London Borough of Hammersmith & Fulham

Social Inclusion and Community Safety Policy and Accountability Committee

Agenda

Wednesday 24 July 2024 at 7.00 pm

145 King Street (Ground Floor), Hammersmith, W6 9XY

Watch the meeting live: youtube.com/hammersmithandfulham

MEMBERSHIP

Administration	Opposition
Councillor Nikos Souslous (Chair) Councillor Omid Miri Councillor Sally Taylor Councillor Lucy Richardson	Councillor Andrew Dinsmore

CONTACT OFFICER: Debbie Yau
Committee Coordinator
Finance and Corporate Services
E-mail: Debbie.Yau@lbhf.gov.uk
Web: www.lbhf.gov.uk/committees

This meeting is open to the public and press. The building has disabled access.

Members of the public are welcome to attend but spaces are limited. If you would like to attend, please contact: Debbie.Yau@lbhf.gov.uk

Date Issued: 16 July 2024
Date Updated: 17 July 2024

London Borough of Hammersmith & Fulham

Social Inclusion and Community Safety Policy and Accountability Committee

Agenda

24 July 2024

Item		Pages
1.	**APOLOGIES FOR ABSENCE**	
2.	**DECLARATIONS OF INTEREST** If a Councillor has a disclosable pecuniary interest in a particular item, whether or not it is entered in the Authority's register of interests, or any other significant interest which they consider should be declared in the public interest, they should declare the existence and, unless it is a sensitive interest as defined in the Member Code of Conduct, the nature of the interest at the commencement of the consideration of that item or as soon as it becomes apparent. At meetings where members of the public are allowed to be in attendance and speak, any Councillor with a disclosable pecuniary interest or other significant interest may also make representations, give evidence or answer questions about the matter. The Councillor must then withdraw immediately from the meeting before the matter is discussed and any vote taken. Where Members of the public are not allowed to be in attendance and speak, then the Councillor with a disclosable pecuniary interest should withdraw from the meeting whilst the matter is under consideration. Councillors who have declared other significant interests should also withdraw from the meeting if they consider their continued participation in the matter would not be reasonable in the circumstances and may give rise to a perception of a conflict of interest. Councillors are not obliged to withdraw from the meeting where a dispensation to that effect has been obtained from the Standards Committee.	
3.	**MINUTES OF THE PREVIOUS MEETING** To approve the minutes of the previous meeting as an accurate record and note any outstanding actions.	4 - 8
4.	**CCTV SERVICE UPDATE AND THE ANNUAL REPORT ON THE COUNCILS USE OF INVESTIGATORY POWERS** This report updates the Committee on the work and progress of the Closed-Circuit Television (CCTV) service, and details on the work and progress of the borough's £5.4m capital investment programme for CCTV with a view to completing the work at the end of 2025/26.	9 - 80

It also provides the Committee with the opportunity to scrutinise the Council's conduct in relation to directed surveillance, covert human intelligence sources (CHIS) in accordance with the Regulation of Investigatory Powers Act (RIPA) and Council policy.

5. ANNUAL PERFORMANCE REPORT FOR THE LAW ENFORCEMENT TEAM 81 - 100

This report provides the Committee with an update following the previous meeting focusing on work of the Law Enforcement Team between December 2023 and May 2024.

6. DATE OF FUTURE MEETINGS

To note the following dates of future meetings:

- 20 Nov 2024
- 4 Feb 2025
- 30 Apr 2025

London Borough of Hammersmith & Fulham

Social Inclusion and Community Safety Policy and Accountability Committee

Minutes

Wednesday 24 April 2024

PRESENT

Committee members: Councillors Nikos Souslous (Chair), Trey Campbell-Simon and Andrew Dinsmore

Other Councillors: Councillor Rebecca Harvey (Cabinet Member for Social Inclusion and Community Safety)

Officers:
Matthew Hooper (Director of Public Protection)
Neil Thurlow (Assistant Director of Community Safety, Resilience and CCTV)
Aysha Esakji (Prevent Coordinator)
Debbie Yau (Committee Coordinator)

1. APOLOGIES FOR ABSENCE

Apologies for absence were received from Councillors Sally Taylor and Omid Miri.

2. DECLARATIONS OF INTEREST

There were no declarations of interest.

3. MINUTES OF THE PREVIOUS MEETING

The minutes of the meeting held on 7 February 2024 were agreed as an accurate record.

4. UPDATE REPORT FOR THE PREVENT TEAM

Neil Thurlow (Assistant Director of Community Safety, Resilience and CCTV) briefed members that the Prevent Team worked across both the London Borough of Hammersmith and Fulham (LBHF) and the Royal Borough of Kensington and Chelsea (RBKC) as one area. Since its inception in 2011, the Prevent Team had built up trust and confidence with the local communities. The report had set out the current threat and risk of LBHF based on the counter-terrorism local profile including those associated with the Gaza War. Although the Prevent Team had faced Home Office's funding cuts, both LBHF and RBKC had agreed to jointly fund the Prevent service as it was the Local Authority's responsibility in discharging the statutory Prevent Duty. While the Team had engaged in sensitive and confidential matters, it had managed and mitigated the risks well through both Prevent Advisory Group (PAG) and Faith Forum.

Aysha Esakji (Prevent Coordinator) highlighted the lasting and trusting relationship with the community partners built over the last decade. When incidents like the Gaza War happened, some of the partners had approached the Prevent Team before any emerging issues were escalated or hijacked by harmful influences.

The Chair was concerned about the Home Office's criteria in assessing the risks across the London boroughs given that LBHF had historically seen significant Daesh extremist activity (page 20). Aysha Esakji advised that in undertaking assessment, the Home Office had a prioritisation process that would assess the threat and risk of each area and list them on a lead table. It had obtained data from various sources and assessed LBHF and RBKC separately. As such, the overall risk for the area was listed towards the bottom of the lead table.

