief guidance in relation to social media. It states that:

> "Forces should check content on publicly available social media sites for the purposes of service reputational reassurance, and to ensure that the applicant's online behaviour is compatible with the Code of Ethics or Standards of Professional Behaviour.
>
> - The applicant must use social media responsibly and safely.
> - The applicant must not have published anything that could reasonably be perceived by the public or by policing colleagues to be discriminatory, abusive, oppressive, harassing, bullying, victimising, offensive or otherwise incompatible with policing principles.
> - The applicant must not have published, or offered to publish, any material that might undermine their reputation or that of the policing profession, or might run the risk of damaging public confidence in the police service."

On the basis of our findings, it seems that forces are now starting to follow this guidance. But those making vetting decisions need better training on how to incorporate the results of social media research into these decisions. In addition, the Vetting APP should make clear that online behaviour not compatible with the Code of Ethics, which include the Standards of Professional Behaviour, is likely to lead to rejection.

Vetting APP needs to be strengthened

The guidance for vetting decision-makers within the Vetting APP needs to be changed to make sure that it puts greater emphasis on recording rationale. Decision-makers should note all identified risks, including any risks to the public, and weigh up all relevant factors when coming to a decision.

Recommendation 4

By 30 April 2023, chief constables should make sure that, when concerning adverse information has been identified during the vetting process, all vetting decisions (refusals, clearances and appeals) are supported with a sufficiently detailed written rationale that:

- follows the National Decision Model;
- includes the identification of all relevant risks; and
- takes full account of the relevant risk factors described in the Vetting APP.

Recommendation 5

By 31 October 2023, the College of Policing, working with the National Police Chiefs' Council lead for vetting, should change the Vetting APP, to give improved clarity in relation to:

- a greater focus on protecting the public;
- mitigation factors that may be employed;
- the weight to be applied to adverse information found on social media; and
- an obligation to record sufficiently detailed rationale, noting all identified risks and taking full account of all relevant factors, when coming to a vetting decision.

An updated decision-making template would help vetting officers to assess all risks

The Vetting APP contains a vetting decision record form. However, the review team believed that an updated and more comprehensive decision template form would assist forces to standardise vetting decisions. This would improve both the application of the Vetting APP and the use of the NDM. On the basis of the findings of the vetting file review, the following should be included in the template:

- all adverse information found through vetting;
- what information has been considered;
- what information has been discounted;
- the level of risk presented and whether it can be managed;
- what risk mitigation has been considered;
- what risk mitigation is achievable, sustainable, and proportionate;
- what consultation has taken place with other units (such as the CCU);
- whether any cultural advice has been sought, or advice relating to any protected characteristic;
- the details of any interviews with the applicant (and full notes of interviews should be placed on the file for future reference);
- the rationale for not holding interviews with the applicant, if these were considered and not carried out;
- a full record of all vetting activity carried out; and
- where clearance is refused, instructions on what can be disclosed to the applicant and what can't.

Recommendation 6

By 31 October 2023, the College of Policing, working with the National Police Chiefs' Council lead for vetting, should include a vetting decision-making template within the Vetting Authorised Professional Practice, to standardise decision-making.

Errors in vetting clearance decisions

Our vetting file review found examples of what we considered to be poor vetting decisions. But we also found instances where forces had granted vetting clearance apparently in error. These ranged from what appeared to be administrative oversights to decisions where the provisions of the Rehabilitation of Offenders Act 1974 (ROA), relating to the issue of spent convictions, had been wrongly applied to police officer roles.

Case study 14

An applicant to be a police officer was given vetting clearance and had a start date to join the police soon after the conclusion of our vetting file review. The applicant had made two previous applications, which had both resulted in the force refusing to grant clearance. Approximately ten years earlier, police had executed a warrant to search premises suspected as being used as a brothel. The applicant was a tenant at these premises and was sub-letting a flat to a woman who used it for soliciting sex. The applicant had been present at the property when the police executed the warrant. He signed a first warning letter to decease soliciting of sexual acts under section 33A of the Sexual Offences Act 1956.

After the police investigation, the applicant remained in a relationship with the woman, which he described as being on a "friends with benefits" basis. The woman remained a sex worker, with profiles on adult websites. There were very strong rationales for each refusal, detailing the risks and potential reputational damage if vetting clearance was granted.

Following his third application, the force granted clearance inadvertently. The vetting decision-maker apparently misread the decision log, thinking it recommended clearance when in fact it was another refusal. This resulted in clearance being granted due to an administrative error. We brought the case to the attention of the force vetting lead for immediate review.

Case study 15

Recruitment vetting (RV) clearance was granted to a PCSO applying to become a police officer in their own force. About 14 years earlier, as an adult, the applicant had received a cannabis warning. He declared this during the vetting process. Five years later, he had received a warning and then a penalty notice, also for possession of cannabis. The applicant didn't declare the last two items during his PCSO vetting: they were not relevant for that post due to the provisions of the ROA. But he didn't later declare them for his police officer application, to which they were relevant.

The applicant was given a vetting interview. He still didn't disclose the later warning or the penalty notice, but these came to light during the force's vetting checks. The force granted clearance despite the apparent deliberate omission of the additional drugs matters. The rationale didn't include the force's assessment of the risks associated with evidence of repeated drugs offences, or any consideration of what deliberate non-disclosure could imply in relation to honesty and integrity. The force then recorded within the decision rationale that the offences were not relevant due to the ROA. This is incorrect as police officers are exempt from the protections of the ROA.

Case study 16

A police officer applicant was granted vetting clearance. Five years earlier, he had received an adult caution for an offence of affray. The applicant disclosed this in his vetting questionnaire. For context, the male victim of the affray was initially the aggressor in the case. But the applicant and a friend then ran after this man and pulled him to the ground. The applicant punched the man and his friend kicked him. In granting clearance, the force acknowledged the potential for the previous caution to make the officer a 'tainted witness' in accordance with Chapter 18 of the CPS *Disclosure Manual* and consulted with the head of PSD. The vetting decision-maker's rationale was that although the applicant had committed a criminal offence, he was not the aggressor, he had over-reacted, and the retaliation was not sustained. The force recorded that the "violence was not aggressive". And as the offence occurred six years ago, it assessed that the applicant posed no risk.

This observation about the applicant's violence not being aggressive was unconvincing. It was our opinion that the force had wrongly concluded that the actions of the applicant were justified by the earlier behaviour of the 'victim'. It is clear to us from the circumstances that the criminal act was retaliation and not self-defence. The FVM acknowledged that in accepting the adult caution the applicant had taken responsibility for his criminal offence. They expressed the view to us that the decision-maker may have felt a degree of sympathy for the applicant. If so, it was misplaced.

The force didn't consider interviewing the applicant or imposing any risk mitigation strategy, such as enhanced monitoring of his use of force.

Forces need to quality assure vetting decisions

Some forces have introduced a process to review a sample of vetting rejection decisions. In particular, forces use these reviews to check the validity of rejection decisions relating to persons with known protected characteristics. Forces use practices like this to help improve the representation of people with protected characteristics in their workforce.

Generally, this helps them fulfil their obligations under the public sector equality duty (in section 149 of the Equality Act 2010). Monitoring data in this way helps forces to assess whether the vetting processes are disproportionately affecting those with a particular protected characteristic (and thereby may involve indirect discrimination). It also helps forces to further opportunities for people with different protected characteristics.

We asked vetting managers if there was any process in their force to routinely quality assure vetting clearances. Some forces told us they occasionally consulted with the head of PSD for difficult cases. Others told us they sometimes use vetting managers in another force to carry out peer reviews of individual cases. We also heard from a small number of forces that have recently introduced processes to randomly select a proportion of vetting decisions for internal review. In our DMIP report, we commented on the Metropolitan Police Service (MPS) sampling five percent of vetting cases to see whether the enquiries had been carried out correctly. The force gives feedback to the vetting officers involved in these cases.

Another force has introduced a random sampling of ten percent of cases, but we heard that occasionally people have joined the force before the dip sample was done. Clearly, such sampling would be more effective if the force completed it before appointing applicants. This would allow the force to re-consider planned vetting clearances if the review identified concerns.

Given the number of occasions where our vetting review team disagreed with vetting clearance decisions (including cases where there appeared to have been an obvious error) there is a clear case to introduce more extensive and routine quality assurance processes. These should include a review of clearance decisions where there are identified risks.

Recommendation 7

By 31 October 2023, chief constables should introduce an effective quality assurance process to review vetting decisions, including routine dip sampling of:

- rejections; and
- clearances where the vetting process revealed concerning adverse information.

Disproportionality in vetting decisions

The Vetting Code of Practice (Vetting CoP) states that forces should monitor their vetting clearances and refusals to make sure that people with protected characteristics are not unfairly treated. If decisions are found to disproportionately affect certain groups, for example people with disabilities or from minority ethnic groups, then forces should take steps to understand the reasons for this.

The Vetting APP also refers to the risk that vetting can affect under-represented groups disproportionately. While referring to the need for forces to be representative of the population, it states that vetting managers should take every opportunity to support forces in their recruitment and retention of applicants with protected characteristics. They should do this “without any bias”.

The Vetting APP also states:

> "Forces must monitor vetting applications, at all levels, against protected characteristics to understand whether there is any disproportionate impact on particular groups. Where disproportionality is identified, forces must take positive steps to address this, **while maintaining the safeguards that vetting provides** [our emphasis]. Developing, implementing, and maintaining risk management strategies will be key here."

We agree that it is important to understand the effect that vetting decisions can have on underrepresented groups. But as the APP also notes, addressing disproportionality should not undermine the safeguards that vetting is intended to provide.

The Vetting APP advises forces to monitor vetting decisions against protected characteristics.

It also says that:

> "Forces and their vetting managers should:
>
> - understand unconscious bias and use training and professional development to address this;
> - provide statistical information about decisions where it is known there is a protected characteristic; and
> - actively engage with potential applicants to "explain the vetting process, dispel myths and potentially manage expectations."

We found that most forces we inspected had very little understanding of disproportionality in their vetting decisions. A few forces don't produce any information about vetting decisions relating to applicants with specific protected characteristics. Other forces produce such data but don't carry out any analysis of it to identify disproportionality. Some forces don't have any access to analytical support to help them to do this. Without any analysis to help forces understand the reasons for disproportionality in their decision-making, they can't take informed action to address it.

We were told that the College of Policing has devised an 'adverse impact ratio calculator'. This measures the impact of decisions on groups with protected characteristics. It has been made available to help forces monitor disproportionality in their vetting decisions, but not all forces are using it.

The MPS approach to monitoring disproportionality

We found the MPS has improved the way it monitors disproportionality in vetting decisions. It produces monthly data showing vetting decisions in relation to applicants' gender and other protected characteristics. The data includes information about the reasons for vetting refusals for each group. In addition to this detailed analysis, in 2021 the MPS established an 'equality cell' to help reduce disproportionality.

The MPS recognised that, in some ethnic minority groups, cultural differences and mistrust of public authorities could lead to applicants failing to disclose some of the information required during vetting. Members of the equality cell told us they attend outreach and recruitment events with the public. At these, they address concerns about the vetting process and how information provided during the process will be handled. This information could include a person's convictions or family history. Members of the equality cell answer any questions potential applicants have about whether this may prevent them from joining the police.

Recommendation 8

By 30 April 2023, chief constables should make sure they comply with the Vetting Authorised Professional Practice by analysing vetting data to identify, understand and respond to any disproportionality.

Vetting appeals processes

The Vetting APP states that an appeals process must be made available when vetting clearance, at any level, is refused or withdrawn. There are four grounds appeals can be based on:

- Further information is available that was not considered by the original decision-maker.
- The decision is disproportionate considering the circumstances or details of the case.
- The decision was perverse or unreasonable.
- No explanation has been given for the decision.

It also specifies that appeals should be considered by an individual of suitable seniority who:

- is independent of the original decision-making process;
- has not been previously involved in any aspect of the case; and
- has a working knowledge of the Vetting CoP and Vetting APP.

Some forces have nominated individuals in the force to act as an appeal body, usually a senior officer within PSD. In other forces, for example where supervisors within the vetting unit make the vetting decision, we found that the vetting manager handles any appeals. An exception to this is when the vetting manager has had previous involvement in the case. If so, a senior officer in PSD usually performs the function. We would be concerned if a vetting manager acted as an appeal body if they have had previous involvement in the process.

Vetting panels

Two forces we inspected have introduced independent vetting panels. Each panel acts as an appeal body, but they operate differently. One of them makes the appeal decision; the other only makes a recommendation to the FVM. Both panels also carry out routine reviews of vetting rejection decisions, including some that have not been appealed.

We disagreed with some vetting panel decisions and recommendations

There is no guidance in the Vetting APP on the use of vetting panels. During our vetting file review, we found several examples of panels overturning well-reasoned decisions, where the risks of doing so were apparently overlooked. As with other vetting decisions that we discussed earlier, we also found numerous examples where these vetting panels didn't effectively record the rationale for their decisions.

Case study 17

A PCSO applied to become a police officer in their own force and was granted vetting clearance following an appeal to a panel. Two years earlier, the PCSO, while serving with the force, was arrested for a common assault and received an adult caution. The assault happened when the PCSO was on a trip with friends. He was intoxicated and found to be helping himself to beer behind a bar. A man in his sixties approached the PCSO to ask him to stop. The PCSO revealed that he worked for the police and stated that he believed the man had drugs and that he was going to search him. A PCSO would not have the power to search someone for drugs in these circumstances. Following this incident, the PCSO was arrested for common assault.

The PCSO faced a gross misconduct hearing where he was given a final written warning that would be 'live' for 24 months. He applied to be a police officer while the final written warning was still live. On that occasion the force rejected him due to the adult caution for assault and the final written warning. He asked for a senior officer to review the decision. This review took place, and the rejection decision was upheld. He applied the following year and the force rejected him again. The FVM recorded extremely detailed and robust rationale to justify why clearance should not be granted. The PCSO appealed this decision, and this time the appeal panel overturned the rejection decision. His vetting was granted, and he became a police officer. The panel's justification was that: the gross misconduct hearing had not dismissed the PCSO; the offence was at the lower end of seriousness; the applicant had the support of their basic command unit commander; the applicant had received positive testimonies as a PCSO, including from the chief constable; and he was seen as an asset. The panel noted that he would "remain under scrutiny".

Case study 18

A police officer applicant was granted vetting clearance by an appeal panel. The applicant had a conviction from 20 years earlier, when he was a teenager, for assault occasioning actual bodily harm. For this, he received a referral order for three months and was required to pay compensation. He also had an unsatisfied (not paid in full) CCJ, as well as four defaulted accounts totalling over £13,000. The defaulted accounts had markers on them such as "gone away" and "debt collection". These indicate that the applicant had made no attempts to clear the debt. The force initially decided to refuse the applicant vetting clearance due to the CCJ, the defaulted accounts and the conviction for assault. The decision-maker referred to the impact regarding the need to disclose convictions as per Chapter 18 of the CPS *Disclosure Manual*. As we discussed earlier in this report, the applicant would need to disclose his conviction to the CPS in every case he was involved as a witness. The CPS would then need to decide whether the officer's conviction may undermine the prosecution.

The applicant cleared the CCJ and appealed the decision. He also made arrangements with his creditors to start a payment plan for the defaulted debt. The appeal panel made a recommendation to the FVM to overturn the vetting refusal decision because of his payment of the CCJ. But the rationale didn't include details of his financial situation. At that stage the applicant couldn't provide any evidence that he had complied with a debt management plan as he had only just contacted his creditors to start the process. The appeal recommendation and subsequent decision made no reference to the assault matter recorded against the applicant and referred only to the CCJ.

Vetting panels should operate in accordance with the Vetting CoP principles

As well as having concerns about some of their decision-making or recommendations, we also have concerns about the make-up of vetting appeal panels and some of their practices. We are aware that some panels include HR professionals. Some may view these as useful members of a vetting panel due to their knowledge of HR matters. And these professionals may be able to help with putting in place risk mitigation measures, such as geographical posting restrictions.

But one of the principles of the Vetting CoP is that "decision-making in respect of vetting clearance should be separate from, and independent of, recruitment and other human resources processes". We question the role that HR professionals, particularly those involved in recruiting, appear to be playing in some vetting panels. If the role is purely to advise the vetting panel, then the risk of breaching this principle may be mitigated. But we are aware that the panel in one of the forces we inspected uses a voting system for the appeal decision. In that force, the HR professional is

given an equal vote to other panel members, including the chair, which appears to breach this principle.

When panels are considering cases where applicants are known to have protected characteristics, some forces invite the relevant staff associations to attend the panel and to provide advice for the panel chair. This should help the panel make a decision with a better understanding of all relevant issues. We support staff associations and networks being used in this way to inform the decision-making process. But we don't expect, as we found in one force, the panel to hold a vote in the decision to accept or reject an applicant.

As previously stated, the Vetting APP requires the appeal body to be an individual of suitable seniority and with working knowledge of the Vetting CoP and the Vetting APP. Adapting this into a voting system that includes colleagues who may have had no training in vetting decision-making, and who may not be conversant with the corruption threats faced by the force, is a concern.

