

**UNDER EMBARGO UNTIL 00.01 ON THURSDAY 17 NOVEMBER 2022**



# **A report into the effectiveness of vetting and counter-corruption arrangements in Kent Police**

**UNDER EMBARGO**

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

**UNDER EMBARGO**

# Contents

<b>About us</b>	<b>i</b>
<b>1. Introduction</b>	<b>1</b>
<b>2. How effectively does the force vet its officers and staff?</b>	<b>2</b>
<b>3. How effectively does the force protect the information and data it holds?</b>	<b>4</b>
<b>4. How well does the force tackle potential corruption?</b>	<b>5</b>

---

# 1. Introduction

## **Vetting, IT monitoring and counter-corruption: Adequate**

In September 2021, HMICFRS changed the way it reports on how effectively forces manage vetting and counter-corruption.

Previously, we inspected these areas as part of our [police effectiveness, efficiency and legitimacy \(PEEL\)](#) programme and provided our findings in the inspection report.

The new arrangements mean we will inspect each force separately to PEEL, although we will continue to use the same methods and produce a report containing our findings, graded judgments and any areas for improvement or causes of concern. The report will be accessible via a web link from the most recent force PEEL report.

Between 31 January and 11 February, we inspected Kent Police to examine the effectiveness of its vetting, IT monitoring and counter-corruption. We briefed senior personnel in the force at the end of the inspection.

This report sets out our findings. It includes areas for improvement identified at the time of the inspection, which we recognise the force may have already addressed.

## 2. How effectively does the force vet its officers and staff?

The [force vetting unit \(FVU\)](#) uses a vetting management IT system. It sends out reminders six months before expiry dates to try to ensure it periodically renews all vetting in line with the [Authorised Professional Practice](#) on vetting. But we found the process isn't working effectively due to delays in the workforce response. As a result, the FVU has introduced a new process, escalating these cases to the [professional standards department \(PSD\)](#). At the time of our inspection, it was too early to say if this approach had improved the process.

The force had produced a recruitment plan for the year ahead, but it hadn't identified how the FVU would meet this demand. At the time of our inspection, the force was prioritising recruit vetting at the expense of routine vetting. The force told us there were 36 cases waiting to be processed, and that the FVU's workload wasn't manageable.

The force has a list of [designated posts](#) that need enhanced [management vetting](#). But it doesn't have an effective system to identify the right level of vetting for officers and staff in these posts. In October 2021, the force reviewed those posts, establishing that there were 273 roles occupied by 991 postholders. The FVU couldn't accurately say who the current postholders were or whether they had the right level of vetting.

We found the force had allowed 58 people to take up a designated post without the enhanced vetting being completed. Some had been in their post for many months. In some cases, the FVU hadn't decided whether to grant clearance for applicants where the vetting process had revealed adverse information. This is a risk to the force as potentially unsuitable individuals held sensitive posts without the required enhanced vetting.

The FVU gives monthly data to the PSD senior leadership team and human resources about vetting refusals for applicants with protected characteristics. But we saw no evidence of the force analysing potential disproportionality. For example, it doesn't analyse the proportion of rejections for applicants with a particular protected characteristic compared to the proportion of rejections for a control group without that protected characteristic. As a result, the force has no way of understanding the reasons for any disproportionality, so it isn't taking any action to address it. We have identified this as an area for improvement.

## UNDER EMBARGO

In our 2019 PEEL spotlight report [\*Shining a light on betrayal: Abuse of position for a sexual purpose\*](#) we made a national recommendation, stating:

“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 appropriate 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.”

While the force had previously shown some progress in meeting this, we found it still needs to improve the management of its vetting. As a result, we have identified this as an area for improvement.

### Area for improvement

- The force should improve the way it manages the vetting of its workforce to make sure all personnel have valid vetting clearance for their role.
- The force should introduce a system to monitor and respond to disproportionality in its vetting decisions.

### 3. How effectively does the force protect the information and data it holds?

The force uses IT monitoring software to effectively monitor systems across all its handheld, mobile and desktop devices. It introduced the system in 2018.

The force also effectively uses software to monitor and analyse force phone-billing data. In our case file review, we found numerous examples of people in the counter-corruption unit (CCU) using the software well to develop intelligence. And in the sexual misconduct files, we found five cases in which the force proactively used its IT monitoring capability.

The force recognises the risk associated with using [encrypted apps](#) on its force devices, so it doesn't allow this, other than for a very small number of specialist groups (for example, wildlife crime). The force subjects these applications to a rigorous authorisation process and ongoing monitoring. It has a clear policy and guidance on the use of social media and has communicated these to the workforce.

## 4. How well does the force tackle potential corruption?

The force has a current and fit-for-purpose counter-corruption [strategic threat assessment \(STA\)](#). We found the STA, published in November 2021, was a comprehensive review and analysis of the counter-corruption threats the force faces.

The force uses the nationally supported template that sets out the CCU's priorities for the [control strategy](#). There were [4Ps](#) (pursue, prepare, protect and prevent) action plans for each of the respective control strategy priorities. Evidence from our case file review clearly shows the force deliberately focuses intelligence development and investigative resources on these priority areas.

At the time of our inspection, the force had recently added two investigation staff members to the CCU, making a total of five. The force considered this sufficient to meet demand.

We found the force correctly categorises corruption intelligence in line with the Authorised Professional Practice on counter-corruption (intelligence) and its agreed corruption categories.

The CCU collects corruption intelligence from a range of sources. The force has an effective and well-used confidential reporting process via email and telephone, and the workforce can overtly report concerns directly to the PSD. In our case file review, we found evidence of the force proactively collecting intelligence, particularly about sexual misconduct.

We found the force uses a wide range of investigative techniques to collect and develop corruption intelligence, and it makes good use of IT monitoring. In our case file review, members of the CCU presented three specific sensitive investigations in which they had used covert tactics effectively. In most cases, the CCU responds effectively to corruption intelligence. But we found a small number of cases in which it had missed investigative opportunities. We gave feedback about this to the force.

We found that the force had taken steps to raise awareness in the workforce about [abuse of position for a sexual purpose](#). Members of the workforce told us they had a good understanding of this type of corruption. They have received training and messaging over the past few years, including NCALT (now [College Learn](#)) e-learning.



## **UNDER EMBARGO**

At the time of our inspection, the force had identified some agencies that support vulnerable people and had made a presentation to share with them. This highlights the work of the CCU and gives them a point of contact for future referrals. But it was unclear how far the force had taken this with the relevant agencies. During our case file review, we found no evidence that links established with those agencies had resulted in abuse of position for a sexual purpose investigations. The force should make sure it progresses and maintains these links.

November 2022 | © HMICFRS 2022

[www.justiceinspectorates.gov.uk/hmicfrs](http://www.justiceinspectorates.gov.uk/hmicfrs)