On the Chair's enquiry about the seven London boroughs that would continue to receive fundings, Aysha Esakji noted that from April 2024, the Home Office had cut the Prevent funding from some of the London boroughs covering 11 areas. The remaining boroughs would also cease to receive funding from April 2025 except seven boroughs which were deemed to have the highest threat and risk currently. They were Westminster, Tower Hamlet, Enfield, Brent, Haringey, Redbridge and Newham. She added that the Home Office would review the situation in two years' time to determine which boroughs had higher threat and risk for future fundings.

The Chair enquired whether there were any changes to the Prevent service after it was funded by the local authorities. Aysha Esakji remarked that the work of Prevent service was guided by the counter-terrorism local profile drawn up by the Police every 18 months. The profile highlighted the current threat and risk locally and in West London. On funding matched by the Government, Neil Thurlow said that the Prevent service was fully funded by the Home Office for over a decade. However, the service had seen significant cuts over this time concluding in April 2023, when service funding was reduced by 50% and notice was given to the Council that funding would completely cease from the end of financial year 2023/24. He also noted that the Council was also required to undertake transitional work to secure long-term funding for growth.

Councillor Andrew Dinsmore asked if the Council had more control now over the locally funded service. Matthew Hooper (Director of Public Realm) said while there was some degree of autonomy for the service now when being funded locally, the local authority still had a statutory Prevent Duty which was assessed against a specific performance benchmark framework set out in the report (page 16).

The Chair further asked if the Prevent service was equipped to deal with extreme far-right terrorism which, in his opinion, had become the biggest threat to the British communities. Aysha Esakji noted that the Prevent service dealt with far-right as well as Daesh extremism. Neil Thurlow added that the far-right extremists would use world events to justify their actions. For example, some far-right followers had used the opportunity of the Gaza War to divide among Muslim and Jewish communities. In response, leaders of the Faith Forum had stood united and sent a letter to the Prime Minister and Home Secretary before Christmas to raise their concerns and seek answers around the Gaza War. Neil noted the Faith Forum was disappointed for not receiving a response or an acknowledgement so far.

Members noted that LBHF scored 5 which showed the quality and depth of service delivery against the Prevent Duty benchmark on engagement with a range of communities and civil society groups. The Chair sought further elaboration. In response, Aysha Esakji highlighted the work of the PAG which was set up in December 2011. As PAG members who knew their communities better would share information on the current threat and risk locally at the monthly meetings, the Prevent Team could work with them to co-produce Prevent strategies to keep the community safe. Together with the leaders in the Faith Forum, the PAG also helped in co-delivering the service with the Team like preventing individuals from travelling out to the conflict zones or diverting individuals away from the path of radicalisation by providing the support they needed.

Neil Thurlow appreciated the consistent approach of Aysha Esakji in listening to the concerns raised at the meetings and providing support to individuals in various aspects from housing, benefits to employment and education. Through the journey, Aysha had gone through difficult conversations concerning accountability before becoming their trusted partner. Aysha elaborated that in addressing concerns about the impact of policy changes at the national level, the Prevent Team had held community question times to enable direct conversations between Home Office officials and the communities. She said that the two sides had a better understanding of each other after frank and honest discussions.

On Prevent referrals, Neil Thurlow said that it was nearly impossible for community groups and family members to make referrals and most identified risks came from the Police and schools. In response to Councillor Dinsmore's concern, Aysha Esakji noted that a lot of far-right referrals had come from schools. A couple of youth groups had also reflected concerns about some young people attending had expressed some extreme idea. She gave a detailed account on how to deal with individual cases which involved the school, Police, Channel Panel comprising health and education colleagues and faith leaders who might help prevent after having a one-to-one intervention. In addition, the Safeguarding Lead would collate information about the individuals received from various departments and pass them to the Police for their further actions.

In reply to Councillor Dinsmore's further questions, Asyha Esakji said that as part of their due diligence efforts, the Home Office had provided a list of intervention providers covering all types of extremism. The Prevent Team would match the identified individual to the best intervention provider who might have faced the same situation previously and hence could share their own experience. Asyha also noted that in general, the Team worked in the prevent space where no crime had been committed. However, the Police had found in the previous year some young people aged between 10 and 15 years old had been in the pursue space. As the age of 10 and 11 were too young, the Prevent Team was still giving these young people support with a view to preventing things from getting worse.

Regarding the Prevent Team's work with other boroughs as raised by the Chair, Aysha Esakji advised the Committee that Prevent Coordinators of the London Prevent Network, particularly those from the West London cohort, would meet and share information monthly to see what the common concerns were and if there were any similar issues.

Responding to the Chair's concern about the collaboration of the Prevent Team with other departments/units, Neil Thurlow highlighted the dynamic working relationship between the Prevent Team and Gangs Unit both of which sat under his oversight via the Community Safety Unit. The officers had all received the WRAP (Workshop to Raise Awareness of Prevent) training. They also worked very closely with the education officer to see who could give the best support to individuals who had been exploited around extremists with a view to preventing violence from happening. Matthew Hooper observed that the ways in which organised groups, be it gangs or alliance on faith issues, sought to exploit and get new people involved were quite similar. It was crucial to identify them at the early stages and put in place the right interventions before it was too late.

As regards public perception of the Prevent Team over time, Neil Thurlow remarked that while Prevent could still be seen as worrying, more people now understood what the Prevent Team was doing and perceived it as a pre-criminal justice space and an early intervention support space. Along with more school teachers and professionals having received the WRAP training, the Prevent Team had gained the trust and confidence of the communities through the PAG meetings and Faith Forum.

Councillor Rebecca Harvey (Cabinet Member for Social Inclusion and Community Safety) remarked that it was very disappointing that the Government had cut the Prevent funding as it was a statutory duty. As the borough had large performance and sport venues, the Council recognised the importance of keeping residents and visitors safe and would continue to fund Prevent. She hoped that the Government would review their decision. Councillor Harvey also gave credits to Aysha's fantastic work in co-ordinating the Prevent service.