The Vetting APP should include more guidance for 'appeal bodies'

We understand that the NPCC lead for vetting has identified that guidance for appeals processes is an area that is lacking in the current version of the Vetting APP. We agree, particularly as the Vetting APP makes no reference at all to the use of appeal panels. The Vetting APP needs to give forces more detailed guidance on how best to achieve a truly independent and effective vetting appeals process.

It is also clear to us that all vetting decision-makers, including decision-makers acting as an appeal body, need better training to make effective and well-reasoned decisions. Senior members of the PUP told us that they are currently working with the College of Policing to devise such training for appeal panel members and that funding is available to support the project.

Recommendation 9

By 31 October 2023, the College of Policing, working with National Police Chiefs' Council lead for vetting, should change the Vetting Authorised Professional Practice to include guidance for dealing with vetting appeals. This should include specific guidance concerning the composition and role of vetting panels.

The guidance should be consistent with the Vetting Code of Practice, particularly in relation to decision-making responsibilities and the involvement of HR professionals.

Reviews of vetting after misconduct proceedings

The Vetting APP states that forces should carry out a review of vetting clearance at the conclusion of misconduct proceedings where the officer, special constable or member of staff is issued with a written warning or a final written warning. The review should consider the applicant's suitability to keep the level of clearance they hold and to continue in the post they occupy. Not all the forces we inspected carry out vetting reviews following misconduct proceedings. They should do so.

We identified the following case during our review of misconduct files.

Case study 19

A female officer alleged that a male colleague, who worked with her in a unit that specialised in investigating offences against vulnerable people, had made several sexual advances to her using text messages. She didn't want or reply to these messages. Some of the messages were clearly racist as well as being extremely sexually graphic. The victim would not give a statement until she had left the police service. The investigating officer's report makes a case for gross misconduct. But the force determined that the behaviour was misconduct only. We do not agree with that decision. Based on this decision, the force discussed the case at a misconduct meeting and gave the officer a final written warning (the most serious penalty available at a misconduct meeting). Despite the finding, the force didn't review the officer's vetting, and the officer still works with vulnerable people.

Forces should review vetting clearance for officers reduced in rank following misconduct proceedings

Under the Police (Conduct) Regulations 2020, there is an additional disciplinary action of 'reduction in rank'. This is deemed more serious than a final written warning. The Vetting APP makes no reference to this action. We believe it should. Its omission may be due to the fact that the APP was still being written at the point the 2020 Regulations were introduced. The Vetting APP should be changed, so that where an officer is reduced in rank following misconduct proceedings, the force should review their suitability to keep the same level of clearance as before.

Recommendation 10

By 31 October 2023, the College of Policing, working with the National Police Chiefs' Council lead for vetting, should change the Vetting Authorised Professional Practice to make it clear that, if an officer is reduced in rank following misconduct proceedings, forces should review their suitability to keep their current level of vetting clearance.

Recommendation 11

By 30 April 2023, chief constables who have not already done so should establish and begin operation of a policy requiring that, at the conclusion of misconduct proceedings where an officer, special constable or member of staff has been issued with a written warning or a final written warning, or been reduced in rank, their vetting status is reviewed.

Forces determine their own 'risk appetite', some more liberally than others

One final point, which we referred to earlier and appears to have muddied the vetting waters, relates to the level of risk forces are willing to tolerate. Some forces refer to this as their 'risk appetite'. This term appears in the Vetting APP as one of the factors for forces to consider, but only in relation to assessing potential financial vulnerabilities and levels of debt.

Some forces have applied the term more liberally, extending it to all risks. But in some cases these forces' risk appetites have led them to grant vetting clearance in the face of concerning adverse information. We believe that sometimes this may be influenced by the need to meet certain recruitment targets. As a result, some forces have too great a risk appetite, which has led them to grant vetting clearance despite knowing disturbing information about applicants. We take the view that such clearance decisions could only ever be compliant with the Vetting APP if they were compatible with all relevant aspects of the APP.

When forces grant vetting clearance to such applicants, and fail to put sufficient mitigation measures in place, they create an unacceptable risk to the force and the public.

Designated posts and management vetting

The Vetting APP sets a higher level of vetting for sensitive posts

Police officers and staff working in more sensitive posts generally need a higher level of police vetting. This is known as management vetting (MV).

The Vetting APP provides guidance on the criteria for designating posts that require MV. The guidance could be clearer as it is separated across two sections and gives somewhat conflicting information.

In the section on MV at page 40, the Vetting APP states that the purpose of MV is:

> "to provide a means of additional assurance in relation to the integrity, reliability, and potential for financial vulnerability of individuals serving in posts with access to sensitive police premises, information, intelligence, financial or operational assets, where:
>
> - the risk of potential compromise of those assets is high
> - the risk of serious damage to the force is substantial"

It further states:

> "All police personnel with long-term, frequent and uncontrolled access to SECRET assets and occasional access to TOP SECRET assets should hold MV clearance."

Within this section the emphasis appears to be mainly on information security. The issue of protecting vulnerable people does not feature.

Elsewhere in the Vetting APP (on page 53, 'Designation of clearance level') there is further guidance on the criteria for designating MV posts. This section introduces the issue of working with vulnerable people as a factor to consider.

It states that a force must review all of its posts, using the following factors to make sure that they have been designated the right vetting level:

- level of access to intelligence concerning covert or sensitive operations;
- level of access to material classified SECRET or above;
- access to source material and true source identities;
- access to information relating to high-profile or sensitive matters, such as royal visits or critical national infrastructure;
- level of access to sensitive personal information;
- level of influence over the management and/or awarding of contracts;
- level of dealings with financial matters, such as access to budgets, authorisation of payments or receipts of income;
- level of access to sensitive material concerning the police service;
- nature and extent to which the role requires working with vulnerable people; or
- level of access to IT assets.

The Vetting APP should give better guidance on which posts to designate for higher levels of vetting

Most forces use the Vetting APP guidance to designate relevant posts. But we were told that some forces have added and removed posts from their designated lists without reference to the guidance. We found disparities across forces as to which posts they had designated. For instance, some forces designated posts that involve working with vulnerable victims, but others didn't. Some forces have added roles to their designated list, such as dog handlers and crime scene investigator supervisors, which were not in others' lists.

The way the Vetting APP presents its guidance, as outlined above, may be contributing to this inconsistency. Most of the advice is focused on the security of sensitive information. Given the threat of corruption in relation to abuse of position for sexual purposes (AoPSP), it is entirely understandable that the APP includes "working with vulnerable people" as a further factor for forces to consider. But the advice is limited in this respect. Accepting that forces have different role names and job descriptions, this part of the Vetting APP would be improved with additional guidance on the types of roles to include.

In its current guise, granting MV clearance to police officers and staff may not be a particularly effective means of making sure they are suitable to work with vulnerable people. The additional vetting enquiries when upgrading from RV to MV status are limited to:

- additional financial enquiries;
- line manager endorsement;
- discretionary interviews with line managers and/or the applicants; and
- more regular vetting reviews.

But we do recognise the benefits of re-vetting someone before they move into a post that involves working with vulnerable people. These enquiries could reveal information about MV applicants which casts doubt on their suitability for a role. The Vetting APP isn't sufficiently clear on how forces should use MV to assess suitability for working with vulnerable people. We are aware that some forces have adopted their own alternative approaches to assessing individuals in advance of them being posted to such roles.

Recommendation 12

By 31 October 2023, the College of Policing, working with the National Police Chiefs' Council lead for vetting, should change the Vetting Authorised Professional Practice to be more prescriptive about what types of roles require management vetting, and give guidance on how people working with vulnerable individuals are vetted. This should include an emphasis on roles that specifically involve working closely with vulnerable people.

Forces' understanding of who occupies designated posts needs to improve

Most of the forces we inspected had a designated post list specifying all roles where MV is required. In general, these forces regularly review and update their lists of posts, for instance if they create new roles or decide to add existing roles to the list.

All the forces we inspected except one were using a specialised IT system to manage their vetting processes. One force was still using a system of electronic folders and word documents. But none of the forces had an HR IT system that was in any way linked to the vetting IT system. This means that vetting units are not automatically updated with relevant HR information (such as leavers, promotions, or internal moves to designated posts). In most forces, the HR department updates the vetting unit with this type of information via emails or weekly meetings. But in others HR is not routinely providing this.

Officers and staff in designated posts might not have management vetting clearance

Forces' understanding of who occupies designated posts is sometimes amateurish. As discussed above, not having an automated system inevitably means that sometimes some relevant information isn't given to vetting units. This means forces are not able to maintain an effective overview of who is occupying designated posts. Some forces partly overcome this by regularly comparing their designated post lists and HR data against their vetting IT system. This allows these forces to check that each designated postholder has the required vetting level.

As a result of the shortcomings described above, there are occasions when forces place police officers and staff who hold RV only in designated posts.

Separately to this problem, we heard in one force that 58 people had been allowed to take up a designated post without the required MV. This was not due to a lack of information from HR, but a lack of capacity within the vetting unit to complete MV checks. Some of these people had already been in the designated post for many months.

Area for improvement 2

Automated links between force vetting and HR IT systems are an area for improvement. When specifying and procuring new IT systems for these purposes, or developing existing ones, forces should seek to establish automated links between them.

Renewals of management vetting clearance are not always completed in time

The Vetting APP states that forces need to review MV clearance after seven years. We found that most forces have effective systems that allow them to determine when vetting renewals are due. This then helps them to make arrangements with the person concerned for them to submit vetting forms. But not all vetting units are aware of individuals' current postings. Only a small number of forces could show that all their management vetting renewals were up to date. Other forces conceded that that their HR and vetting data wasn't accurate enough.

Placing people in designated posts with RV only, or allowing postholders' MV to expire, is potentially placing forces and therefore the public at unnecessary risk.

Management vetting for sensitive, high-risk posts is not a new area for forces to consider. We have highlighted the risks of not managing MV processes effectively in various annual PEEL reports and made a number of individual force recommendations. In 2019, we published *Shining a light on betrayal: Abuse of position for a sexual purpose*. In that report, we recommended:

> "All forces that are not yet doing so should immediately comply with all elements of the national guidance on vetting. By July 2020, all forces that haven't yet done so should vet all personnel to the right standard. Forces should also have a clear understanding of the level of vetting required for all posts, and the level of vetting held by all their officers and staff. Forces should make sure all personnel have been vetted to a high enough level for the posts they hold."

Regrettably, for some forces this 2019 recommendation remains outstanding. It is encouraging that most forces have compiled a list of designated posts. But our findings are not reassuring. Even after a specific recommendation three years ago, some forces still don't know whether people who hold designated posts have been vetted to MV level. This is not what we would expect to see in any police force with effective and well-integrated vetting and HR functions.

Recommendation 13

By 31 October 2023, chief constables who have not already done so should establish and begin operation of a process to:

- identify the required vetting level for all posts within the force, including designated posts requiring management vetting; and
- determine the vetting status of all police officers and staff in designated posts.

As soon as possible after this, these chief constables should:

- make sure that all designated postholders are vetted to the enhanced (management vetting) level using all the minimum checks listed in the Vetting Authorised Professional Practice; and
- give continued assurance that designated postholders always have the requisite level of vetting.

Vetting renewal intervals are too long

A person's vetting must be renewed periodically to make sure they are still suitable to work in the police. The Vetting APP states that renewal periods should be every seven years for MV and ten years for RV. For a person's vetting to be renewed, they must submit a full application and all the required vetting checks must be completed again. During our inspection, numerous interviewees, including some with national policing responsibilities, expressed the view that these renewal periods are too long.

In his review of London's preparedness to respond to a major terrorist incident, *London Prepared: A City-Wide Endeavour*, published in 2022, Lord Harris also referred to the time frames for vetting renewals. That report recommends full vetting renewals at least every three years.

There does not appear to be strong evidence to say exactly what the renewal period should be. But there is certainly a growing consensus that the current renewal periods are too long. We too think shorter renewal periods would be more appropriate.

Everyone experiences significant changes in personal circumstances from time to time. This applies to vetting applicants and their friends and family. There is an obligation for police officers and staff to report changes of personal circumstances that may affect their vetting. But, as we explain below, our inspection found that some police officers and staff are not aware of this obligation. Others may be reluctant to report matters for fear of their vetting status being affected.

South Wales Police vetting initiative

South Wales Police has a process to reconcile its designated post list with HR records and vetting records every six months. Three months in advance of this happening, the vetting IT system alerts the vetting unit of renewals. The vetting unit then engages with police officers and staff to make sure they re-submit vetting forms in a timely way. The force has also introduced a process mid-way through the vetting clearance period which allows it to carry a partial re-vet including Police National Computer (PNC), PND, financial checks and social media checks on the applicant only. The force does this at the five-year point for RV status and after three years for MV.

Shortening vetting intervals will increase the workload of vetting units

Introducing shorter renewal periods for RV and MV, or introducing 'halfway checks' like those in South Wales Police, would immediately increase the workloads of vetting units.

The evidence from this inspection and Lord Harris's report suggests that, on balance, the additional capacity needed to shorten vetting renewal intervals would be justifiable.

Recommendation 14

By 31 October 2023, the College of Policing, in consultation with the National Police Chiefs' Council lead for vetting, should change the Vetting Authorised Professional Practice to prescribe intervals substantially shorter than ten and seven years for the renewal of recruitment vetting and management vetting respectively.

Reporting changes of circumstances

Given the timescales between vetting renewals, individuals with current vetting are required to self-report changes in personal circumstances. The Vetting APP states:

> "Vetting is based on a snapshot in time. Because an individual's circumstances can change, it is important that their ability to maintain their security clearance is assessed. A comprehensive aftercare regime allows such assessments to be made. Aftercare is therefore an important part of any vetting process and is the responsibility of both the applicant and the force vetting manager (FVM).
>
> All individuals who are subjected to the vetting process must report any changes in their personal circumstances. … Failing to report such changes may result in an individual's vetting clearance being downgraded or withdrawn."

Changes in personal circumstances include being the subject of, or a person of interest in, a criminal investigation. They also include a change of address, a change of partner, and significant changes in financial status. Such changes should be reported to the vetting unit as soon as possible after the change has occurred. The Standards of Professional Behaviour also requires that police officers self-report any action taken against them for a criminal offence (including arrest), conditions imposed by a court, and the receipt of a penalty notice. For police staff, the Police Staff Standards of Professional Behaviour only requires them to report convictions or cautions.

All forces have a policy that requires police officers and staff to self-report 'notifiable associations'. A notifiable association policy will generally, but not exclusively, concern links to individuals with a history of criminal offending (this is covered more extensively later in this report).

Some police officers and staff don't know that they should report changes in circumstances

During our fieldwork we found that most police officers and staff were aware of the obligation to report changes in circumstances. But we also found some in each force who were not.

We included a question about this in our survey. The results largely reflected what we found during our fieldwork: only 75 percent of respondents reported that they knew what changes they had to report for vetting purposes. A quarter of respondents weren't confident to say they are aware of what changes of circumstances should be reported.

As well as the obligation for individuals to report any changes, there is also an onus on line managers to be aware of this requirement. The Vetting APP states:

> "When information that might question the suitability of an individual's vetting clearance comes to the attention of police personnel, especially supervisors, the appropriate vetting authority must be informed."

Some forces have incorporated integrity checklist questions in annual appraisal forms for police officers and staff. But these may be of limited value, since we heard that performance and development review processes are not always complied with or are not used consistently. We didn't find any force that had specifically targeted line managers to increase their understanding of their responsibilities. That said, 81 percent of supervisors responding to our survey told us they understood the type of information they would need to make aware about their police officers and staff.

In December 2021, the Civil Nuclear Constabulary introduced a new process that requires police officers and staff to update the vetting unit with any changes to their personal circumstances every year using a vetting appraisal form. This appraisal form explains the obligation to report changes and asks a series of questions, including questions about:

- changes of co-residents;
- changes to relationship status;
- any domestic relationship problems;
- any convictions/cautions/fixed penalties;
- any police contact as victim/perpetrator or witness;
- any criminal associations;
- any mental health conditions;
- business interests; and
- financial issues.

It also seeks information about any performance-based concerns and use of social media. There is a separate form for supervisors to complete. This asks their views on any behavioural traits or characteristics of the applicant which may affect their vetting status.

Forces deal differently with information about changes in circumstances

When force vetting units are made aware of changes to personal circumstances, in most cases they carry out relevant vetting enquiries to determine whether there is any effect on the person's vetting status. But we found gaps in some forces' processes. For example, in some forces police officers and staff were reporting changes in their circumstances to the HR department which were not always forwarded on for vetting purposes. And in some forces, if a change of circumstances involves only a new address, the vetting unit merely records the details and does not carry out any vetting enquiries.

In one force, we found that even when individuals told the vetting unit about changes in personal circumstances, the unit didn't carry out any review of vetting status.

Recommendation 15

By 30 April 2023, chief constables should:

- make sure that all police officers and staff are made aware of the requirement to report any changes to their personal circumstances;
- establish a process through which all parts of the organisation that need to know about reported changes, particularly the force vetting unit, are always made aware of them; and
- make sure that where a change of circumstances creates additional risks, these are fully documented and assessed. If necessary, additional risks should lead to a review of the individual's vetting status.

Using the Police National Database to identify unreported changes in circumstances

Most forces acknowledged that that they can't be fully confident that all adverse information or intelligence that could affect an individual's vetting clearance is being given to the vetting unit. For example, the force may not be aware if members of its workforce have been arrested outside the force area if police officers and staff don't report this information themselves.

In our 2022 DMIP report, we explained that the MPS had carried out a PNC check on its entire workforce. This found that about 350 had committed criminal offences. Most, but not all, of these had been disclosed to the force during the recruitment process. But the vetting unit had not brought the majority of these to the attention of the directorate of professional standards. The figure included 205 police officers, three of whom had committed offences while serving with the force.

The other forces we inspected had not carried out a similar PNC enquiry for their whole workforce. In South Wales, the introduction of 'half-way' partial vetting checks, which we described in Chapter 5, means that the whole workforce will have been re-checked on the PND and PNC after about 18 months from the end of our inspection.

All the other forces are reliant on police officers and staff reporting such information themselves.

As we have already reported above, there is a notable percentage of police officers and staff who don't appear to understand when to report changes. There is also the potential for police officers and staff to deliberately withhold relevant information, particularly if they are involved in criminality.

If forces are to mitigate the risks posed by such police officers and staff, there is a measure they should adopt. It involves making more effective use of the PND.

Forces use the Police National Database to support decision making

Use of the PND is regulated by the Code of Practice on the Operation and Use of the Police National Database. This code states (at paragraph 2.1) that the PND is to be "used solely for policing purposes", which are defined as:

> "Protecting life and property; preserving order; preventing the commission of offences; bringing offenders to justice; and any duty or responsibility of the police arising from common or statute law."

This is to prevent offences and to comply with the duty on chief constables to enforce the Police (Conduct) Regulations 2020 and the Police Regulations 2003, as well as equivalent employment responsibilities in relation to police staff. This definition would encompass the vetting of police officers and staff to make sure they are suitable for their roles.

In addition, the Vetting APP states that all forces should check the PND, among other systems, when vetting all persons named on a vetting application form. So checking the PND already takes place prior to new applicants taking up an appointment or, once appointed, due to self-reported changes in circumstances, a change in role, or at the point vetting is renewed. This is done with their full knowledge and approval.

Automated PND checks of the workforce could be used to help prevent corruption and inform vetting decisions

The PND contains about 5 billion records, including information in crime reports, custody records, intelligence databases, and child and domestic abuse records. We contacted the company that operates the PND on behalf of the Home Office to ask if it was feasible to automate PND checks of all officers and staff. This would mean forces could be notified automatically if any new information was placed on the PND in relation to their police officers and staff. The company was confident that an automated check against these names, dates of birth and addresses could be set up for each force.

The company was at the time piloting two much smaller schemes that used information on the PND – one with North Yorkshire Police and one with Northamptonshire Police. The North Yorkshire Police pilot was to make aware possible concerns regarding breaches of domestic violence non-molestation orders. The Northamptonshire pilot was to examine incidents at addresses where firearms were registered.

Monthly checking of PND – a pilot scheme

Following our contact with the company, work on a further pilot scheme in North Yorkshire Police began, with the support of the NPCC lead for intelligence. This involves the monthly checking of all police officers and staff against the PND.

The scheme uses data from the force's vetting IT system, consisting of names, dates of birth and home addresses. It has created automated and repeated searches, using agreed search limits and a set of defined rules, to check information on the PND for updates. These searches will not add any details of police officers and staff to the PND.

The purpose of the scheme is to check whether the PND holds any relevant information that the force is unaware of. This will allow the force to address potentially serious matters at the earliest opportunity and identify people who fail to disclose relevant matters.

It should not escape any reader of this report that the police officer who murdered Sarah Everard came to police notice in the period leading up to her murder.

After an initial review of information held on PND, subsequent checks will only look for any updated information. Any relevant information found is reported to the force's PSD, who can check to make sure that the person has already reported the facts to them. If they haven't, they can then determine what action, if any, is needed to protect the public, the force and the individual concerned.

We are aware that some staff associations have questioned the human rights implications of these piloted schemes. We sought legal advice about the scheme's potential effect on the privacy of police officers and staff. Having considered that advice, our view is that use of the PND in this way is justified and proportionate in a context where police officers and staff should understand that:

- police officers (and some police staff) hold roles which afford them coercive powers and considerable responsibility for the most vulnerable, in which the utmost integrity is required in order to sustain public trust and the model of policing by consent;
- they ought to be self-reporting such matters anyway;
- the actual level of intrusion into their private lives will be minimal (particularly where there is no information held about them on PND);
- everyone is treated equally by being frequently searched; and
- public confidence in the police service as a whole will be enhanced by the knowledge that the small minority who commit offences and cause serious harm will be more quickly identified, using a tool uniquely available to the police.

We consulted each of the vetting units in the forces being inspected about this proposed use of the PND, and we found that it received overwhelming support. At the time of writing this report, it was too early to comment on any findings of the pilot. But we would support the introduction of this process throughout all forces in England and Wales as soon as possible (after any unexpected problems revealed by the pilot have been resolved).

Recommendation 16

By 31 December 2023, chief constables should make routine use of the Police National Database (PND) as a tool for revealing any unreported adverse information about officers and staff. To help this, the College of Policing should:

- working with the National Police Chiefs' Council lead for counter-corruption, change the Counter-Corruption (Intelligence) APP to include a requirement for the PND to be used in this way; and
- change the PND Code of Practice (and any subsequent code of practice concerning the Law Enforcement Data System) to include a specific provision that allows for the PND to be used in this way.

Staffing levels within vetting units

The PUP gave each force an annual recruitment target and funding to support them to meet these targets. The funding is allocated not only to support the initial recruitment and wages of new police officers and staff, but also the extra infrastructure forces needed to help the uplift to continue. Some forces have chosen to use the funding to recruit more staff to work in vetting units.

Despite this, not all the forces we inspected had enough staff within their vetting unit to cope with the current demands they face. Others were able to meet their force's agreed timescales for vetting and told us their workload was manageable. Interviewees in one force told us it had carried out its own comprehensive review of demand with business analysts from its organisational development department. This gave the force a clear understanding of the additional demand associated with the PUP and made possible a corresponding increase in vetting resources.

But we found other forces in a very different position, with staff levels in their vetting units falling short of what was required to meet demand. These forces told us that increasing vetting demand from the PUP was creating pressure and that their workload was no longer manageable. In some forces, this problem is exacerbated by the use of the vetting unit for other tasks such as firearms licencing checks and managing notifiable associations processes. Some forces are operating with vacancies in their vetting unit. One vetting supervisor told us:

> "Workload is overwhelming – I am awake at night sometimes worrying about the potential to miss things…"

Some force vetting units told us they feel under pressure to support the force in meeting its targets for police recruitment. We heard from some vetting units that they were having to prioritise initial RV over other vetting tasks. Staff in one force told us that they had fallen behind with vetting renewals.

The use of technology to carry out automated vetting checks may benefit from national co-ordination

Many aspects of the vetting process, particularly the enquiries routinely carried out, are repetitive and straightforward. Generally, processes of this nature lend themselves to automation.

Some forces are aiming to improve their efficiency using technology that can carry out automated vetting enquiries, such as PNC and financial checks. Although several trials are underway, the success of these is mixed. We heard anecdotal evidence that automated checks are having to be rechecked manually, which clearly defeats the purpose of the trials.

The PUP has carried out some research into the use of this technology. The programme estimates that, when working effectively, the technology could save about 40 minutes of vetting unit time per applicant. Based on this estimate, the effective automation of vetting enquiries would make vetting units substantially more efficient. We found that several forces were independently exploring the use of this technology. We think this is an area that deserves close attention and national co-ordination.

Vetting training needs to be improved

An online training module and a series of National Vetting Portfolio continuous professional development (CPD) events give a useful overview for vetting decision-makers to better understand their role. But we don't believe that they place enough emphasis, or give detailed enough guidance, on how all the factors outlined in the Vetting APP should be considered when making vetting decisions. And they don't include enough information about the use of risk mitigation strategies or how to record a detailed rationale for complex vetting decisions.

Our vetting file review found that there are significant skills gaps in some forces. Vetting decision-makers at all levels, including those who act as an appeal body, would benefit from improved guidance on Vetting APP risk factors, how to record the rationale and how to put effective mitigations in place.

All of the forces we inspected have given training to their vetting units on how to use relevant systems such as PNC and PND. But beyond this, some rely mainly on colleagues within the vetting unit to provide informal 'on the job' learning. Encouragingly, the national take-up across the service for the April 2022 CPD event was much higher than in previous years. Only one force in England and Wales failed to send a delegate to the CPD event or arranged access to the event online.

Other than the online module and the CPD events, there are currently no other professional development opportunities specifically aimed at those charged with making vetting decisions.

Additional training is being developed

The PUP is providing funding for additional relevant training to be developed. Warwickshire Police, whose chief constable is the NPCC lead for vetting, is in the process of gaining International Organisation for Standardisation (ISO) accreditation for a classroom-based training module for vetting practitioners. This would be an intensive course that would greatly reduce the time taken to train someone in vetting. The course is intended to improve professional competence and standardisation of vetting processes throughout forces.

6. Vetting of officers and staff transferring between forces

The Vetting Authorised Professional Practice (Vetting APP) states that:

> "Forces must ensure that the integrity of an individual wishing to transfer into the force (or re-join) is beyond question."

Anyone with previous police service – whether as a police officer, special constable, or member of police staff – will have previously been granted vetting clearance.

Principle 7 of the Vetting Code of Practice (Vetting CoP) states that vetting clearance may be transferrable between forces on the condition that a vetting 'health check' is completed. But this only applies where the applicant to transfer has received vetting clearance in the preceding 12 months to the level required for the role they are moving to. In such cases, the full vetting file should be passed to the receiving force. If vetting clearance was completed more than 12 months beforehand and/or to a level lower than that required for the post they will be moving to, a full re-vet will be required.

Forces are consistently sharing information and choosing to re-vet all transferees

In our 2019 spotlight report *Shining a light on betrayal: Abuse of position for a sexual purpose*, we recommended specific information that forces should share in respect of all transferees. This included information on performance, sickness, complaints, business interests, notifiable associations, and corruption-related intelligence.

Following that report, when the Vetting APP was updated in 2021 it stated that in all transferee cases, the receiving force must request the full complaint and misconduct history of the officer or staff member from all forces where they have previously served. This applies whether vetting clearance is to be transferred or a full re-vet is required. Following such a request, the professional standards department (PSD) for the originating force should make sure that it provides a full complaint and misconduct history, as well as details of any corruption-related intelligence.

In each of the forces we inspected, we found that regardless of how recently any transferees or persons seeking to re-join the police service had been vetted, the receiving forces were now choosing to carry out a complete re-vet.

We also found that forces are consistently and routinely requesting a full complaint and misconduct history, and that originating forces are supplying this as requested. Forces told us that, when confidential information is held about a transferee, the two forces' counter-corruption units (CCUs) will make arrangements to make sure the information is passed on securely.

We found that, overall, forces have responded well to this aspect of our 2019 spotlight report. This means that forces can, in general, decide to grant vetting clearance to people wishing to transfer or re-join the service with full knowledge of all the available information from their previous police service.

Inconsistencies between forces

We found examples of several forces refusing vetting clearance to prospective transferees. In some of these cases, the rejection decision was based wholly or in part on the PSD history or CCU intelligence shared between the forces. For example, we examined a transferee case where a force refused vetting clearance because of concerns about previous behaviour towards women in the workplace. When the individual appealed this decision, the force upheld the original refusal.

Worryingly, we also found a small number of transferee cases where vetting was refused, even though the decision was based on the same information considered by the previous force when it had granted clearance. Some vetting managers told us that forces' willingness to accept risk has diminished since the murder of Sarah Everard.

Although the sharing of transferee information has improved, we found that forces aren't always using this information effectively to support their vetting decisions.

In most of the forces we inspected, we found examples of poorly documented decision-making rationales in transferees' vetting files. We found an instance in one force where the transferee had a misconduct finding involving "corrupt practice". The receiving force didn't further explore this with the originating force. The receiving force granted vetting clearance without recording any decision-making rationale. In other examples, the PSD history included multiple unproven public complaints that the receiving force didn't sufficiently consider. This is wholly unsatisfactory.

In one instance, we found that a receiving force identified risks in the form of unsubstantiated allegations made by colleagues but allowed the transfer to go ahead anyway.

Case study 20

A police officer transferee was granted clearance following a full re-vet. Their originating force supplied the PSD history and CCU intelligence. This showed that the transferee had been the subject of 25 public complaints during a 10-year period. Many of these complaints were for excessive use of force and incivility. Most of the complaints were unsubstantiated but four had resulted in management action. The transferee had been arrested at the end of that period for being drunk and disorderly, but without any action being taken. There was no evidence that the receiving force considered the circumstances and frequency of the public complaints in the context of a pattern of concerning behaviour. There was no evidence that the receiving force considered any risk mitigation measures.

Case study 21

During our intelligence file review, we identified a case that involved a police officer allegedly engaging in improper sexualised touching of a member of the public and junior officers (the allegations, if proven, may amount to sexual assault). There were several complainants. The incidents spanned a period of years. None of the complainants would support any action. As a result, the force was unable to prove the allegations.

The force advised the officer about their future conduct. When we asked the force what action it had taken, we found that this officer had subsequently transferred to another force. The receiving force had undertaken full re-vetting of the transferee and requested the PSD history and CCU intelligence. The originating force made a full written disclosure, including the unproven allegations and other concerning information.

Initially the receiving force's vetting unit was considering refusing vetting clearance. But the officer was subsequently granted clearance by the chief constable. The chief constable's recorded rationale was largely on the grounds that accepting the transferee would make the force more diverse. We didn't agree with the chief constable's decision. While allowing the transfer to proceed, the receiving force assessed the risks associated with this officer to be sufficiently great as to require imposing several risk mitigation measures. These included subjecting the officer to more intrusive supervision than would be the norm.

We consider that in granting vetting clearance to this transferee, the receiving force gave undue weight to diversity considerations at the expense of an objective assessment of the facts. In doing so, the receiving force ran the risk of conveying the wrong message to officers in the originating force who made the allegations. At worst, the decision could also expose female officers in the receiving force to unnecessary risk.

Vetting clearance granted to transferees with family members linked to crime

We found examples in three forces where transferees had family members linked to criminality. One of these family members was listed on the Police National Computer as 'wanted', one was recently released from prison and one had previously been arrested on suspicion of drugs supply offences. We also examined a case where an originating force had previously granted vetting clearance despite there being two occasions where the applicant had been arrested for serious crime but with no resulting prosecution. One of the arrests was on suspicion of causing grievous bodily harm and the other for an allegation of rape.

In each of these transferee cases, the associated risks were not documented in sufficient detail, and there was no evidence within the recorded decision-making rationale that they had been properly considered.

Case study 22

A receiving force granted vetting clearance to a transferee. The force secured the PSD history from the originating force. She had previously been arrested for fraud, along with a brother who was later convicted. There was no criminal action taken against her. After a police misconduct investigation, the transferee was given 'management advice'. Another brother had also come to police attention for allegedly being involved in money laundering and fraud, but no action had resulted from this. The applicant had management vetting (MV) clearance in her own force, was open about the criminal history of her family members and stated that she was transferring forces to get away from them.

But there was a further brother living in the receiving force area who was linked by intelligence to gang-related serious and organised crime. He was suspected to be involved in the supply of controlled drugs and previously had been shot. The rationale referred to the applicant's openness and acknowledged her reasons for wishing to distance herself from family members involved in criminality. The receiving force also took note of the fact that the originating force had granted MV clearance. But the receiving force does not appear to have considered the intelligence relating to the organised crime group-linked brother, who was based in its area, and didn't put any risk mitigation measures in place.

Some forces grant vetting clearance to transferees with unresolved complaints or misconduct matters

The Vetting APP states that where an officer is subject to a complaint or conduct investigation that has not yet been finalised, they should not be allowed to transfer forces. This can be waived with the agreement of both forces. We examined several transferee cases where this situation arose. In some cases, forces put the transfer on hold until the complaint or conduct investigation was complete. In other cases the head of PSD approved the transfer. We also found occasions where forces allowed the transfer to go ahead without any record of the required agreement between the forces. In one of these cases, the decision to allow the transfer to go ahead despite a live complaint was not supported by any rationale at all. There was merely a stamp in the file declaring "no vetting objection".

A vetting refusal for a transferee should trigger a review of their current vetting status

Some force vetting managers told us that when another force refuses to grant vetting clearance for a transferee application, this triggers them to carry out their own review of the individual's vetting status. This is not a requirement of the Vetting APP but seems to us to be a sensible approach. The refusal decision does not set any precedent that the originating force is bound to follow.

Forces inevitably have different tolerances to some risks, and one force may be able to mitigate risks that another force cannot. But vetting enquiries for the transferee application could, in theory at least, reveal new information that the originating force has not accounted for. For example, it may reveal financial risks or additional adverse information that the transferee applicant failed to disclose previously.