Echoing her disappointment, the Chair hoped that the Council might receive advanced notice about funding in future. Neil Thurlow said Aysha had been lobbying colleagues in the Home Office regularly. However, the Government's position was not changing, and the Team had worked to accept that reluctantly.

The Chair expressed appreciation to the work of the Prevent Team.

RESOLVED
That the Committee noted the report.

5. DATE OF FUTURE MEETINGS

The Committee noted the following dates of future meetings:

- 24 Jul 2024
- 20 Nov 2024
- 4 Feb 2025
- 30 Apr 2025

Work Programmes:

- Update on the CCTV Network
- Review of the Regulation of Investigatory Powers Act
- Law Enforcement Team Update
- Hate Crime Strategy
- Violence against women and girls
- Anti-social behaviour

Meeting started: 7.04 pm
Meeting ended: 7.44 pm

Chair .....

Contact officer: Debbie Yau
Committee Co-ordinator
Corporate Services
E-mail: Debbie.Yau@lbhf.gov.uk

LONDON BOROUGH OF HAMMERSMITH & FULHAM

Report to: Social Inclusion and Community Safety PAC

Date: 24 July 2024

Subject: CCTV service update and the Annual Report on the Councils use of Investigatory Powers (RIPA and IPA)

Report author: Neil Thurlow, Director of Public Protection.
Jayne Bacon, Programme Manager for CCTV upgrade
Mohammed Basith, RIPA lead officer.

Responsible Director: Neil Thurlow, Director of Public Protection

---

SUMMARY

This report provides the PAC committee with three updates:

The first, an update on the work and progress of the Closed Circuit Television (CCTV) service.

The second, detail on the work and progress of the boroughs £5.4m capital investment programme for CCTV which is at its midpoint with two years' work completed, we are in year three with a completion at the end of 2025/26

For the purposes of the investment programme the PAC committee are asked to note that locations of key infrastructure cannot be shared due to security considerations. Where we cannot give specific locations the broader town centre area will be referenced.

The third, to provide the committee with the opportunity to scrutinise the council's conduct in relation to directed surveillance, covert human intelligence sources (CHIS) in accordance with the Regulation of Investigatory Powers Act (RIPA) and council policy.

There are no decisions required from this report.

RECOMMENDATIONS.

For the Committee to note and comment on the report

Wards Affected: All

Our Values	Summary of how this report aligns to the

	H&F Values
Building shared prosperity	We are investing in technology to help protect our residents via the capturing of crime and ASB. A safer borough is a more prospective borough
Creating a compassionate council	The safety of our residents is our number one priority. The work of CCTV is intrinsic to that with our work leading to arrests removing offenders from the streets
Doing things with residents, not to them	The service responds to residents needs by looking at concerns, looking at intelligence and tasking operators accordingly. Where residents experience crimes and there are no cameras, we seek to deploy our temporary asset to these areas as often as possible
Being ruthlessly financially efficient	We operate a traded service agreement with two other boroughs increasing efficiencies and value for money within this service area
Taking pride in H&F	We are proud to have the most comprehensive CCTV offer with the most cameras per head of population in the UK
Rising to the challenge of the climate and ecological emergency	Our upgrade programme seeks to minimise landfill waste by re-using and/or re-cycling materials wherever practicable and as we replace equipment, we do so with more energy efficient assets. We embrace new technologies to share data electronically saving the use of DVDs and other items that cannot be recycled or reused

Background Papers Used in Preparing This Report

1. CCTV Capital Investment Strategy, approved on 07/03/22 cabinet.
2. Issue details - CCTV Capital Investment Strategy | London Borough of Hammersmith & Fulham (lbhf.gov.uk)

DETAILED ANALYSIS

CCTV SERVICE UPDATE

Service headlines and performance:

1. The Councils CCTV Service is one of the largest and most substantive systems in the UK. We are proud to have the highest number of cameras per head of population

in the country and, with our upgrade programme now at its midpoint, our previously advertised camera number of circa 1,800 cameras across the borough has increased further to over 2,000 cameras in the public realm and across our housing estates.

2. The service is provided 24/7, 365 and contributes to identifying, reducing, and tackling crime and ASB (Anti-Social Behaviour) alongside supporting our residents, visitors, business community, housing estate tenants alongside internal and external partners through the provision of monitored cameras alongside broader functionality.

3. The purpose of any good control centre is to be at the heart of tackling crime and our stated priorities that we use the CCTV system for are:

- Deter anti-social behaviour.
- Disrupt and prevent street crime.
- Look for illegal waste dumping.
- Observe unlicensed activity in entertainment premises.
- Observe fraudulent behaviour.
- Gather evidence for court proceedings.
- Identify persons wanted by the police.
- Emergency planning.
- Supporting public safety
- Gathering evidence for highway collisions.

4. We benefit from a stable and settled workforce who, through their longevity, commitment and dedication know the boroughs which we serve very well and offer the highest standards in customer service and investigatory skills.

5. The service is hosted, and staff employed by, Hammersmith and Fulham Council with all operators working within our buildings and to our terms and conditions.

6. The service runs a traded offer with two neighbouring boroughs:

- The first is a long-established partnership with Royal Borough Kensington and Chelsea

- The second, launching in summer 2024, with Westminster City Council (WCC).

7. By bringing WCC on board we will be the first Borough Command Unit (BCU) to have all Council cameras monitored through the same control room and we will have greater opportunities to track, deter and investigate criminality across borough boundaries.

8. The work and remits for all three boroughs are principally the same. The times of operation vary slightly with both LBHF and WCC operating 24/7 with RBKC operating 15:00-01:00. All service provision runs 365 days a year.

9. The service structure sees the service lead by Adrian Rutkowski as our CCTV Manager and he is supported by a team of supervisors and officers.

10. The service currently operates on a minimum staffing level of two officers at any time. Minimum staffing levels will increase once the WCC contract comes into effect.