Recommendation 17

By 31 October 2023, the College of Policing, working with the National Police Chiefs' Council lead for vetting, should change the Vetting Authorised Professional Practice to give guidance that:

- in every case where a transferee is refused vetting clearance, the originating force should carry out its own review of the individual's vetting status; and
- the two forces involved exchange relevant information about the reasons for the refusal decision.

7. Detecting and dealing with misogynistic and predatory behaviour

Defining misogynistic and predatory behaviour in a policing context

In her letter of 18 October 2021, the then Home Secretary asked us to examine forces' ability to detect and deal with "misogynistic and predatory behaviour".

To identify more precisely the types of behaviour in question, we had to define what they were. We found no nationally agreed definition we could use (although, in 2020, UNISON listed examples of behaviour that may constitute sexual harassment). To give clarity to forces (mainly about the information we asked them to provide), to the police officers and staff who assisted us during this work and our own inspectors, we defined 'prejudicial and improper behaviour' as:

> Any attitude and/or behaviour demonstrated by a police officer or police staff that could be reasonably considered to reveal misogyny, sexism, antipathy towards women or be an indication of, or precursor to, abuse of position for a sexual purpose (AoPSP).
>
> It may include, but is not limited to: inappropriate, crude or offensive comments; telling sexualised jokes; asking intrusive questions about someone's private life; inappropriate touching; abusive, manipulative, coercive, controlling or predatory behaviour; bullying and harassment; and any other type of behaviour that may give cause for concern over whether a person is fit to serve as a police officer or as police staff.

As a result, our terms of reference included:

> How effectively do forces identify, prevent, detect and deal with prejudicial and improper behaviour based on gender by their police officers and staff?

During the inspection, we heard numerous examples, mainly from female police officers and staff, of such behaviour towards them. This was usually, but not exclusively, from their male colleagues.

When police officers and staff don't treat colleagues with respect and courtesy, it suggests that they may behave in a similar way towards the public, and towards vulnerable women. An unpublished 2022 report by Bournemouth University found that police officers involved in sexual misconduct in the workplace are statistically

more likely to be the subject of intelligence reports from the public about their sexualised behaviour.

An improving police culture, but with persistent problems

Almost invariably, police officers and staff we interviewed told us that, although this type of behaviour in policing has reduced over the last decade or so, it persists.

Reasons they gave for the reduction included:

- higher standards of expected behaviour;
- internal communication and training relating to these standards;
- learning from high-profile incidents involving prejudicial and improper behaviour;
- changing attitudes in society, which are reflected in the workforce; and
- an increasing proportion of female officers and staff, including more in higher ranks and grades.

The view that there had been an improvement in culture and behaviours was also reflected in the survey results. But there was still a significant proportion of respondents who believed that these behaviours hadn't changed or had got worse in the last five years.

Most survey respondents also thought that their force's culture discouraged prejudicial and improper behaviour. In general, men were more positive about the culture.

Despite these results, we found a culture where misogyny, sexism and predatory behaviour towards female police officers and staff and members of the public still exists. Some female police officers and staff we spoke to described the deeply negative effect such behaviour has had on them.

Concerningly, some female police officers and staff told us they felt they needed to acquiesce to prejudicial and improper behaviour. Others told us that some of their female colleagues adopted stereotypically masculine character traits to help them progress or be accepted within the service.

During our fieldwork, some female officers didn't want to take part in women-only focus groups. We are concerned that a fear of repercussions may have discouraged some women from participating in these groups. This aligns with published academic research that suggests that people may be ostracised if they are seen to speak out against their peers.

In addition, some of the women we spoke to as part of our survey confirmed that they wouldn't have shared their experiences so openly in a focus group (regardless of gender), because they didn't want their colleagues to know what they were telling us.

Some interviewees suggested that prejudicial and improper behaviour was especially prevalent in areas where there are fewer supervisors or where teams work very closely together and there is little turnover of staff, such as rural areas and specialist units.

One-to-one telephone interviews with survey respondents revealed misogynistic and predatory behaviour

Of the 11,277 officers, staff and volunteers who responded to our survey (this was the highest ever response to one of our surveys), 668 volunteered for follow-up interviews with us. We interviewed 42 of them (all except one were women). Their accounts included sensitive detail, some of which amounted to allegations of criminal offences. These included female officers and staff alleging sexual assault by male colleagues in the workplace and at social events. Other, less serious matters (some of which may nevertheless amount to misconduct, and in some instances possibly gross misconduct) included:

- senior male officers pursuing women in lower ranks for sex, including via the force email system;
- viewing pornography at work – for example, male officers (including supervisors) viewing pornography on suspects' phones (not as part of investigations) and inviting other officers to view the images on screen;
- sending pornography to female colleagues' phones;
- inappropriate sexual comments by male officers, including comments about a victim's breasts, comments about vulnerable sex workers who were victims of crime, and many other disparaging and insulting comments about female victims in general;
- at work-related social events, a senior male officer pestering female colleagues for sex. He sought to take advantage of those who he could see had clearly been drinking alcohol;
- male officers making a point of stopping cars driven by women they regard as pretty, a practice they referred to as "booty patrol"; and
- male officers, including supervisors, making sexually explicit comments about female members of the public.

Telephone interviewees told us that, in many cases, the perpetrator was someone who had previously been reported for similar behaviour, which either hadn't been taken seriously or hadn't been thoroughly investigated.

Much of the sexual misconduct the interviewees described could be an indicator of similar conduct towards members of the public.

Other poor behaviour towards women needs addressing

Most forces have diversity and inclusion policies. Evidence shows that a culture that is fair, diverse, and inclusive can lead to a sense of legitimacy where the workforce feels valued and is ultimately more efficient and effective. To this end, the College of Policing has produced training, policies, and guidance to help forces create positive work environments based on equity and respect. Despite this, our fieldwork revealed a worrying picture of how some police officers and staff view women. A general antipathy towards women was prevalent and, in some forces, was clearly on display.

For example, during interviews, many police officers and staff told us that there was still a stigma around pregnancy and part-time working. A group of male officers told us that they were frustrated by having to work harder to fill the gaps left by female officers who go on maternity leave. One supervisor said:

> "These are women who get pregnant while they have jobs on front-line duties … this leaves a gap and [in a team of 5] creates 20 percent extra work [for the remaining staff] … I think because of this the issue will carry on … women tend to go part time when they have a family, and this leads to prejudice … the perception being the males must work harder to fill the gap."

Many female interviewees stated they were the subject of negative comments about their part-time status. Comments such as "you managed to turn up today" were not uncommon. Some female officers also told us they had to work harder than male colleagues to be accepted into some specialist teams.

We were also told about other improper behaviour by male police officers and staff, including:

- regularly telling sexist jokes about women;
- making comments about female colleagues' bodies;
- ignoring women in meetings; and
- making female colleagues feel uncomfortable by staring at them.

One female senior officer told us she held a folder across her chest every time she went to a meeting where a particular male colleague was going to be present, as he consistently stared at her breasts.

Worryingly, some of these attitudes and comments came from supervisory ranks. The behaviours and standards that go unchallenged are the behaviours and standards that are accepted. It seems to us that if supervisors aren't challenging blatantly sexist comments – and in some cases they are the people making the comments – then this type of behaviour becomes normalised.

The type of poor behaviour towards women described above is prevalent in many forces. It is time for that culture to change. Much of the behaviour we were told about was outside our terms of reference. But the lid has been lifted and there is a need for further work to be done to make systemic changes.

Forces need to understand their culture before trying to improve it

We heard conflicting views from interviewees about forces' attempts to prevent prejudicial and improper behaviour and improve their cultures generally.

Most officers and staff we spoke to told us that the culture in their forces was positive and that they enjoyed working there. But some female officers and staff told us, both in the fieldwork and via the survey, that forces were just "paying lip service" to wanting to change the culture and prevent prejudicial and improper behaviour. They said that forces "talk a good job" about wanting to do the right thing, but don't always reinforce this with appropriate action. Later in this report, we give many examples of this.

Conversely, we heard from some officers and staff who believed forces were going too far in their attempts to prevent prejudicial and improper behaviour. Some male officers told us that they felt they were being "tarred with the same brush" as high-profile male offenders.

We heard views that prejudicial and improper behaviour towards women is not treated as seriously as racism or homophobia. Officers told us that racism and homophobia were seen as "career ending", while there was a higher level of tolerance of sexism towards women. In this inspection, we didn't compare the outcomes for these categories of misconduct. But in our investigation file review we found many examples of an unacceptably high level of tolerance of prejudicial and improper behaviour (case studies appear later in this report).

We found that, often in reaction to the murder of Sarah Everard or other high-profile cases, many forces had taken steps to improve public confidence and address prejudicial and improper behaviour within their workforce. But some hadn't done any preparatory work to sufficiently understand the scale of this. This meant they were putting solutions in place to solve a problem they didn't fully understand. There was one notable exception to this.

Devon and Cornwall Police cultural audit

In 2021, following a series of high-profile misconduct cases relating to racism and homophobia, Devon and Cornwall Police commissioned a cultural audit. The purpose of the audit was to determine why these cases were happening. The audit identified issues relating to both racism and homophobia. It also identified concerning levels of gender-based discrimination.

Without exception, every female respondent interviewed in the cultural audit reported experiencing some form of sexual harassment or discrimination in the workplace. This prompted chief officers to reflect on the force's culture. One said:

> "The dawning realisation that the experiences of large numbers of colleagues [are] very different to your own was difficult. And, unwittingly or otherwise, I've been a bystander. I may have been a perpetrator; I can't rule it out. Whatever way you look at it, it's happened on our watch."
>
> "That's happened around me and I've been blind to it."

Most chief officers we interviewed at other forces tended to be more defensive. In contrast, Devon and Cornwall Police has come to a position of understanding about the nature and scale of gender-based discrimination within the workplace. Senior leaders' acceptance of the audit's findings represents a sound basis upon which to bring about positive cultural change over the longer term. Other forces may wish to adopt a similar approach.

Area for improvement 3

Forces' understanding of the scale of misogynistic and improper behaviour towards female officers and staff is an area for improvement. Forces should seek to understand the nature and scale of this behaviour and take any necessary action to address their findings.

Challenging and reporting prejudicial and improper behaviour

Most police officers and staff told us they would recognise prejudicial and improper behaviour and knew how to report it. This aligned with our survey results, where over 90 percent of respondents said they knew how to report these behaviours.

Challenging the behaviour of colleagues

During our fieldwork, interviewees told us they often informally challenged prejudicial and improper behaviour rather than reporting it to a supervisor. Many interviewees felt this was an appropriate way for such behaviour to be dealt with.

Conversely, some officers and staff who had personally experienced prejudicial and improper behaviour told us it was often witnessed by colleagues, including supervisors. But they said that these colleagues rarely challenged the people responsible.

A smaller proportion of women than men told us they would be confident to report prejudicial and improper behaviour

When asked if they would be confident reporting prejudicial and improper behaviour exhibited by a colleague, three quarters of women, and a slightly higher proportion of men, said they would be confident to report it. Among those who said they wouldn't be confident to report it, twice as many were women.

The percentage of positive responses decreased when respondents were asked if they thought their team would support them if they raised concerns about a colleague's behaviours and attitudes. Only two thirds of women and three quarters of men felt their teams would support them. Indeed, many of the telephone interviewees told us they didn't feel supported by their colleagues when they challenged or reported such behaviour.

Many women are used to tolerating a degree of prejudicial and improper behaviour before reporting it

Despite being able to recognise prejudicial and improper behaviour, many female interviewees told us that they are used to tolerating a certain amount of it without reporting it. They told us their reasons for not reporting these behaviours included:

> "Anyone reporting anything would instantly be labelled as a grass. If it was just one incident, nothing would happen, so people wait for more things to happen, so they aren't seen as petty and it makes it more serious and taken more seriously."
>
> "If I felt something would be done, then I would report. I am not convinced anything would happen. Even less so if it is a senior officer."
>
> "I don't bother to report anymore, I have no faith and nothing will happen."

Many women fear the repercussions of reporting

Many female officers and staff also told us they were worried about the repercussions of reporting such behaviour. They were concerned that they would be viewed as a troublemaker, be ostracised and even that their colleagues might not come to their assistance if they needed back-up while on patrol.

They told us:

> "Females are regarded as trouble makers, [if they complain] they are soon isolated."
>
> "I wouldn't report anything as it would be my name dragged through the mud rather than the offender. I would be labelled a grass."

> "The problem is when you report something, as the victim, you are identifiable and you are subject to the bias of the masses. If you report something you get judged – it is a huge deterrent."

These are not isolated comments. It is our belief that this is how the overwhelming majority of female officers and staff view their workplace.

Most officers and staff are dissatisfied with the outcome of reporting prejudicial and improper behaviour

Tellingly, in instances where survey respondents had reported prejudicial and improper behaviour, only 28 percent of women and 35 percent of men said they were satisfied with the outcome.

Many of the telephone interviewees told us that the quality of the investigation into their allegations had been poor. As we describe later in this report, in too many cases our investigation file review led us to a similar conclusion. Female interviewees believed their forces took criminal allegations from the public more seriously than those from police officers and staff. Many said that they didn't feel supported after they complained and that their criminal allegations weren't all recorded as crimes. Many respondents had lost all confidence in their force after reporting prejudicial and improper behaviour.

Comments from women included:

> "I have zero percent trust in the force – I will never report anything again. I will be hung out to dry."
>
> "There is no way on God's green earth that I would report anything ever again."

Recommendation 18

By 30 April 2023, chief constables should make sure that there is a robust response to any criminal allegation made by one member of their force against another. This should include:

- consistent recording of allegations;
- improved investigation standards; and
- sufficient support for victims and compliance with the Code of Practice for Victims of Crime in England and Wales.

The rights of dissatisfied police victims need to be strengthened

Members of the public who are dissatisfied with the standard of a criminal investigation can make a complaint under the Police (Conduct) Regulations 2020. If they are dissatisfied with the outcome of their complaint, they have a right of appeal to the Independent Office for Police Conduct (IOPC).

Section 29 of the Police Reform Act 2002 prevents police officers who are similarly dissatisfied from making a complaint against an officer from their own force (but they can complain against an officer from a different force). As they can't complain against officers from their own forces, they have no right of appeal.

It appears unreasonable to us that police officers who may be victims of criminal offences enjoy fewer rights than other members of the public. Where a member of a police force makes a criminal allegation and they aren't satisfied with how it was handled or investigated, they should have a right to complain and a right to appeal.

We encountered a similar situation when investigating a super-complaint into the treatment of victims of police-perpetrated domestic abuse. Many such victims are police officers. In a joint report with the College of Policing and the IOPC, published in 2022, we recommended that the Home Office considers making changes to legislation to give these victims greater rights.

The problem is wider than police-perpetrated domestic abuse. We believe these rights should be expanded to include victims of all criminal allegations against a colleague in the same force. This may need an additional change in legislation. As this inspection has established, a significant number of police officers make criminal allegations against officers from their own force. However, many of these criminal complaints were not recorded or the allegation was investigated poorly.

Recommendation 19

By 31 October 2023, the Home Office, working with the National Police Chiefs' Council lead for complaints and misconduct, and the Independent Office for Police Conduct, should make sure that police officers who make criminal allegations against other members of their own force are afforded rights similar to those held by members of the public who make criminal allegations. These should include:

- the right to complain about the conduct of officers concerned with the handling of the allegation, including its recording and investigation; and
- the right to appeal against the outcome of such a complaint.

Policies and procedures relating to prejudicial and improper behaviour

All forces have a range of policies aimed at preventing corruption. But very few of these relate to the type of behaviour that falls within our definition of prejudicial and improper behaviour.

In fact, of the 667 documents forces sent to us, only a small number covered behaviour that we would consider prejudicial and improper. Given that police forces in England and Wales do not have a definition of prejudicial and improper behaviour, this is hardly surprising. But our inspection revealed that such behaviour is prevalent. This suggests to us that forces should have policies to support officers and staff to identify, deal with and investigate this type of behaviour.

Only one of the forces we inspected had a specific sexual harassment policy. This policy was "designed both to help prevent any Sexual Harassment and to offer support to any individual who feels they are subject to such behaviour". It stated that:

> "The force is committed to providing a working environment free from harassment, bullying and victimisation and ensuring that all staff and officers are treated, and treat others, with dignity and respect, and that any concerns can be confidentially reported without fear of intimidation."

Other forces that we inspected had more generic policies that cover harassment, bullying and victimisation. Generally, interviewees stated they had a good awareness that these policies existed and would refer to their force intranet for more detailed information if required.

The UNISON survey

As we mentioned earlier in this report, in 2018, UNISON published the results of a survey assessing the prevalence of workplace sexual harassment experienced by police staff members.

In February 2020, UNISON then published guidance and a model sexual harassment policy for all police forces (and other organisations that employ its members). Given the findings of UNISON's survey, the publication of its guidance and model policy and the time that has elapsed since then, we were surprised to find that more forces hadn't introduced their own sexual harassment policies.

We understand that in August 2022 the National Police Chiefs' Council (NPCC) sent a sexual harassment policy to forces, together with information to support them with its implementation.

Recommendation 20

By 30 April 2023, chief constables should adopt the National Police Chiefs' Council sexual harassment policy.