11. The service has much to be proud of. Some of our 2023/24 highlights:

- £1.9m spent on the second year of our upgrade programme (more below).

- Our officers work directly assisted the Met to secure arrests of 535 people.
- Operators captured 4,896 incidents.
- Ten new solar powered cameras have been installed in our parks (Ravenscourt, Hurlingham, Wormholt and Bishop Park alongside Furnivall Gardens)
- 79 deployable cameras were managed allowing for cameras to be installed in areas of need for specific reasons.
- Some 45 businesses within the Hammersmith BID area have direct access into the control room, and vice versa, via the Radio scheme.
- Working in partnership we provide, and receive, direct access to, and from, our football clubs on match days.
- Officers work and support internationally recognised events such as the Notting hill Carnival, the Boat race, Queens Tennis, Hammersmith Apollo etc.
- CCTV operators provide additional help and support to our LET officers ensuring that they are supported and protected when addressing challenging matters.
- Compliments received regularly from Police and others in regard the professionalism of the service.

Future ambitions

12. The ambitions of the service are to constantly evolve and become better.

13. With the upgrade programme at its midpoint, we are entering into an exciting new era where the control room can become multi-disciplinary and add further benefits to others as will be explained below.

14. We are keen to add further functionality and offerings for traded services of the CCTV whether via business, regeneration, commercial or local authority contracts. When our upgrade is complete, we will see and feel real tangible differences for all.

15. The service will also seek to achieve accreditation which would further recognise the work and the standards to which service delivery is achieved.

CCTV UPGRADE PROGRAMME – A MIDPOINT REVIEW

16. In March 2022 the Council announced its £5.4m investment into the CCTV service.

17. This investment, the largest in a generation for CCTV, further evidenced the authority's commitment to investing in, and tackling, crime and ASB.

18. The funding, to run over four financial years (2022/23 through to 2025/26) is designed to improve and grow our CCTV offer alongside improving the services resilience and enhancing the use of new and/emerging technologies to place Hammersmith and Fulham at the forefront of innovation and service delivery.

19. The upgrade has been, and remains, a long and complex project to deliver but we are proud of our achievements and proud to state that the capital work programme is both on track and on budget.

20. This section of the report seeks to highlight key workstreams and achievements to the PAC committee and to the residents of the borough.

How did we understand need, and evidence where works were to take place in a priority order?

21. At the start of the project a comprehensive survey report was undertaken of the entire CCTV assets across the whole borough. This survey focused on the infrastructure - rather than the cameras - as infrastructure and security aspects underpin the service provision and our operational integrity.

22. Our key deliverables for the programme included work to deliver:

- The consolidation of several service platforms (ICT systems) resulting in a single, secure, and fully auditable system.
- Improving security and reliability of the CCTV network
- Improving security and functionality of the ways in which CCTV footage is released to increase efficiency and maximise regular security upgrades.
- Replacing critical fibre routes and wireless links where issues regarding type or functionality have been proven to be substandard.
- Maximising technological advances to maximise wider council benefit.
- Not initially included but being delivered installation of smoke detection to all CCTV equipment areas.

Key progress/success for years 1-2:

23. Working within clear project management frameworks we established a CCTV Board to oversee delivery and to bring the authority, and partners, fully into the workstreams.

24. The main outcomes for years one and two can be summarised as follows:

- Complete replacement of power lines and power supply to the CCTV equipment areas in the Shepherds Bush area
- Completed 50% replacement of power lines and power supply to the CCTV equipment areas within the Hammersmith area.
- The main CCTV equipment room in Shepherds Bush has been fully replaced - old equipment removed and upgraded to our new Genetec equipment.
- All CCTV sites in the North of the borough, which feed into our Shepherds Bush hub, have also been upgraded.
- All main equipment hubs across the borough have smoke and fire suppression systems installed which are appropriate for their environment.
- Sensors for fire and power have been installed within all the main equipment areas and are connected back to the Control room. The technology within the equipment rooms will provide early alert motivation to the control room in case of any issue allowing for a swifter response.
- We have successfully implemented a new way of sharing footage with police. Our “Clearance” system provides secure and fully auditable data sharing and removes the need to excessively store data, burn DVDs, host numerous visits from Police etc ensuring that the service can function more efficiently and that our partners receive footage safely.
- Upgraded and increased CCTV coverage in Shepherds Bush Green area.

25. The above workstreams have already resulted in the equipment being protected from power disruptions, and the new infrastructure offers greater network security.

26. The alerts and links to the control room give us proactive rather than reactive management to ensure protection of the service.

What does year three look like and what is being done?

27. As we enter the third year of our investment programme, we will build on our first two years of programme delivery, and we will complete the following works:

- Commence and complete the upgrade of power works within the Fulham area.
- Complete the remaining 50% of works in the Hammersmith area.
- To have installed at least one of the three core fibres supporting the backbone of the network - this specific aspect is time consuming, complex, and costly as fibres can run for more than a mile in length – with one upwards of three miles - and all must be completed without breaking connectivity and through the digging of trenches to replace ducting within which the fibres sit.
- Reinvest in the LET upgrading the CCTV Van and replacing the Body Warn Cameras
- Rollout upgraded temporary CCTV cameras to continue and enhance our ability to deploy cameras where there is evidenced need to help address crime and ASB.
- Continue upgrading our ICT moving all cameras and functionality from three systems to one single, unitary platform.
- We will continue to upgrade and improve our external security to include new security locks on all main equipment doors, smoke detection to be installed across key equipment areas and CCTV cameras to be installed where the need has been identified to protect our assets.

28. As the work of the service, and the wider benefits of the upgrade programme are realised, over the next 12 months we will also seek to deliver addition benefits to the Council and residents as we:

- Seek to explore further commercialisation opportunities to help further grow CCTV provision.
- Continue to expand and connect the control room with other Council buildings as we enhance the broader benefits – the connection plans are expected to include libraries and possibly community buildings. Alongside this where panic alarms are installed in buildings, we will seek to connect these to the control room for staff and public safety.