National guidance on external and internal relationships

As we have mentioned earlier in this report, the College of Policing and NPCC have produced two joint guidance documents:

- *Maintaining a professional boundary between police and members of the public*; and
- *Appropriate personal relationships and behaviours in the workplace*.

Most interviewees didn't know that these documents existed.

The first document, published in 2017, describes the privileged position police officers and staff find themselves in. It provides broad principles to support their decision-making and professionalism when considering whether to form relationships with members of the public they have met during their duties. It includes the following guidance for officers and staff. They should:

- not establish or pursue any form of sexual relationship with someone they meet in the course of their duties;
- inform a supervisor if a member of the public attempts to form an improper relationship with them;
- be aware of the imbalance in power between themselves and members of the public and always maintain professional boundaries;
- be aware any breach of the guidance would be aggravated should the member of the public be considered particularly vulnerable;
- not use force systems to assess someone's background with the intention of approaching them to form a personal relationship; and
- not use personal social media, email, or telephone to contact a member of the public they meet during current work or duties.

The guidance informs supervisors of their responsibilities if a suspected breach is brought to their attention. It also anticipates that potential breaches would be likely to require a mandatory referral to the Independent Police Complaints Commission (now the IOPC).

The second document published in 2019, in response to the UNISON survey, gives guidance regarding personal relationships and behaviours in the workplace. This guidance relates to "intimate or sexual relationships, rather than any other 'social' relationship".

It states:

> "In determining whether or not a relationship creates any negative impact on the legitimate aims of policing, the following factors could be considered:
>
> - a power imbalance is not used to initiate, control, or maintain the personal relationship;
> - physical and intimate relations do not take place on duty, or off duty on police premises including police vehicles;
> - the relationship does not have an adverse impact on the workplace, for example by creating division and/or friction between those in the relationship or among work colleagues;
> - there is no fear, fraud or workplace benefit driving the relationship;
> - the relationship has no influence on workplace decisions or activities and is not being used to gain or provide some workplace advantage; and
> - lines of reporting are not abused or compromised."

In our opinion, the document *Appropriate personal relationships and behaviours in the workplace* was too narrowly drawn. It focuses on managing consensual intimate workplace relationships rather than preventing any prejudicial and improper behaviour, which includes non-consensual behaviours. And it doesn't sufficiently address some of the concerns the UNISON survey had revealed.

Recommendation 21

By 30 April 2023, the College of Policing, working with the National Police Chiefs' Council lead for ethics and integrity, should extend the scope of the *Appropriate personal relationships and behaviours in the workplace* guidance. An amended version should include guidance in relation to non-consensual behaviours as well as consensual relationships.

The Standards of Professional Behaviour

The Standards of Professional Behaviour (Schedule 2 to the Police (Conduct) Regulations 2020) set out a clear framework of what type of conduct by a police officer is or is not acceptable. The framework includes the following categories that we believe are the most relevant to prejudicial and improper behaviour:

> **Authority, Respect and Courtesy**
>
> "Police officers act with self-control and tolerance, treating members of the public and colleagues with respect and courtesy. Police officers do not abuse their powers or authority and respect the rights of all individuals."

Equality and Diversity

"Police officers act with fairness and impartiality. They do not discriminate unlawfully or unfairly."

Discreditable Conduct

"Police officers behave in a manner which does not discredit the police service or undermine public confidence in it, whether on or off duty."

There is no one standard that covers all aspects of prejudicial and improper behaviour.

Another important standard places a responsibility on officers to report wrongdoing. That is:

Challenging and Reporting Improper Conduct

"Police officers report, challenge or take action against the conduct of colleagues which has fallen below the Standards of Professional Behaviour."

All aspects of prejudicial and improper behaviour would generally be covered by the standards of professional behaviour. So there is a specific duty for police officers to report, challenge or act if they witness it, or become aware of such behaviour exhibited by a colleague.

The College of Policing's Code of Ethics sets out in detail the principles and expected behaviours that underpin the standards of professional behaviour. The code places a duty on all police staff, as well as officers, to report any improper conduct.

How the police should deal with conduct matters

The Home Office guidance document, *Conduct, Efficiency and Effectiveness: Statutory Guidance on Professional Standards, Performance and Integrity in Policing*, sets out how the police should deal with reports of criminality or misconduct by officers. Where there is a breach of the standards of professional behaviour that is serious enough to justify disciplinary action, this would be classed as a "conduct matter".

Considering our definition of prejudicial and improper behaviour, it is likely that many reports of this nature will be criminal and require recording and investigating as such. Others will fall within the definition of, and should be recorded as, conduct matters.

Forces are unable to easily identify cases of prejudicial and improper behaviour

Without a standardised definition, most forces are unable to accurately assess the prevalence of prejudicial and improper behaviour. We carried out an investigation file review into cases of prejudicial and improper behaviour recorded in the preceding three years. All forces found it difficult to differentiate such cases from other conduct matters. There was no single category that could be used to identify them, or other means of flagging cases. We had to manually trawl all recorded cases to identify those that included elements of prejudicial and improper behaviour.

Recommendation 22

By 30 April 2023, the National Police Chiefs' Council, and the College of Policing, in consultation with the Independent Office for Police Conduct, should define prejudicial and improper behaviour, using the definition contained in this report or a suitable alternative.

All forces operate a professional standards database, in which they record details of public complaints and misconduct investigations. Almost all use the same IT system, but they tend to configure this slightly differently. The database has a flagging system, through which a flag to identify prejudicial and improper behaviour can be readily attached to reports.

Recommendation 23

By 31 October 2023, the National Police Chiefs' Council lead for complaints and misconduct, in consultation with the relevant IT provider and the Independent Office for Police Conduct, should arrange to add a prejudicial and improper behaviour identifier flag to the professional standards database used to record complaints and misconduct.

Recommendation 24

By 31 October 2023, chief constables should make sure their professional standards departments attach a prejudicial and improper behaviour flag to all newly recorded relevant cases.

Forces need to do more to collect intelligence relating to prejudicial and improper behaviour

We consider later in the report how forces can gather intelligence in relation to other forms of police corruption. During this inspection, we reviewed 236 complaint and misconduct cases that we considered fell under our definition of prejudicial and improper behaviour. Most of these cases came from reports from the public or from colleagues. Only 15 originated from forces actively looking for intelligence. This indicates that overall, forces are not doing enough to collect relevant intelligence.

In addition, in some of our previous reports discussed in Chapter 2, we have recommended that, in cases involving sexual misconduct, forces should routinely widen their inquiries. This is to establish whether the matter under investigation is part of a wider pattern of behaviour. Many of the examples in this report suggest that it often is. This includes both AoPSP and prejudicial and improper behaviour towards colleagues. The wider inquiries that forces should routinely make include:

- reviewing the use of IT systems;
- reviews of incidents;
- use of work mobile devices;
- reviews of body-worn video (BWV) recordings;
- radio location checks; and
- misconduct history.

During our investigation file review, we found that forces usually didn't carry out these wider inquiries.

Case study 23

A tutor constable sent text messages to a female student officer. She was aware that he had done this previously with other female student officers. She believed this was an attempt to form a sexual relationship with her, so reported the matter to a supervisor. The only enquiries the force's professional standards department (PSD) made were to check the officer's conduct and complaint history. This showed him to be of previous good character. The PSD didn't interview the tutor constable or any of his female student officers, nor did it carry out any other form of investigation. The PSD didn't attempt to establish whether the tutor's behaviour was part of a wider pattern. It filed the case with no further action taken. At the very least, we would have expected the PSD to speak with the tutor constable, clarify his intentions and, if necessary, take steps to make sure that any assessment of the trainees' conduct was carried out by someone not seeking or in a sexual relationship with any of them.

Recommendation 25

By 30 April 2023, chief constables should make sure their professional standards departments and counter-corruption units routinely carry out all reasonable wider inquiries when dealing with reports of prejudicial and improper behaviour. These inquiries should ordinarily include (but not be limited to) sampling the following, in relation to the officer under investigation:

- their use of IT systems;
- incidents they attended, and incidents they are otherwise connected to;
- their use of work mobile devices;
- their body-worn video recordings;
- radio location checks; and
- misconduct history.

Reports of prejudicial and improper behaviour should be dealt with more consistently

Reports of prejudicial and improper behaviour must be dealt with consistently. Initially, forces must consider the seriousness of the allegation and whether it is a crime or conduct matter. If it is a crime, it should be recorded and investigated as such. Reports of prejudicial and improper behaviour must be dealt with in accordance with the requirements of the:

- *Home Office Counting Rules 2022/2023*;
- Police (Conduct) Regulations 2020;
- Home Office Guidance, *Conduct, Efficiency and Effectiveness: Statutory Guidance on Professional Standards, Performance and Integrity in Policing*; and
- IOPC *Statutory Guidance*.

Conduct matters

The Home Office statutory guidance states:

> "The threshold for meeting the definition of a conduct matter is low. There need only be an indication that the person serving with the police may have committed a criminal offence or behaved in a manner that would justify disciplinary proceedings. However, not all conduct that comes to the attention of the appropriate authority will meet this threshold. For example, an indication that there has been a breach of the Standards of Professional Behaviour is not necessarily sufficient to meet the definition of a conduct matter, if disciplinary proceedings would not be justified. If the appropriate authority considers that there is no indication that the behaviour of the person in question may amount to a criminal offence or warrant disciplinary proceedings, the conduct can be dealt with outside of the formal conduct regime."

Under the Police Reform Act 2002 and the Police (Conduct) Regulations 2020, all complaints or conduct matters must be referred to a chief officer who performs the role of appropriate authority (AA). This role involves assessing the severity of the matter in question. This initial 'severity assessment' is followed by later interim assessments (as required) and a final assessment.

Under the Regulations, chief officers can delegate the role of AA to an officer of at least the rank of inspector (or police staff equivalent). And in practice, all chief officers do delegate the role. The AA decides whether the case is investigated and if so at what level.

Only cases that the AA determines may potentially constitute gross misconduct can result in dismissal. An assessment of gross misconduct doesn't mean that the officer concerned will automatically lose their job. It means that, if the case is proven, the chair of a misconduct hearing may choose to dismiss them. Conversely, an assessment of misconduct means that, even if the case is proven at a misconduct meeting, the chair may not dismiss them. Put simply, an individual to whom the chief constable has delegated the role of AA can't dismiss an officer. But they can place an officer in front of a gross misconduct panel under threat of dismissal and, arguably more importantly, they can decide not to do so.

So for the effective administration of the police discipline system, it is essential that police officers and staff performing the role of AA have a sufficiently high level of experience and training. The importance of this role cannot be overstated. By acting as a form of 'moral compass', they are the guardians of their police force's and – by extension – the police service's reputation.

Initial assessments by some appropriate authorities reveal leniency, apathy and too much tolerance of prejudicial and improper behaviour

In most of the 236 cases, we found that the standard of the decision-making was good. But there were examples of cases assessed at the outset as not misconduct, or as lower-level misconduct, which should have been assessed, at least potentially, as gross misconduct. By not assessing them as potential gross misconduct at this stage, the AA may effectively close the door to dismissal before any substantive investigation of the facts has taken place.

Case study 24

In 2021, a male police officer on patrol showed a female colleague an image of himself naked, in which his genitals were exposed. She had not asked for this and didn't want to see the image. She reported the incident. The AA assessed the case as misconduct only. The AA recorded in the file that it was at the "lower end of the misconduct scale". We don't know the full facts of this case, but it seems to us at least possible that an incident such as this could conceivably, depending on the circumstances, result in dismissal.

We heard of three other comparable cases. Two involved officers showing similar images to members of the public, while one involved showing an image to a colleague. The outcomes of these were dismissal, final written warning, and "words of advice". This inconsistency is concerning.

Case study 25

In 2021, a male officer met a female burglary victim at her home. He later contacted her via his personal WhatsApp account, requesting to take her out for a date. His use of her mobile number (obtained for a policing purpose only) potentially breached the Data Protection Act 2018. She made a complaint to the force. The officer's approach was contrary to the College of Policing's guidance on maintaining professional boundaries (referred to earlier).

On this occasion, while the AA recognised it as a potential AoPSP, it was assessed as 'misconduct only' and wasn't referred to the Independent Office for Police Conduct (IOPC). Once recognised as potential AoPSP, it should have been investigated as such and referred to the IOPC.

Case study 26

In 2021, a male officer repeatedly asked colleagues for details of his ex-girlfriend's (a serving member of police staff) shift pattern and work location. He also misused force computer systems to identify her work location. There were potential offences under the Computer Misuse Act 1990, the Protection from Harassment Act 1997, and the Data Protection Act 2018. She reported her concerns and alleged that he had stalked her four years previously.

In the initial assessment, the AA determined that the case didn't amount to misconduct. The PSD didn't investigate any of the allegations. In this case, the AA decided only to informally warn the officer about his behaviour.

Case study 27

In 2021, a young female police officer received several anonymous texts, the contents of which she found disturbing. She alleged that they came from a fellow officer and gave evidence to support her allegation.

At the time our fieldwork ended, this case (and several others involving allegations against the same officer) remained under investigation. The officer potentially committed offences under the Malicious Communications Act 1988, the Protection from Harassment Act 1997, and the Communications Act 2003. On the basis of the facts we heard, we believe that an assessment of gross misconduct was clearly warranted, as was a criminal investigation. So did the AA who initially assessed the case. But another AA disagreed and repeatedly sought to downgrade the initial assessment.

It appeared to us that, while this disagreement continued, the force didn't investigate the case. We concluded that the force's handling of this case (up to the point our fieldwork finished) was lamentable.

Case study 28

In 2020, a male police officer used the force email system to send a female colleague a series of emails, with the aim of developing a relationship with her. She was concerned about his behaviour and confided in another colleague, who reported it to the force. Based on the number and content of the emails, the force considered the matter to be criminal and recorded a crime of harassment accordingly.

A PSD officer spoke to the woman, but she didn't support any formal action. The AA determined that, despite the incident being recorded as a crime, there was no requirement for an investigation and that the case was suitable to be dealt with through the reflective practice review process. We found no evidence that the AA had considered continuing with the case without the support of the victim. In our opinion, the case should have been assessed as gross misconduct and investigated.

The standard of investigations

Forces have the capability to effectively investigate prejudicial and improper behaviour based on gender

Once the AA has determined that a case is to be investigated, a suitably trained investigator should be appointed. The investigator should be independent and have the requisite level of knowledge, skill, and experience to plan and manage the investigation.

We found PSDs had police officers from a range of policing backgrounds. Most had detective experience and accreditation to level two of the Professionalising Investigations Programme. In the preceding two years, forces had increased the resources available to PSDs and recruited officers with experience in working with vulnerable people and investigating sexual offences. This has increased their capability to investigate prejudicial and improper behaviour more effectively.

In one force, basic command units that assessed cases locally as gross misconduct sent them to the force's PSD. Sometimes, the PSD re-assessed these cases as misconduct only, and returned them to the basic command unit for a local misconduct investigation. In some cases, this resulted in the investigation being carried out by individuals who weren't suitably qualified investigators.

In most forces, PSDs briefed chief officers on the more serious allegations under investigation.

As we described earlier, we found some cases that forces had not referred to the IOPC in accordance with the statutory guidance. But in the main, forces did refer cases when required by the guidance to do so.

Of the 236 investigations we reviewed, most were effective and carried out in a timely way. In most cases, investigators followed relevant lines of inquiry. But they didn't always adopt the wider focus we discussed earlier in this report.

In 46 cases (almost 20 percent of the total), we found shortcomings in the investigation. In most of these cases, there was no investigation plan and a lack of supervisory oversight. And often, not all relevant lines of inquiry had been completed before the case was closed.

Case study 29

A student officer reported that her tutor constable was sexually harassing her. The PSD interviewed the tutor, who admitted his behaviour was wrong. Nothing was recorded on the file to show what (if any) wider investigative action the PSD took, and the file was closed with no further action taken. The PSD didn't record its rationale for this decision.

Case study 30

An officer's supervisor suspected him of being in a relationship with a woman and having sex with her while on duty. The force held intelligence to suggest that the woman was a victim of domestic abuse and had in the past been a victim of child sexual abuse. The circumstances of this case led us to conclude that it would have been reasonable to suspect misconduct in public office (a common law offence) or an offence of corrupt or improper exercise of police powers and privileges under the Criminal Justice and Courts Act 2015. Accordingly, the officer could have been arrested and search powers could have been used to look for any other evidence, such as digital devices. The investigating officer proposed arrest, but the AA opposed it. The PSD contacted the woman concerned, who declined to help. The PSD didn't contact any other witnesses, didn't make any wider inquiries, and closed the case prematurely.

Case study 31

A female officer reported her supervisor for sending her numerous and unwelcome text messages with a sexual connotation. She believed he had sent similar messages to other female officers. She reported her concerns. There were potentially offences under the Protection from Harassment Act 1997 and the Communications Act 2003.

The AA decided that the case was suitable to be addressed through reflective practice and chose not to investigate it. We believe this case should have been investigated.