What does year four look like and what is being done?

29. With some nine months of the 2024/25 financial year remaining, we know that the work plans for next year can change. However, in the final year of works we expected to:

- Review and enhance current asset records to provide a fully complete, and updated, audit of all new infastructure, technology etc from year four ensuring that the borough has a robust, thorough and accurate document library to provide long lasting support.
- Complete the remaining installations of core fibre routes – likely two routes running over several miles within the borough.
- Install Dash Cam analytics to specific Cameras to fully realise the benefits of Smart technology within our CCTV software suite.

REGULATORY INVESTIGATION POWERS ACT (RIPA) – ANNUAL REPORT

30. This annual report is presented to provide the PAC with an oversight of our work in regard to Regulatory Investigation Powers Act (RIPA).

31. In May 2023, the investigatory powers commissioner's office (IPCO) communicated its intention to conduct an in-person inspection in August 2023.

32. The purpose of the visit was to review the council's use of covert surveillance and to seek updates on what measures had been taken to implement their recommendations from their previous inspection in April 2020.

33. Following the previous inspection in April 2020 the council were informed by the IPCO inspection that *"the council (H&F) has a good level of compliance with the legislation*".

34. This report, and findings, were very welcome. The IPCO inspector made two recommendations for our further evolution in this area. These recommendations were:

- To review the retention period for Police RIPA applications
- To review how LBHF stored submitted RIPA applications.

35. This report notes to PAC that all recommendations following the inspection have been complied as staff sought Police guidance and, following feedback, will only retain RIPA applications for three years as this is in line with current Police procedures.

36. In addition, to ensure compliance with the second recommendation all applications were stored in a secure online file in an electronic format as opposed to paper copies.

37. Our inspection in August 2023 noted that the use of RIPA, and related intelligence work, has been limited. The use of RIPA should be managed accordingly and, with limited use assisted in evidencing the proportional approach taken in the borough.

38. Following the inspection on 14 August 2023, the IPCO inspector provided the outcome of the inspection on the same day. He stated his satisfaction of the Councils ongoing compliance with RIPA 2000 and the Investigatory Powers Act 2016 which the Council had maintained. He also commented that our approach and regulation around the use of powers was of a high standard.

39. Whilst there has been no use of the covert powers available since the previous inspection, the process by all local authorities to appropriately manage covert material, when gathered, remains a focus for IPCOs inspections.

40. The inspector noted that all legacy hard copy covert material had been destroyed, with the use of electronic systems now in place to securely retain covertly obtained material.

41. The inspector also noted the policy decision, taken by the Council, to destroy any such material within three years. As such, all matters noted for improvement during the previous inspection had been attended to.

42. Additionally, the inspector noted the continuing regime of RIPA training was in place as well as a satisfactory oversight regime by the Senior Responsible Officer (SRO).

43. As the country began emerging from the pandemic there have been a small number of requests for surveillance work requested by the Police and National Crime Agency. These have been reviewed and, where appropriate approved, with work undertaken as identified below.

44. All work in this area is governed by three policies which were reviewed and updated in May 2023. These are:

- Policy for Use of Direct Surveillance and Covert Human Intelligence Sources (Regulation of Investigatory Powers Act 2000)
- Policy for Use of Direct Surveillance (without Judicial Approval / "Non-RIPA") (Regulation of Investigatory Powers Act 2000)
- Policy for Accessing Communications Data (Investigatory Powers Act 2016)

45. The council's use of these powers since the last report are detailed below.

Directed surveillance (May 2023 to June 2024)

46. Directed Surveillance refers to covert, but not intrusive, surveillance which is not an immediate response to events.

47. It is undertaken for a specific investigation or operation in a way likely to obtain private information about a person (any information relating to private or family life, interpreted broadly to include relationships with others). It must be necessary for the purpose of preventing or detecting crime or disorder and proportionate to what it seeks to achieve (and must meet the serious crime threshold which attracts a six month or more custodial sentence, except for offences relating to the underage sale of alcohol and tobacco).

48. Our use is captured in the table below.

Department	Authorising Officer	Number of applications	Reason
The Environment: Safer Neighbourhoods and Regulatory Services Division	Strategic Lead for Environmental Health and Regulatory Services	5	Met Police and National Crime Agency (NCA) requested and authorised for use of LBHF CCTV assets to assist Police & NCA led operations.
The Environment: Safer Neighbourhoods and Regulatory Services Division	Strategic Lead for Environmental Health and Regulatory Services	0	N/A

Non-RIPA Surveillance (May 2023 to June 2024)

49. Local authorities have an obligation to address anti-social behaviour (ASB) under the ASB Policing and Crime Act 2014. This work involves investigating day-to-day incidents of crime, nuisance, and disorder as even what is perceived as 'low level' ASB, when targeted and persistent, can have a devastating effect on a victim.

50. Due to the above it may be necessary for Council Officers to conduct intelligence work to identify and confirm patterns of behaviour and/or which may lead to the identification of an individual(s) that, at the time of reporting, are unknown. Such investigations cannot be authorised by RIPA as they do not meet the legal threshold.

51. The council has a policy for the Use of Direct Surveillance without Judicial Approval / "Non-RIPA" which sets out the circumstances when officers may use surveillance techniques where the crime threshold is not met.

52. There were no applications for the last year as can be seen below:

Department	Authorising Officer	Number of applications	Reason
The Environment: Safer Neighbourhoods and Regulatory Services Division	Strategic Lead for Environmental Health and Regulatory Services	0	N/A

Communications Data (May 2023 to June 2024)

53. Under the Investigatory Powers Act (2016), local authorities can access certain communications data from Communications Service Providers for the purpose of preventing or detecting crime or preventing disorder. Independent, external authorisation must still be given before communications data can be obtained.

54. Communications data is defined as the 'who', 'when', 'where' and 'how' of communication but not it's content (i.e., it is not the interception of communications).

55. The use of communications data is as follows:

	Authorising Officer	Number of applications	Reason
Finance: Corporate Anti-Fraud Service	Head of Fraud	4	Investigations of tenancy fraud, checking the subscriber and location data of mobile phones.
The Environment: Safer Neighbourhoods and Regulatory Services Division	Strategic Lead for Environmental Health and Regulatory Services	1	Investigations of scam builders for fraud offences

56. Each of these powers is contained as appendices in case PAC members wish to read the legislation within which RIPA is managed:

- Policy for Use of Direct Surveillance and Covert Human Intelligence Sources (Regulation of Investigatory Powers Act 2000) (**Appendix A**)
- Policy for Use of Direct Surveillance (without Judicial Approval / "Non-RIPA") (Regulation of Investigatory Powers Act 2000) (**Appendix B**)

- Policy for Accessing Communications Data (Investigatory Powers Act 2016) (**Appendix C**)

57. There have been recent amendments to the Regulation of Investigatory Powers Act 2000 (RIPA 2000) that all staff need to be aware of. These changes are crucial for us to maintain compliance and ensure the proper handling of investigatory powers.

58. Data Retention and Investigatory Powers Act 2014 (DRIPA 2014):

59. In July 2014, the government passed "emergency" amendments to RIPA via DRIPA 2014, extending RIPA to cover overseas communication providers.

60. Investigatory Powers Act 2016:

61. The Investigatory Powers Act 2016 introduced significant modifications to RIPA, including the replacement of oversight bodies by the Investigatory Powers Commissioner and the introduction of new statutory error reporting requirements.

Error Reporting Requirements:

62. The new statutory error reporting requirements for RIPA were introduced as part of the Investigatory Powers Act 2016. Here are the key points you need to be aware of regarding error reporting:

- Public authorities involved in covert techniques are now required to have processes in place to identify and report errors promptly.
- These processes cover various types of errors, including procedural errors, technical errors, and errors related to the handling of information obtained through covert techniques.
- Examples of errors might include unauthorised surveillance, mishandling of data, or breaches of privacy.
- When an error occurs, the Council must follow established procedures to report it, aiming to maintain transparency, accountability, and compliance with legal safeguards.
- These requirements are designed to enhance oversight and prevent misuse of investigatory powers.

63. Since the new statutory error reporting requirement came in there have been no breaches to report.

64. Our management are regularly trained in RIPA and the requirements of it as referenced earlier in this report. These regular reviews and training ensure that processes are in place, correctly prepared and readied in case needed in the future.

LIST OF APPENDICES

Appendix A - Policy for Use of Direct Surveillance and Covert Human Intelligence Sources (Regulation of Investigatory Powers Act 2000)

Appendix B - Policy for Use of Direct Surveillance (without Judicial Approval / "Non-RIPA") (Regulation of Investigatory Powers Act 2000)

Appendix C - Policy for Accessing Communications Data (Investigatory Powers Act 2016)

Appendix A

London Borough of Hammersmith & Fulham

Regulation of Investigatory Powers Act 2000

Policy for Use of Direct Surveillance and Covert Human Intelligence Sources

June 2015
Revised May 2016
2nd Revision November 2017
3rd Revision November 2019
4th Revision June 2020
5th Revision July 2023

CONTENTS

1. INTRODUCTION

1.1. The Regulation of Investigatory Powers Act 2000 (RIPA) provides a statutory framework for police and public authorities to use surveillance data, where necessary and proportionate, for the purpose of preventing or detecting crime. RIPA regulates the use of these powers in a manner that is compatible with the Human Rights Act.

1.2. Officers of the London Borough of Hammersmith & Fulham who want to undertake directed surveillance must do so in accordance with this policy.

1.3. Whilst RIPA itself provides no specific sanction where an activity occurs which should otherwise have been authorised, any evidence thereby obtained may be inadmissible in court. The activity may also be unlawful under the Human Rights Act and may result in an investigation by the Ombudsman and/or the Investigatory Powers Tribunal.

1.4. This is a sovereign policy and where the term "the Council" is used it will apply to the London Borough of Hammersmith & Fulham.

1.5. This policy must be read in conjunction with current Home Office guidance issued in 2018.

2. DIRECT SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES

2.1. Part II of Chapter II RIPA deals with Direct Surveillance and Covert Human Intelligence Sources. It covers intrusive surveillance, directed surveillance and use and conduct of Covert Human Intelligence Sources (known as "CHIS") who are more recognisable as agents, informants or undercover officers. The provisions aim to regulate the use of these investigative techniques and to prevent the unnecessary invasion of the privacy of individuals, essentially to a strike a balance between private and public rights. Please note the Council does not use CHIS powers (see 2.3 below).

2.2. Surveillance

2.2.1. Surveillance

Surveillance has a broad definition in the Act. It includes:

a) Monitoring, observing or listening to persons, their movements, conversations or other activities or communication. “Persons” includes limited companies, partnerships and cooperatives as well as individuals;

b) Recording anything monitored, observed or listened to in the course of surveillance; and

c) Surveillance by or with the assistance of a surveillance device.

2.2.2. Covert Surveillance

C*overt surveillance* is *surveillance*:

“Carried out in a manner calculated to ensure that persons who are subject to the surveillance are unaware that it is taking place”.

Note: Surveillance which is carried out in the open and is not hidden from the persons being observed does not need to be authorised under RIPA.

2.2.3. Intrusive Surveillance

Local authorities **cannot** carry out or authorise intrusive surveillance in any circumstances. ***Intrusive surveillance*** is surveillance:

a) Carried out in relation to anything taking place on any residential premises or in any private vehicle; and

b) Which involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device; or

c) Is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being present on the premises or in the vehicle, where the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

Surveillance will not be intrusive if it is carried out by means of a surveillance device designed principally for the purpose of providing information about the location of a vehicle.