The focus of investigations is sometimes too narrow

In some of the cases we reviewed, investigators had focused only on the circumstances of that case. As we discussed earlier in this report, investigators often don't consider that current alleged behaviour may well be an indicator of a wider pattern of behaviour. This lack of consideration means that investigators frequently miss opportunities to identify further misconduct or even criminal behaviour, potentially involving members of the public. Expanding investigative parameters in this way should be built into investigation plans.

Recommendation 26

By 30 April 2023, chief constables should make sure their professional standards departments:

- produce and follow an investigation plan, endorsed by a supervisor, for all misconduct investigations; and
- check all reasonable lines of inquiry in the investigation plan have been concluded before finalising the investigation.

Some appropriate authorities' final assessments were too lenient

When an investigation is completed, the investigator submits a report to the AA, giving their opinion as to whether there is a case to answer. The AA makes the final decision whether there is a case to answer and, if so, at what level (misconduct or gross misconduct). If there is no case to answer, the matter will be closed or may be dealt with through reflective practice.

In many of the cases we reviewed, we found that the quality of the investigating officer's report and the final decision made by the AA was good.

But we found too many occasions where the investigating officer recommended a case to answer for gross misconduct, only for the AA to disagree. These included the AA reducing cases from gross misconduct to misconduct only, or even deciding that no further action will be taken. We often found a lack of recorded rationale behind these decisions. In some cases, even when the decision-maker had recorded their rationale, we strongly disagreed with their decision.

Case study 32

A police officer alleged that his supervisor (a senior officer) had acted inappropriately towards him on five separate occasions. The behaviour appeared to amount to sexual harassment. The senior officer was alleged to have made sexual comments on four occasions. These comments were not witnessed by anyone else. On the fifth occasion, the senior officer twice slapped the complainant's inner thigh and declared to another officer who was present that he and the complainant were in an intimate relationship. The male officer then made a report to PSD.

The AA recorded that it was the complainant's lack of earlier objection that "failed to nip this behaviour in the bud". In our view, this was a serious misjudgment and a wholly inappropriate placing of responsibility on the victim. The AA concluded the conduct was not serious enough to justify misconduct proceedings and that 'management advice' was sufficient. The senior officer was advised about his conduct. We believe that this was a case of potential gross misconduct and a possible criminal offence under the Sexual Offences Act 2003 and should have been investigated as such.

This case study aligns with our fieldwork, which revealed a widely held perception that allegations against senior officers were less likely to be dealt with properly.

Case study 33

A female officer alleged that she had been sexually assaulted twice by a male colleague. She also alleged that he had made several homophobic comments about other police officers and staff. We found corroboration in the case file to support the allegation of homophobic comments. The investigating officer recommended there was a case to answer for gross misconduct. The AA disagreed, and the case was closed with no action taken. We do not agree with this decision. We believe there was a case to answer for gross misconduct as there were two possible criminal offences and the use of homophobic comments amounted to discriminatory behaviour.

Case study 34

A sergeant reported that a male police officer had sexually assaulted three female student officers while out socially. This sergeant had witnessed the behaviour. The AA initially assessed the case as gross misconduct. The incident was the subject of an investigation. The three female officers all stated that the male had sexually touched them, but they declined to make a formal allegation. The officer, a student officer, was interviewed and he admitted that his behaviour was wrong. The investigating officer concluded there was a case to answer for gross misconduct. The AA disagreed and directed that the student officer was given advice regarding his behaviour. We do not agree: the facts in the case file support a case of gross misconduct.

Case study 35

An off-duty officer was involved in a domestic incident with his partner. During the argument the officer brandished a knife and grabbed his partner's arm to prevent her calling the police. The partner contacted the police, and they arrested the off-duty officer on suspicion of assault. The officer made some admissions when he was interviewed, including preventing the victim from telephoning the police. The police investigated the case as a crime of assault and submitted a file to the Crown Prosecution Service (CPS), seeking authority to charge the off-duty officer. The CPS didn't authorise the charge, mainly because the victim didn't support the prosecution. The AA had initially assessed the case as gross misconduct. But at the conclusion of the criminal investigation, it was re-assessed as misconduct due to the CPS decision. The CPS decision didn't alter the facts of the case and should not have influenced the AA.

The case was considered at a misconduct meeting and the officer received a final written warning. We believe the AA failed to properly consider culpability, harm, aggravating and mitigating factors and that the facts supported a case of gross misconduct.

The negative effect of overly lenient assessments

We were told in focus groups, and in our survey, that when appropriate authorities make overly lenient assessments this can undermine staff confidence, discourage the reporting of wrongdoing and harm the police service's reputation. Many interviewees said that their allegations weren't taken seriously. One woman, who reported sexual misconduct by a colleague, told us:

> "I will never report anything again – I have lost every piece of confidence I had in my force. I will never put myself through that again."

Another interviewee said:

> "There has been a sea-change at the top of the organisation, but this has not reached the bottom yet. Instances [of prejudicial and improper behaviour] are often not reported because there are still examples of what female officers regard as poor decisions."

The same interviewee stated that a sergeant on their team had been reported three times for racist and sexist comments. The interviewee described the sergeant as a "sex pest" towards female officers. The allegations were referred to the AA as potential gross misconduct. On each occasion, the AA returned the case to the local area, with a recommendation for reflective practice rather than misconduct proceedings. The interviewee found this incredibly frustrating and believed that it sent a message that the organisation didn't support female officers who reported such matters.

The reflective practice review process is designed to deal with lower-level misconduct or performance issues. We believe reflective practice wasn't suitable in this case.

An absence of quality assurance processes

None of the forces we visited used any kind of quality assurance process for AA decisions, from the initial assessment through to the final decision. It is patently wrong that an allegation in one force can be assessed as gross misconduct (meaning an officer is under threat of dismissal), while in a different force a similar allegation can be assessed as misconduct only, suitable for reflective practice or even that no further action is needed.

Based on the evidence we gathered in this inspection, consistency in decision-making needs to be improved.

Recommendation 27

By 30 April 2023, the National Police Chiefs' Council lead for complaints and misconduct should design a sampling regime for appropriate authorities' decisions. This is to quality assure the decisions and identify any learning. The sampling should make sure that appropriate authorities' decisions:

- are consistent;
- maintain public confidence in, and the reputation of, the police service;
- uphold high standards in policing and deter misconduct; and
- protect the public.

MPS *Rebuilding Trust Plan* and Operation Rainier

In October 2021, the Metropolitan Police Service (MPS) published its *Rebuilding Trust Plan*. As part of this plan, the force reviewed all current investigations into sexual misconduct and domestic abuse allegations against its police officers and staff. This review aimed to make sure complainants were properly supported and that investigations were carried out to the required standard. The MPS assessed that only 68 percent of investigations were of the required standard.

As part of the plan, the MPS also carried out a dip sample of historic sexual misconduct and domestic abuse cases. These involved allegations from the preceding ten years, where the alleged perpetrator was still working in the force. This work, known as Operation Rainier, involved the review of 348 criminal and misconduct cases. The MPS assessed that only 58 percent of these cases were investigated to the required standard.

Neither of these reviews commented on the AA's decision-making.

The MPS was the only force we inspected that had carried out reviews of historic cases where officers were still serving. The force deserves credit for doing so. These reviews revealed lessons to be learned. We are encouraged that the MPS review has resulted in several recommendations intended to improve the way that it deals with misconduct investigations.

NPCC review of sexual misconduct cases

In December 2021, the NPCC requested that all forces review all their current sexual misconduct cases involving police officers and staff. The terms of the review requested by the NPCC are different from our file review. Given the concerning findings from our file review, we believe that all forces should also carry out a more thorough review in line with the following recommendation.

Recommendation 28

By 30 April 2023, in the forces where we have not carried out fieldwork during this inspection, chief constables who have not already carried out a review of all allegations relating to prejudicial and improper behaviour should do so. The review should be of cases from the last three years where the alleged perpetrator was a serving police officer or member of staff. The review should establish whether:

- victims and witnesses were properly supported;
- all appropriate authority assessments, including assessments which didn't result in a complaint or misconduct investigation, were correct;
- investigations were comprehensive; and
- any necessary steps are taken to improve the quality of future investigations.

These reviews will be subject to examination during our next round of inspections of professional standards departments.

The College of Policing keeps a list of police officers and staff on the barred and advisory lists

The College of Policing has responsibility to keep a list of all police officers, special constables and staff members that have been dismissed from police forces. This is called the barred list, which is published. When processing recruitment applications, police forces routinely refer to the barred list to see if any applicant's name appears on it. Individuals stay on the list indefinitely unless they win an appeal against their dismissal or make a successful review application. (For the latter, they would have to provide clear evidence as to why they were now suitable to re-join the police.)

There is also an advisory list, which is not published. This contains the details of all police officers, special constables and staff members who have resigned or retired during an investigation or who leave before an allegation comes to light. They cannot remain on the advisory list permanently. They stay there until the conclusion of any proceedings, which should continue even after they have left the service.

If a case of gross misconduct is found against them, and the decision would have been dismissal, they will be added to the barred list. If no disciplinary proceedings are brought, or it is decided that the matter is misconduct only, the person will be removed from the advisory list.

Forces must continue gross misconduct investigations after resignation or retirement

The Home Office's guidance on *Police Officer Misconduct, Unsatisfactory Performance and Attendance Management Procedures* requires forces to continue with proceedings against former police officers. The document states:

> "Those officers who choose to give notice to resign or retire following an allegation that amounts to gross misconduct will remain subject to the Conduct Regulations and the Complaints Regulations by virtue of the Former Officer Regulations. This allows misconduct investigations and proceedings that could have led to dismissal to be taken to their conclusion, notwithstanding the departure of the police officer."

This is intended to make sure that the purposes of the misconduct process are met. These are to:

- maintain public confidence in, and the reputation of, the police service;
- uphold high standards in policing;
- deter misconduct; and
- protect the public.

The requirement to continue with proceedings aims to make sure that police officers who retire or resign to avoid gross misconduct proceedings are still accountable for their actions.

We were pleased to find that forces usually continue with investigations when police officers and members of staff resign or retire. Often, this leads to a misconduct hearing.

Of the 236 cases we reviewed, there were four occasions where police officers left the service (they either retired or resigned) and the forces concerned didn't continue with their gross misconduct investigations. In each instance, the force didn't record its rationale for not continuing with the case. In these cases, it was far from clear to us whether the force had made a sound decision to discontinue.

8. Discharging unsuitable student officers

Regulation 13 of the Police Regulations 2003

Regulation 13 of the Police Regulations 2003 provides a relatively straightforward way to "discharge" an officer who remains within their probationary period (the relevant Home Office guidance uses the term "dispense with the services of"). The purpose of the provision is to provide a similarly easy way to discharge those in their probationary period as applies in other workplaces. The test to be met for Regulation 13 to be applied is that the chief officer considers that the police officer in question:

> "is not fitted, physically or mentally, to perform the duties of his office, or that he is not likely to become an efficient or well conducted constable".

The probationary period applies to the services of a constable, direct entry (DE) inspector and DE superintendent.

Some forces are reluctant to use regulation 13

We were told during our inspection that when it comes to conduct, Regulation 13 can work well. It is a simple and effective tool. However, some forces are reluctant to use it.

A senior officer told us that, given the nature of policing, officers often feel more comfortable operating in a more structured environment, such as those provided by the Police (Conduct) Regulations 2020. They are less comfortable with the more flexible arrangement of Regulation 13. This officer said:

> "The service is frightened of a shadow of its own making and, that in reality, doesn't exist."

Indeed, we found occasions when the Police (Performance) Regulations 2020 ('the performance Regulations') had been used rather than Regulation 13 to manage underperforming police officers who haven't completed their probationary period. But the performance Regulations do not apply to officers who haven't completed their probationary period.

If an officer is under-performing in their probationary period, their services can and should simply be discharged under Regulation 13 as an officer who is not likely to become an efficient or well-conducted officer. The extensive protections and procedures set out in the performance Regulations are superfluous in such a case.

We have sought legal advice on this matter. Any use by a force of the performance Regulations in respect of an officer in their probationary period, even if to provide that officer with additional protections, is, in our view, unlawful. There is no legal justification for it.

Recommendation 29

With immediate effect, chief constables must make sure that forces use Regulation 13 of the Police Regulations 2003 for underperforming officers during their probationary period, rather than the Police (Performance) Regulations 2020.

The introduction of the Police Education Qualification Framework means regulation 13 should be extended to include academic ability

Some senior officers were concerned that the terms of Regulation 13, and particularly the test to be satisfied, were not suitable to address cases in which officers during their probationary period have not successfully met the academic requirements imposed on them by new entry routes into the police under the police education qualification framework (PEQF).

The PEQF creates new entry routes into the police service and provides education to degree level for successful applicants. Inevitably, this imposes academic requirements that student officers must meet to complete their probationary period. Officers joining through a DE route must also pass examinations.

This raises the question of whether an officer who, during their probationary period, has failed the academic requirements of their entry route can be discharged by a chief officer on the grounds that they aren't fit mentally to perform their duties, or that they aren't likely to become an efficient officer. Currently, Regulation 13 is the only available option for police forces in this context. In some senses, academic performance could be said to be relevant to the mental fitness of an officer. But the Regulation's reference to physical and mental fitness together is clearly intended to address matters relating to the health of the officer, rather than their academic ability.

The likelihood of a person becoming an "efficient" officer encompasses, on a natural reading of the term, a very broad array of factors.

A person who cannot meet the educational standards required by the PEQF (or failed to make sufficient efforts to make sure that they did) is unlikely to become an efficient and well conducted officer.

The language of efficiency in Regulation 13 appears broad enough to provide a way to discharge all unfit officers during their probationary period, regardless of their entry route into the service. But we acknowledge a degree of legal risk because the point is untested, and there is likely to be litigation in connection with it at some stage. Although we would expect such litigation to be successfully defended, the matter might be put beyond doubt if Regulation 13 was changed to address the issue relating to entry routes.

Recommendation 30

By 31 December 2023, the Home Office, working with the National Police Chiefs' Council lead for complaints and misconduct and the College of Policing, should make sure that forces can use Regulation 13 of the Police Regulations 2003 effectively to discharge probationers who don't achieve the required educational or academic standard during their probationary period.

Using Regulation 13 to deal with misconduct

Chief officers have discretion whether to use the misconduct procedures (within Police (Conduct) Regulations 2020) or Regulation 13 of the Police Regulations 2003 (discharge of probationer) as the most appropriate way of dealing with a misconduct matter involving a student officer.

The Home Office's guidance on *Conduct, Efficiency and Effectiveness: Statutory Guidance on Professional Standards, Performance and Integrity in Policing* states that allegations of gross misconduct should usually be subject to disciplinary proceedings rather than the Regulation 13 route. In addition, in cases where the conduct is denied, misconduct proceedings should be used.

Current advice from the National Police Chiefs' Council states that:

> "Where a student officer breaches the Standards of Professional Behaviour only to the extent that a written warning would be justified for an officer confirmed in the rank, for that student officer, the level of the breach could be sufficient to determine that they would not likely become a 'well conducted constable'."

So even for conduct cases that are not classed as gross misconduct, if proven or admitted, it is appropriate that the discharge of the officer under Regulation 13 should be considered. This too is consistent with how those in a probationary period would usually be treated in other forms of employment.

Officers discharged in accordance with regulation 13 are not placed on the College of Policing barred list

Where a Regulation 13 procedure has been used and it has led to the discharge of an officer during their probationary period, the Police Barred List and Police Advisory List Regulations 2017 do not allow for the officer to be added to the police barred list. This includes officers who have been discharged using Regulation 13 for conduct matters.

We have stated earlier in this report that during the police officer recruitment process there is often an absence of pre-employment checks. This creates the potential for an individual who has had their service discharged under Regulation 13 to reapply to another police force without disclosing that they had previously served with another force. They could therefore be reappointed or re-employed in policing in future without their new force being aware of their previous service.

We find that this is unsatisfactory. There may be a case for the Home Office and the College of Policing to consider creating a separate list, containing the details of individuals who have had their services discharged under Regulation 13 for conduct-related matters. It may be appropriate to restrict access to the list to those involved in the future employment of police officers and staff.

Recommendation 31

By 31 October 2023, the Home Office, working with the College of Policing and the National Police Chiefs' Council lead for complaints and misconduct, should make sure that, during pre-employment or vetting checks, police forces can identify any applicants previously discharged under Regulation 13 of the Police Regulations 2003.

9. Managing corruption-related intelligence

We examined how well the forces we visited attempted to prevent corrupt activities by officers and staff. This included the abuse of position for a sexual purpose (AoPSP).

Awareness of AoPSP among officers and staff is good

In the forces we inspected, officers and staff had been required to complete online training relating to AoPSP. Forces kept records of the staff who had completed this. Most of the staff we spoke to understood what AoPSP was and recognised it as police corruption.

In 2021, South Wales Police surveyed its workforce to sample its knowledge of what AoPSP and inappropriate relationships are. A total of 823 members of the workforce completed the survey. Results indicated that 90 percent knew what these are, how to report them and the types of people who could be victims.