2.2.4. Directed Surveillance

RIPA provides that ***directed surveillance*** is surveillance, which is covert and not intrusive and is undertaken:

a) For the purpose of a specific investigation or a specific operation;

b) In such a manner likely to result in obtaining ***private information*** about any person (whether or not one specifically identified for the purposes of the investigation or operation); and

c) Otherwise than by way of an immediate response to events or circumstances where it would not be reasonably practical for an authorisation to be sought.

2.2.5. **P*rivate information*** is any information relating to a person's private or family life including his or her relationships with others. The term is broadly interpreted and may include business or professional activities. The fact that covert surveillance is carried out in a public place or on business premises does not mean that it cannot result in obtaining personal information. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites.

2.2.6. When conducting covert test purchase operations at more than one establishment, it is not necessary to construct an authorisation for each premise to be visited but the intelligence must be sufficient to prevent "fishing trips". Premises may be combined within a single authorisation provided that each is identified at the outset. Necessity, proportionality and collateral intrusion must be carefully addressed in relation to each of the premises. It is unlikely that authorisations will be considered proportionate without demonstration that overt methods have been attempted and failed.

2.3. **Covert Human Intelligence Sources ('CHIS')**

2.3.1. It is Council policy of H&F not to use covert human intelligence sources. It is important that officers understand when the RIPA provisions regarding CHIS come into play so that they can avoid such circumstances.

RIPA defines a person as a CHIS if:

a) They establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c) below;

b) They covertly use such a relationship to obtain information or to provide access to any information to another person; or

c) They covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

2.3.2. A person who reports suspicion of an offence is not a CHIS and they do not become a CHIS if they are asked if they can provide additional information, e.g. details of the suspect's vehicle or the time that they leave for work. It is only if the person reporting suspicion establishes or maintains a personal relationship with another person for the purpose of covertly obtaining or disclosing information that they become a CHIS.

2.3.3. If you believe that using a CHIS is essential for your investigation and you want the Council to depart from the usual policy of not using covert personal relationships you should discuss this with an Authorising Officer.

2.3.4. Officers are advised to consult paragraphs 2.17 to 2.26 of the Covert Human Intelligence Sources Revised Code of Practice 2018 which provides further information on when human source activity will meet the definition of a CHIS.

3. AUTHORISATION PROCEDURE

3.1. The Home Office has produced model forms to assist with the requirements of the authorisation process. Copies of the forms, adapted for use by the Council, are attached at Appendices 3 – 6.

3.2. Authorisation must be obtained in relation to each separate investigation. All applications for authorisations, and the authorisations themselves, must be in writing.

3.3. **Judicial Approval**

3.3.1. The Authorisation does not take effect until the court has made an order approving the grant of the authorisation.

3.3.2. The court has the power to refuse to approve the authorisation and to make an order quashing the authorisation**.**

3.3.3. The Procedure for authorising RIPA applications and seeking Judicial Approval is attached as Appendix 1.

3.4. **Authorising Officers**

3.4.1. The Authorisation does not take effect until the court has made an order approving the grant of the authorisation.

3.4.2. RIPA provides that responsibility for authorising directed surveillance, use of a CHIS lies, within a local authority, with an 'Director, Head of Service, Service Manager or equivalent'.

3.4.3. The following Officers are empowered to act as Authorised Persons for applications for surveillance and CHIS:

- Andy Hyatt: Tri Borough Head of Fraud
- Valerie Simpson: Strategic Lead for Environmental Health and Regulatory Services
- Matthew Hooper: Chief Officer for Safer Neighbourhoods & Regulatory Services

3.4.4. Authorising Officers should not be responsible for authorising investigations in which they are directly involved.

3.4.5. All Authorising Officers must have current working knowledge of human rights principles, specifically those of necessity and proportionality.

3.4.6. All Authorising Officers are required to attend the necessary training in accordance with section 12 of this policy.

3.5. Confidential Information

3.5.1. Investigations which may involve "confidential information" must not be conducted without first consulting Legal Services. Confidential information in this context is defined by RIPA and consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.

3.5.2. Surveillance involving confidential information cannot be authorised by an Authorising Officer, only the Chief Executive can authorise surveillance of this nature.

3.6. Necessity and Proportionality

3.6.1. A local authority is required to show that an interference with an individual's right to privacy is justifiable, to the extent that it is both ***necessary and proportionate***.

3.6.2. Directed Surveillance can only be authorised where the Authorising Officer believes, in the circumstances of a particular case, that it is ***necessary*** for the purpose of preventing or detecting crime or of preventing disorder **and** meets the "Crime Threshold" where the criminal offences being investigated meets one of the following conditions:

- The criminal offences, whether on summary conviction or on indictment, are punishable by a *maximum term* of at *least 6 months imprisonment* or an offence under:
  - S146 of the Licensing Act 2003 (sale of alcohol to children)
  - S147 of the Licensing Act 2003 (allowing the sale of alcohol to children)
  - S147A of the Licensing Act 2003 (persistently selling alcohol to children)
  - Section 7 of the Children and Young Persons Act 1933 (sale of tobacco, etc to persons under 18).

3.6.3. ***Proportionality*** is a key concept of RIPA. The Authorising Officer must also believe that the directed surveillance or use of a CHIS is

proportionate to what it is sought to achieve. In effect, any intrusion into individual's privacy should be no more than is absolutely necessary.

3.6.4. The authorisation should demonstrate how an Authorising Officer has reached the conclusion that the activity is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate (the proverbial 'sledgehammer to crack a nut').

3.6.5. The following elements of proportionality should be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; and
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

3.7. Collateral Intrusion

3.7.1. As part of this process an assessment should be made of the risk of what is termed '*collateral intrusion'* - intrusion into the privacy of persons other than those that are the subjects of investigation. Measures should be taken, wherever possible, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation.

3.7.2. If collateral intrusion is inevitable, publication of the material/evidence obtained must be carefully controlled. If the evidence is used in court proceedings, if may be possible to deal with collateral intrusion by appropriate submission.