Most of the forces we inspected use examples of previous AoPSP cases for training purposes. Some also pose 'ethical dilemmas' on their intranet, some of which relate to AoPSP. These prompt police officers and staff to think about how they would react to circumstances in which they may find themselves. They post their responses online, which are then assessed centrally. The force then publishes its desired outcome. If the workforce responses don't broadly match this, the force repeats the exercise, posing a similar dilemma a few months later.

In an earlier inspection, we found that forces weren't always referring AoPSP cases to the Independent Office for Police Conduct (IOPC) when they should. Our findings prompted a recommendation and a firming up of the IOPC's *Statutory Guidance*, which mandated all forces to refer all AoPSP cases. During this inspection, we found that knowledge of the relevant requirements had improved considerably. With one exception, all the cases we reviewed had been correctly referred.

Some improvement in the management of the risk of AoPSP is needed

If forces become aware of a police officer or member of staff who is potentially a perpetrator of AoPSP, they should assess the risk posed by that individual. During our review of counter-corruption unit (CCU) intelligence cases recorded as sexual misconduct, we found that forces we visited tended to do this using a 'risk matrix' (that forces continue to modify). This prompts the assessor to consider all the circumstances and record the findings. CCUs then categorise each case as low, medium, or high risk.

The types of behaviour that would trigger someone to be assessed against the risk matrix include:

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

Individuals assessed by forces as medium or high risk should be subject to additional oversight. We found that some forces were good at providing this additional oversight, but others weren't. An example of the former is South Wales Police.

Operation Waterloo

South Wales Police has run Operation Waterloo since 2016. It is a proactive CCU operation to identify police officers and members of staff who may pose a risk of AoPSP. Following the risk assessment, the force keeps a list of those whose behaviour causes concern and monitors them accordingly. The additional oversight generally involves enquiries such as monitoring officers' IT use, examination of their body-worn video (BWV), and dip sampling the quality of their work.

We were less impressed with the quality of additional oversight that other forces provided.

Recommendation 32

By 30 April 2023, chief constables should make sure that:

- all intelligence concerning possible sexual misconduct by officers or staff (including abuse of position for a sexual purpose and internal sexual misconduct) is subject to a risk assessment process, with action taken to minimise any risk identified; and
- rigorous additional oversight arrangements are in place to monitor the behaviour of officers subject to the risk assessment process, especially in cases assessed as high risk.

Not all forces record AoPSP correctly

Of the 616 intelligence files we reviewed, we found that 158 related to sexual misconduct. Of those, 28 items had been incorrectly recorded as AoPSP. These cases related to sexual misconduct involving police officers and staff only, rather than involving officers pursuing relationships with members of the public.

We define AoPSP as:

> Behaviour by a police officer or police staff member, whether on or off duty, that misuses their position, authority or powers to pursue a sexual or improper emotional relationship with a member of the public.

The National Police Chiefs' Council has a more detailed definition in its national strategy. Both definitions describe AoPSP as sexual misconduct between a member of the workforce and a member of the public. Neither includes sexual misconduct towards or between colleagues.

The mis-recording of AoPSP has consequences for force and national-level analysis of the risks. If the data isn't accurate, it can't be wholly relied on.

Area for improvement 4

Forces' data quality is an area for improvement. Forces should make sure that they accurately categorise all items of sexual misconduct intelligence. Sexual misconduct cases that don't meet the definition of AoPSP (because they don't involve the public) shouldn't be recorded as AoPSP.

Police should forge better links with organisations that support vulnerable people

In our 2019 PEEL spotlight report *Shining a light on betrayal: Abuse of position for a sexual purpose*, we recommended that all forces that hadn't yet done so should establish regular links between their CCUs and agencies and organisations that support vulnerable people. This has also been included as specific force recommendations in other individual force reports.

We found that most, but not all, forces have developed links with organisations that support vulnerable people.

One force received information from a support agency that an officer was having sex with a woman in return for advising her where to shoplift with the least likely chance of being caught.

In another force, counter-corruption staff told us they had held 13 events with staff in external agencies that support vulnerable people. These were to highlight to attendees the signs of AoPSP and encourage any intelligence relating to it to be reported to the police.

Where these links weren't in place, it was sometimes because of CCUs believing it was someone else's responsibility. Most, if not all forces, will have some form of operational link with these agencies. In larger forces, there can be a perception that someone else in the force would be told if staff from an agency reported concerns about an officer.

Forces told us that, due to the pandemic, these links had, for obvious reasons, weakened. They need to be reinvigorated and maintained. Especially as staff in all agencies and police CCUs can change on a regular basis.

Recommendation 33

By 31 March 2023, chief constables should make sure that counter-corruption units (CCUs) have established relationships with external bodies that support vulnerable people who may be at risk of abuse of position for a sexual purpose, such as sex-worker support services, drug and alcohol and mental health charities. This is to:

- encourage the disclosure by such bodies, to the force's CCU, of corruption-related intelligence relating to the sexual abuse of vulnerable people by police officers and staff;
- help the staff from these bodies to understand the warning signs to look for; and
- make sure they are made aware of how such information should be disclosed to the CCU.

Forces don't do enough to collect corruption-related intelligence

In our 2019 report *Shining a light on betrayal: Abuse of position for a sexual purpose* we recommended:

> "By April 2020, all forces that haven't yet done so should make sure they have enough people with the right skills to look proactively for intelligence about those abusing their position for a sexual purpose, and to successfully complete their investigations into those identified."

All forces should be constantly looking for corruption-related intelligence, which obviously includes the internal and external elements of sexual misconduct. Most forces react well when they receive corruption-related intelligence, but the better CCUs proactively look for it.

As part of our intelligence file review, we asked forces to identify 100 items of corruption-related intelligence from the top 9 national corruption intelligence categories. From those, we randomly selected 60 to review. We also asked the forces to identify all the sexual misconduct intelligence files they created between 1 October 2018 and 30 September 2021.

In total we reviewed 616 files. Almost all the files we reviewed as part of this inspection involved forces reacting to items of intelligence that had been referred to the CCUs. Only 15 were as the result of proactive intelligence collection, and these were all using IT monitoring.

We expected to find greater use of other forms of proactive intelligence collection, such as:

- more extensive monitoring of IT systems;
- access to mobile data;
- analysis of communications data;
- people intelligence meetings;
- internal reports of sexual misconduct;
- identification of financial irregularities, such as inappropriate or excessive overtime claims or abuse of corporate credit cards;
- identification and assessment of officers with a propensity to attend certain types of incidents (usually those involving vulnerable people); and
- monitoring compliance with counter-corruption policies.

The evidence from this inspection – from the survey, from interviewees, from our analysis of events, from the investigation file reviews – tends to suggest that, if forces went looking for corruption, they would find it. The fact that, largely, they aren't is regrettable. Forces should do more to proactively search for such intelligence, using the well-established methods we describe above.

Recommendation 34

By 30 April 2023, chief constables should make sure that their counter-corruption units actively seek corruption-related intelligence as a matter of routine.

Lawful business monitoring

Lawful business monitoring (LBM) is a legitimate way for forces to monitor their information systems and methods of communication.

LBM is governed by the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018, which authorises public authorities to monitor and record internal business communications.

Use of LBM helps forces make sure that access to police systems and use of communication devices is for a lawful policing purpose. By using LBM, forces seek to identify unlawful access to police records, wrongful disclosure of police data, computer misuse and improper use of communication devices.

The Counter-Corruption (Intelligence) APP gives guidance on IT monitoring

The Counter-Corruption (Intelligence) APP (unpublished) states that the use of monitoring and auditing software has significant prevention, intelligence gathering and enforcement advantages. This APP lists these as:

- ensuring the integrity and security of personal data and operational information held by forces;
- deterring computer misuse;
- enhancing the operational security of serious and complex investigations; and
- providing a reactive and proactive investigative capability.

The use of such systems allows alerts to be created, which immediately tell investigating officers when a specific file has been accessed or printed.

CCUs should use IT monitoring software more effectively

Most forces have the capability to use IT monitoring to gather corruption-related intelligence to enhance their ability to identify corrupt individuals. IT monitoring can be particularly useful when identifying irregular use of systems and use by officers and staff who are of concern to the force. Automated checks can be used:

- when investigating individuals where there are integrity concerns;
- in cases where mitigations are required because of notifiable associations;
- where concerns are raised through the vetting process; and
- to make sure that access to force data is for a lawful policing purpose.

In some of the forces we visited, we found IT monitoring was being used to support investigations reacting to intelligence received. As we discussed earlier in the report, we found little evidence of IT monitoring being used proactively to identify corruption-related intelligence.

In January 2017, we stated in our national report *PEEL: Police Legitimacy 2016* that:

> "The ability of a force to prevent and detect misuse of the information held on its computer systems is an important means of preventing corruption. Protecting this information is vital to integrity and operational effectiveness. Forces must therefore be able to monitor and audit all their information technology (IT) systems to help identify individuals who misuse them for corrupt activity. For example, this could include inappropriate access to personal information, passing on information to organised crime gangs or using systems to identify vulnerable victims for sexual abuse."

Similarly, in our 2019 PEEL spotlight report *Shining a light on betrayal: Abuse of position for a sexual purpose* we made a national recommendation that by April 2020:

> "Where forces are yet to implement an effective ICT monitoring system that allows them to monitor desktop and handheld devices, they should do so as soon as reasonably practicable."

Despite this 2019 recommendation, we found that three of the forces we inspected still lacked this essential capability. We were told that plans were in place to introduce IT monitoring systems in two of the forces.

In forces where there was IT monitoring, it was often used for proactive intelligence collection and as an option to further the scope of investigations. In those forces without it, the absence of IT monitoring capability undoubtedly has a detrimental effect on their capabilities. The comments we made about the Metropolitan Police Service in the DMIP report apply to some other forces too. It is high time that those forces that have not yet introduced IT monitoring took the matter much more seriously, learned from other forces that have done so, and resolved to deal with the material threat of the abuse of their IT systems by corrupt officers and staff.

As a result of our findings in this inspection, we are compelled to repeat our recommendation from 2019.

Recommendation 35

By 31 March 2023, to protect the information contained within their systems and help them to identify potentially corrupt officers and staff, chief constables should make sure that:

- their force has the ability to monitor all use of its IT systems; and
- the force uses this for counter-corruption purposes, to enhance its investigative and proactive intelligence gathering capabilities.

There are gaps in the management of mobile devices

Management of mobile devices is important when protecting information. It is essential that forces have accurate records of who has each device so that the person can be held accountable for its use. Police officers and staff must also understand the restrictions on the use of force-supplied devices to make sure they are not used for unauthorised purposes.

Some forces told us they could not attribute all force mobile devices to named personnel. Forces that could do so had worked with their IT departments to prevent access to force systems unless the device was attributed. This should be seen as standard practice.

The forces that told us they couldn't attribute all force mobile devices are carrying greater information security and corruption risks. In at least one instance, the matter was on the force risk register.

Recommendation 36

By 30 April 2023, chief constables should establish and begin operation of an improved system of mobile device management, with accurate record keeping concerning:

- the identity of the officer or staff member each device is allocated to; and
- what each device has been used for.

Most forces don't allow the use of encrypted apps on force devices

The use of encrypted apps on mobile phones makes it very difficult to monitor what officers and staff are sharing on their work phones. We were pleased to see that most forces do not allow encrypted apps on their force mobiles as a matter of routine.

We found examples of force information being shared to private devices through encrypted apps. Forces cannot monitor or audit such use. We recognise that operational information may be shared on private phones with the best of intentions – for example, because not all officers are provided with a work phone, or it isn't as easy to share images on work phones. But it is nonetheless unacceptable, regardless of the intention of the officer.

Personnel in most forces told us they were uncertain of their forces' policies on the use of social media and encrypted messaging platforms for work purposes (on work and personal devices).

Using intelligence to identify officers and staff who pose a corruption risk

Few forces hold 'people intelligence meetings'

People intelligence meetings help to identify officers and staff who may pose a corruption threat to the force. 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 is not limited to, information relating to:

- unsatisfactory performance management;
- sickness management and absenteeism;
- public complaints;
- corruption-related intelligence;
- internal misconduct cases;

- internet use;
- 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.

Officers and staff discussed in these meetings can often appear in more than one category. Because relevant information is often held by several departments, corruption risks can easily be missed.

During this inspection, we found that only one of the forces we visited regularly held people intelligence meetings. In some forces, we were told that there were informal arrangements to help these conversations to occur. Without an established process, forces are missing opportunities to identify officers and staff of concern.

Recommendation 37

By 30 April 2023, chief constables should:

- convene, and hold on a regular and continuing basis, people intelligence meetings; or
- establish and begin operation of an alternative process to support the presentation and exchange of corruption-related intelligence, to identify officers and staff who may present a corruption risk.

Most CCUs are correctly categorising corruption-related intelligence

The Counter-Corruption (Intelligence) APP lists 12 categories of corruption-related intelligence. It is good practice for forces to use these categories when recording intelligence. All forces should do this consistently to help them understand the threats they face. The National Crime Agency (NCA) combines local and regional counter-corruption threat assessments (discussed later) to produce a national assessment.

Forces should compare their local assessment to the national document and identify any gaps in their understanding. These should be addressed in their control strategy (which we discuss later). Use of the national corruption-related intelligence collection categories is essential if forces are to play their part in this process.

The Counter-Corruption (Intelligence) APP states that only behaviours that meet the definition of police corruption should be reported as such. The categories are:

- infiltration;
- disclosure of information;
- perverting the course of justice;
- sexual misconduct;
- controlled drug use and supply;
- theft and fraud;
- misusing force systems;
- abuse of authority;
- inappropriate association;
- vulnerability;
- commit, incite, aid, and abet, or assist an offender in the commission of, a crime; and
- other [corruption-related intelligence not categorised elsewhere].

We used the first nine of these to identify the corruption-related intelligence during our intelligence file review.

In our 2019 PEEL spotlight report *Shining a light on betrayal: Abuse of position for a sexual purpose* we recommended that, by April 2020, all forces that haven't already done so should record corruption using the national corruption categories.

Despite this recommendation, regrettably, two of the forces we inspected were still not routinely using the national categories. One force told us that it was planning to start using them. The other had implemented an IT solution as a 'workaround', but it wasn't working properly.

Recommendation 38

By 30 April 2023, chief constables should make sure that all corruption-related intelligence is categorised in accordance with the National Police Chiefs' Council counter-corruption categories (and any revised version of these).

Most officers and staff were aware of how to report wrongdoing by colleagues

The Code of Ethics places a duty on officers and staff to challenge and report improper conduct. This means that an officer or a member of staff would be in breach of the standards of professional behaviour and at risk of misconduct procedures if they don't report wrongdoing.

In the forces we visited there was a variety of ways in which police officers and staff could raise a concern or report a wrongdoing. These include:

- telling a supervisor or colleague;
- reporting directly to the professional standards department (PSD) or the Independent Office for Police Conduct;
- using an internal confidential system, either on the phone or online; and
- contacting an independent third-party company contracted by the force to carry out this function, such as CrimeStoppers.

In the forces we visited, we found that most staff were aware of the confidential reporting system and how to access it. All the officers and staff we spoke to were aware of their responsibility to report wrongdoing.

Of the 616 corruption-related intelligence files we reviewed, 118 originated from reports made through confidential internal systems.

Some staff told us that they were concerned that the system was not truly confidential and that individuals who wished to remain anonymous could be identified. All the systems we saw allowed the reporter to remain anonymous, and we found no instances where confidentiality had been breached. Nevertheless, forces may wish to give personnel further reassurance.

All forces inspected had a policy that described the support available to any police officer or member of staff who reported wrongdoing. Most interviewees believed that anyone reporting wrongdoing would be supported. But there were some who believed that such individuals could feel exposed and isolated. And some survey respondents made broadly similar comments.

Counter-corruption strategic threat assessments

The Counter-Corruption (Intelligence) APP says that all forces should produce an annual counter-corruption strategic threat assessment, detailing the corruption threats they face. They should then use this assessment to:

- identify corruption threats and emerging issues;
- identify locations for corruptors and corrupt activity;
- profile potentially corrupt officers and corruptors; and
- highlight individual and organisational vulnerabilities.

Forces should then use the findings from this, and the NCA's national threat assessment (unpublished), to identify any intelligence gaps they have and produce a control strategy. This should identify the action the force will take to tackle corruption. This is usually achieved through an action plan with nominated individuals who are responsible for implementing the actions and giving timely updates as progress is made.

The threat assessment often contains sensitive information which is unsuitable for disclosure to the entire workforce. For example, it may identify vulnerabilities, enforcement tactics and details of operational security. The Counter-Corruption (Intelligence) APP advises that a sanitised version, with these details removed, can be used to convey the main points to the whole workforce. They are then better informed and equipped to identify potential signs of corrupt activities.

Most forces are now using strategic threat assessments to understand corruption risks

We found that most of the forces we inspected had prepared a counter-corruption strategic threat assessment that was fit for purpose. In those forces, a control strategy had also been produced. This was used to make sure that any work needed to deal with the threats identified was carried out. In most forces there was oversight and responsibility for these tasks. But in one force it was not clear who was responsible for this work, and we found no evidence that the work had taken place.

In another force, no threat assessment or associated control strategy had been prepared. Without these, the force lacked a detailed enough understanding of the corruption threats and risks it faced. It couldn't provide essential information to inform the regional and national threat assessments. This is not acceptable.

This isn't a new finding. In our 2019 PEEL spotlight report *Shining a light on betrayal: Abuse of position for a sexual purpose*, we said that "twenty-six forces either didn't have a current local strategic CCU threat assessment or had one that we judged to be unsatisfactory". We recommended that, by April 2020, they should produce a strategy in accordance with the Counter-Corruption (Intelligence) APP.

We are compelled to repeat this recommendation.

Recommendation 39

By 30 April 2023, chief constables should make sure they have a current counter-corruption strategic threat assessment, in accordance with the Counter-Corruption (Intelligence) Authorised Professional Practice.

Missed opportunities to inform the workforce of current corruption threats

Some forces were effective at informing their workforce about the corruption threats faced by the force. Often these were summarised and available on the force intranet. In some forces, senior PSD officers briefed local senior management teams regarding the current threat assessment.

In others, we found that police officers and staff were not made aware of the corruption threats. This reduces the effectiveness of any threat assessment. These forces are missing opportunities to get the whole workforce involved in the fight against corruption.

Area for improvement 5

Workforce awareness of corruption-related threats is an area for improvement. Forces should routinely brief police officers and staff on the pertinent and sanitised content of their annual counter-corruption strategic threat assessment.

Developing corruption-related intelligence

We examined forces' intelligence development processes. In most forces, corruption-related intelligence reports were recorded within the CCU on a secure, stand-alone computer system. With one exception, we found these systems fit for purpose. In most of the 616 cases we examined, the intelligence was developed effectively. But in 53 cases, forces didn't do everything we thought they should: for example, checking for unlawful access to police records.

In most cases where we identified shortcomings, the force had no plan for how the intelligence was to be developed. Where such plans had been prepared, they were generally of good quality. We believe that all corruption-related intelligence should have a development plan prepared by the investigator and overseen by a supervisor.

Capability and capacity to tackle corruption

Resources in CCUs has improved

In our 2019 PEEL spotlight report *Shining a light on betrayal: Abuse of position for a sexual purpose*, we identified that some forces had not allocated enough resources to deal with police corruption. The Police Uplift Programme will, sadly but inevitably, bring with it an expansion in the volume of complaints, misconduct, and incidents of corruption (but we can't predict exact numbers).

Part of the uplift funding was designed to make sure forces have enough funds not only to recruit new officers but also to provide the infrastructure and support needed for them. So we were keen to see whether forces had allocated sufficient resources to CCUs.

Most forces we inspected had increased their counter-corruption resources over the previous two years. In most forces, people working in CCUs reported to us that resources had increased and workloads were manageable.

CCUs should plan to meet the likely increase in demand

Where new IT monitoring systems are being introduced, forces also need to be aware that, if used effectively, these systems will undoubtedly increase demand on CCUs. This will also need resourcing accordingly. One of the forces we visited was about to introduce a new IT monitoring system but hadn't considered how to cope with the additional demand the system would create. That demand will come in two forms: demand for checks to be carried out; and demand for further investigation when checks reveal potential corruption.

The investigations we reviewed were mostly in response to intelligence that had been received. We have recommended that forces become more proactive in seeking corruption-related intelligence. If forces do this it is likely that the current level of resources in CCUs will be insufficient to deal with this additional demand. All forces should review the level of resources in their CCUs to make sure proactive intelligence collection can take place. This is likely to lead to an increase in investigations.

A good level of capability exists within the CCUs

We found that force CCUs had officers and staff from a range of policing backgrounds, with most officers having detective experience and accreditation to Professionalising Investigations Programme level 2. Most units had prepared a skills matrix and used it to make sure that the right training is provided. Most forces also provide some in-house training in counter-corruption.

The College of Policing provides two national training courses for staff involved in counter-corruption investigations. The counter-corruption bronze course is often attended by sergeants, and the counter-corruption silver course by officers of inspector rank and above. We found staff in each CCU we inspected who had either received this training or were expecting to attend a course.

CCUs mostly carry out effective investigations

During our intelligence file review, we found that in most cases CCUs carried out their investigations well and in a timely way. But we identified 53 cases (out of 616) where there were missed opportunities, which could have developed the intelligence further.

Where investigations were not as thorough, we found that there was no investigation plan to identify all the relevant inquiries that were needed. The absence of any effective supervision was also a common issue.

CCU staff didn't always consider that the intelligence may well be an indicator of a wider pattern of behaviour. This lack of consideration means that CCU staff sometimes miss opportunities to identify further intelligence or even criminal behaviour, potentially involving members of the public.

IT auditing, speaking to potential witnesses, reviewing BWV, reviewing previously attended incidents and considering any misconduct history would all increase the potential to develop corruption-related intelligence. Expanding investigative limits in this way should be built into investigation plans.

Recommendation 40

By 30 April 2023, chief constables should make sure their counter-corruption units:

- produce and follow an investigation plan, endorsed by a supervisor, for all counter-corruption investigations; and
- check all reasonable lines of inquiry in the investigation plan have been concluded before finalising the investigation.

10. Counter-corruption policies

Most forces follow Counter-Corruption (Prevention) APP guidance in relation to their counter-corruption policies

The Counter-Corruption (Prevention) APP states that the risks to operational security and organisational integrity increase significantly when police officers and staff experience personal difficulties. Such difficulties may include financial hardship and problems at work or at home, which can affect their judgment and make them more susceptible to corruption.

There are significant corruption threats to forces if inappropriate relationships are not identified when people enter policing, or they develop them during their service. Officers and staff can become susceptible to the influence of numerous potential corruptors. These can come from a range of groups such as criminals, family members and other people with an interest in accessing police information, such as private investigators. Officers and staff may act corruptly for various reasons, such as financial gain, misplaced loyalty, or because they have been blackmailed.

Clear and concise corruption prevention policies help to guard against corrupt activity, but cannot guarantee to prevent corruption, or in themselves stop corrupt practice. They set limits for how the police officers and staff should behave. Such policies should clearly state what is expected of the individual and what actions they should take to protect themselves and the organisation from corruption.

The Counter-Corruption (Prevention) APP sets out what policies forces should have and gives guidance on their content.

We examined forces' policies in respect of:

- **gifts and hospitality** (covering the circumstances in which police officers and staff should accept or reject offers of gifts and/or hospitality);
- **business interests** (covering when the force should allow or deny officers and staff the opportunity to hold other jobs and how the force will manage the risks that arise when they are allowed to hold them); and
- **notifiable associations** (covering how the force should manage the risks associated with officers and staff who may associate with, for example, criminals, private investigators, or members of extremist groups and require the disclosure by officers and staff of such associations).

In our inspection, we found that in most forces, the content of these three policies reflected the APP guidance.

(The APP also specifies other counter-corruption related policies: service confidence; debt management; social networking; and media; but we didn't examine these in this inspection.)

Gifts and hospitality

It is very important that forces have clear and robust policies in respect of how offers of gifts and hospitality are dealt with. It is not sufficient to allow individual police officers and staff to decide for themselves what is and isn't acceptable to receive.

In many organisations, customers may choose to adopt a perfectly acceptable practice and reward good service with a gift or tip. In policing the situation is very different. If officers and staff accept gifts or hospitality in the course of their duties, their impartiality may be justifiably called into question, or even compromised.

The Counter-Corruption (Prevention) APP advises that forces should maintain a central record of all gifts offered, accepted, or refused. Where a gift is accepted, a senior officer, normally the operational commander or departmental head, should decide what happens to the item in question.

The Counter-Corruption (Prevention) APP does not comment on the appropriateness of accepting alcohol or cash. In March 2022, in our DMIP report, we recommended that the College of Policing change the APP to make clear that gifts of cash should never be accepted.

Most forces manage gifts and hospitality effectively

All forces had a process for officers and staff to follow if they were offered a gift or hospitality. These processes all involved reporting via an online form that the professional standards department (PSD) retains in a register.

We examined these registers and found most of them to be well-maintained. Supervisors had considered the suitability of the gift or hospitality and recorded their decisions in compliance with force policy.

When we spoke to staff, they stated that they were aware of the policy relating to gifts and hospitality or knew how to access it using the force intranet. Many stated that if they were offered a gift they would speak to a supervisor for advice.

But in one force, we found that there were few if any entries on the registers. This suggests that the policy in respect of gifts and hospitality was not always being complied with.

Business interests

Police forces have a responsibility to avoid any conflict between the business interests of their officers and staff and their roles within policing. Regulations 6 to 9 of the Police Regulations 2003 provide the legislation relating to business interests as they apply to police officers and guidance is available to forces through the Counter-Corruption (Prevention) APP.

For police officers and their relatives, business interests can be summarised as:

- holding any office or employment for hire or gain (otherwise than as a member of the force) or carrying on any business; or
- involvement in the sale of alcohol, betting and gaming or places of entertainment in the area of the police force in question.

Where an officer or their relative has a business interest, the officer is required by law to declare it. A senior officer should then decide whether it is compatible with the officer's role. Where a force considers the business interest incompatible, the request can be refused. If the individual is determined to pursue the interest, they may not be allowed to continue to be a police officer.

Where an interest gives a cause for concern, but a force does not wish to refuse the application, it may be managed through restrictions or conditions – for example, a condition covering where the business may be carried out. It is not always possible to manage business interests this way.

For police staff members, their contracts of employment usually include similar provisions relating to business interests.

The Counter-Corruption (Prevention) APP states that business interest policies should specify:

- the requirement for authorisation;
- factors to be considered before approval;
- the application process;
- the monitoring and review process; and
- how to manage subsequent appeals.

Business interest policies were compliant with the Counter-Corruption (Prevention) APP guidance

We found in each force we inspected that responsibility for the oversight of the business interest process and subsequent authorisation was held by the PSD.

During our inspection, we spoke to staff in focus groups. Most stated that they understood their responsibilities in relation to business interests and knew how to find the relevant policy on the force intranet. Some forces require supervisors to discuss counter-corruption policies, including business interests, as part of a performance review. This supports the understanding that police officers and staff have of counter-corruption policies.

Each PSD maintained a central register of business interest applications. We found most of these registers to be well maintained and that decisions to accept a business interest complied with the forces' policies. We found that, in most cases, an authorisation for a business interest was valid for 12 months before being subject to a review and renewal.

There are weaknesses in the monitoring of compliance with business interests policies

We found very few records relating to applications that had been refused.
We identified that not all forces routinely make supervisors aware of any conditions imposed on any business interests their staff may have. This restricts supervisors' ability to monitor compliance with the conditions.

Most forces didn't have a process to check whether, despite a business interest application being refused, an officer or staff member had pursued it anyway. We also found that in some forces, the annual review of business interests was not completed.

Recommendation 41

By 30 April 2023, chief constables should strengthen their business interest monitoring procedures to make sure that:

- records are managed in accordance with policy and include cases where authorisation has been refused;
- the force actively monitors compliance with conditions that are attached to the approval, or where the application is refused;
- regular reviews of each approval are carried out; and
- all supervisors are properly briefed about business interests held by members of their teams.

Notifiable associations

The purpose of this policy is to protect police officers, staff and the force from people who may, or may be perceived to, compromise their integrity. The Counter-Corruption (Prevention) APP advises that officers and staff should declare specific associations with people who, for instance:

- may have unspent criminal convictions;
- are under investigation or awaiting trial;
- are the subject of criminal intelligence; or
- are a potential corruptor.

In this context, 'association' is any relationship or connection with another individual. This can include via social media. The types of people the Counter-Corruption (Prevention) APP suggests that could be potential corruptors includes family, friends, partners, private investigators, and members of extremist groups. Following a number of historic high-profile instances of corrupt police officers passing information to the media, journalists are also included as a notifiable association.

In cases where the association presents a significant risk, conditions and restrictions may be applied as part of a risk management plan. These should be subject to regular review and monitoring.

Most notifiable association policies were compliant with Counter-Corruption (Prevention) APP guidance

During the inspection, we examined the policies used by forces relating to notifiable associations and found that in most cases they were compliant with the Counter-Corruption (Prevention) APP. But one force didn't have a notifiable association policy. It informed us that it was about to introduce one.

In those forces that had such a policy, PSDs were responsible for managing the policies and maintaining records of all notifiable associations that had been declared.

Most forces recorded notifiable associations in a stand-alone database, and the CCU assessed the level of risk posed by the association. Most forces had access to all relevant information that would allow the appropriate level of risk to be identified. In forces that didn't maintain such a database to manage notifiable associations, we found that, on occasion, cases weren't being reviewed at a later date to check for any changes in the circumstances.

Monitoring compliance with this policy is another weakness for forces

Some forces didn't routinely check for compliance with the conditions set by the CCU. In these forces, checks are only made when the CCU receives further intelligence regarding the individual concerned. This is not an effective way to manage any risks that have been identified and mitigated by applying appropriate conditions.

As stated above, the Counter-Corruption (Prevention) APP lists the type of associations that should be notified. We found that some forces' policies didn't include a requirement to notify associations with all those listed in the APP. Omitting these types of association from its policy reduces the ability of a force to manage the risks they pose.

We identified that not all forces routinely make supervisors aware of members of their team with a notifiable association and any necessary conditions related to this. Forces that do not brief supervisors on known risks miss opportunities to manage these risks.

Recommendation 42

By 30 April 2023, chief constables should strengthen their notifiable association procedures to make sure that:

- they are compliant with the Counter-Corruption (Prevention) Authorised Professional Practice (APP) and that the obligation to disclose all associations listed in the APP is explicit;
- there is an effective monitoring process to make sure that any conditions imposed are being complied with; and
- all supervisors are correctly briefed on the notifiable associations declared by members of their teams.

Awareness of counter-corruption policies is improving

Effective communication is essential if police officers and staff are to understand what is required of them. They need to understand why the policy exists, why it is important and how it is going to affect them. Policies should be clear, concise, and easy to understand and find. Training on them should be given if necessary.

The knowledge and understanding of the counter-corruption policies in the forces we inspected was mostly good. Most people told us that, even if they didn't have detailed knowledge of the actual policy, they knew how to find it on the intranet and had confidence that their supervisors could give them advice if required.

But in every force, some officers and staff told us they had not received any guidance or communication in relation to the policies. In some forces, this gap had already been recognised and additional resources were being used to make sure that the communication of counter-corruption policies was more effective. This involved officers being used as 'prevent' officers with specific responsibilities to improve the understanding of such policies and other risk areas. This was achieved by giving training and briefings to police officers and staff throughout the force.

All forces should introduce annual integrity reviews

Some forces have introduced an annual integrity review during which supervisors discuss corruption policies and other risks such as abuse of position for a sexual purpose with members of their team. In these reviews, supervisors ask if there have been any changes to an individual's personal circumstances. They also check for any changes to recorded business interests or notifiable associations.

Integrity reviews can play an important role in reinforcing and maintaining the standards of the organisation. For them to do so, there should be a robust method of making sure the reviews are completed for all officers and staff. We found that some forces had chosen to do this at the time of an individual's annual performance and development review. But not all forces insist on a performance and development review for all personnel.

Recommendation 43

By 30 April 2023, chief constables should make sure that a robust process is in place for completing annual integrity reviews for all officers and staff.

Annex A: Vetting checks

Minimum checks

Recruitment vetting (RV): police officer, police staff, special constables

Checks to be carried out on applicant, partner, all family (aged ten years old and above), associates and co-residents:

- Police National Computer (PNC);
- all force databases (including non-conviction databases);
- Counter Terrorism Unit; and
- Police National Database (PND) and other force checks.

Checks to be carried out on applicant only:

- record management system check;
- crime report allegations;
- voters' records;
- check of vetting database;
- credit reference check and consideration of financial position;
- open-source enquiries (for example, search engines and social networking sites);
- professional standards check where necessary;
- Ministry of Defence (MoD) checks where relevant;
- Criminal Records Office (ACRO) check where appropriate; and
- Counter Terrorist Check (CTC) may be applied where appropriate.

Management vetting (MV): individuals identified as working in a post assessed as meeting the criteria for MV

Checks to be carried out on applicant, partner, all family (aged ten years old and above), associates and co-residents:

- PNC;
- local intelligence checks;
- PND and other force checks;
- all force databases (including non-conviction databases); and
- Counter Terrorism Unit.

Checks to be carried out on applicant only:

- voters' records;
- checking of vetting database;
- MoD checks where relevant;
- professional standards checks;
- personal finances (including financial questionnaire, force credit reference check and assessment of information returned);
- business interest and secondary employment check (where relevant);
- liaison with occupational health (where relevant);
- open-source enquiries (for example, search engines and social networking sites);
- enquiries relating to vulnerability to pressure or inducements (including the indiscriminate use of alcohol or drugs and/or gambling), where relevant;
- appraisals from current and/or former supervisors to cover a minimum 12-month period (where applicants are existing staff);
- interviews with current and former supervisors at the discretion of the force vetting manager (FVM);
- interviews with the person subjected to the vetting procedure at the discretion of the FVM;
- line manager endorsement (reference);
- aftercare must be carried out for MV clearances;
- ACRO check where appropriate; and
- Security Check (SC) and Developed Vetting (DV) may be applied where appropriate.

www.justiceinspectorates.gov.uk/hmicfrs