4. DURATION OF AUTHORISATIONS – REVIEW, RENEWAL AND CANCELLATION

4.1. Directed Surveillance

4.1.1. An authorisation for directed surveillance will last **3 months** unless cancelled or renewed and must be cancelled when no longer necessary or proportionate.

4.1.2. Regular reviews of all authorisations must be undertaken to assess the need for the directed surveillance to continue. The results of the review should be recorded on the central register (see below).

4.1.3. Authorisations can be renewed before the date on which they would cease to have effect provided that they continue to meet the relevant criteria. Judicial approval is required for a renewal. The renewal takes effect on the day on which the authorisation would have expired and continues for a **3 or 12-month period** according to the type of activity. Details in relation to any renewal should also be included in the central register.

4.1.4. An Authorising Officer must cancel an authorisation if he or she is satisfied that the activity no longer meets the criteria on which it was based. As before, details of this should be recorded in the central register.

5. CENTRAL RECORD OF AUTHORISATIONS

5.1. The Council must hold a centrally retrievable record of all applications that must be retained for a period of at least 3 years from the ending of an authorisation. This should include the unique reference number ('URN') of the investigation and details of the authorisation, review, cancellation and any renewal. The date of the court order approving the application will also be recorded in the central register.

5.2. The central record is maintained by Mohammed Basith, RIPA Coordinator. Copies of all relevant documentation relating to applications should therefore be emailed to Mohammed.Basith@lbhf.gov.uk.

6. SENIOR RESPONSIBLE OFFICER (SRO)

6.1. The Act also requires the Council to have an SRO who is responsible for ensuring compliance with the Act and Code of Guidance and the integrity of the process in place within the authority to acquire communications data. Bram Kainth, Executive Director of Place, acts as the SRO for the Council.

7. REPORTING

7.1. The Head of Community Safety will report on the use of RIPA to the Hammersmith & Fulham Council Community Safety and Environment Policy and Accountability Committee annually.

7.2. The SRO may, after consultation with the Authorising Officers, make changes to the list of Authorising Officers as they consider appropriate in accordance with the requirements of RIPA.

8. HANDLING AND DISCLOSURE OF MATERIALS AND DOCUMENTS

8.1. The Authorising Officer should retain RIPA related documents for a period of 3 years. However, where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.

8.2. A copy of all completed RIPA forms, including applications (whether granted or refused), authorisations, reviews, renewals and cancellations, must be forwarded by the Authorising Officer to the RIPA Coordinator.

8.3. Material obtained or produced during the course of investigations subject to RIPA authorisations should be processed, stored and destroyed in accordance with the requirements of the Data Protection Act 2018, the Freedom of Information Act 2000, any other legal requirements, including those of confidentiality, and the Council's policies and procedures currently in force relating to document retention.

8.4. All RIPA records, whether in original form or copies must be kept in secure locked storage when not in use.

8.5. All electronic copies of RIPA records, as well as the Central RIPA register, must be stored and shared in accordance with point 8.3. and password protected.

8.6. If there is any doubt regarding information handling and confidentiality, advice should be sought from the RIPA Coordinator or the SRO.

9. CCTV

9.1. The general usage of the Council's CCTV system is not affected by this policy. However, if Council officers want to use the Council's CCTV cameras for covert surveillance covered by RIPA then they must have a RIPA authorisation. The Police and Transport for London (TfL) are the

only other organisation permitted to use the Council CCTV for RIPA purposes.

9.2. Where the Metropolitan Police wish to use the Council's CCTV system for their own purposes, they shall seek their own authorisation in accordance with Sections 28 or 29 of the Act. In such circumstances authorisation shall usually be obtained from the Superintendent pursuant to the Regulation of Investigatory Powers (Prescription of Officers, Ranks and Positions) Order 2000.

10. SOCIAL MEDIA

10.1. Officers conducting online investigations should consult Note 289 on 'Covert Surveillance of Social Network Sites' of the OSC Procedures and Guidance.

10.2. Officers conducting online investigations should also consult paragraphs 3.10 - 3.17 of the Home Office Covert Surveillance and Property Interference Code of Practice 2018.

10.3. Officers checking Facebook, Instagram, Flickr and other forms of social media as part of an investigation, need to be aware that such activity may be subject to RIPA either as directed surveillance or deploying a CHIS (see paragraph 3.3.1 above for the definition of a CHIS) and the Council do not authorise the use of CHIS. Browsing public open web pages where access is not restricted to "friends", followers or subscribers is not covert activity provided the investigator is not taking steps to hide her/his activity from the suspect. The fact that the suspect is or may be unaware of the surveillance does not make it covert. However, any surveillance activity carried out in a manner which is calculated to ensure that a person subject to surveillance is unaware that surveillance against them is taking place is activity which is covert and officers will need to consider obtaining a RIPA or NON-RIPA authorisation. Similarly, repeat viewing of "open source" social media sites may constitute directed surveillance. This should be considered on a case by case basis and officers will need to consider obtaining a RIPA or NON-RIPA authorisation.

10.4. Officers must not covertly access information on social media which is not open to the public, for example by becoming a "friend' of a person on Facebook, or communicating via social media with the suspect as this

type of activity conducted in a covert manner would engage the CHIS provisions which the Councils do not authorise. An example of non-permitted covert surveillance is the creation of a fake profile. However, this may not apply if the only interaction avoids establishing a relationship by only doing the minimum required to make a test purchase (as per paragraph 10.7 below).

10.5. The gathering and use of online personal information by the Council will engage Human Rights particularly the right to privacy under Article 8 of the European Convention on Human Rights. To ensure such rights are respected the data protection principles in the Data Protection Act 2018 must also be complied with.

10.6. Where online surveillance involves employees then the Information Commissioner's Office's (ICO) Employment Practices Code (part 3) will apply. This requires an impact assessment to be done before the surveillance is undertaken to consider, amongst other things, necessity, proportionality and collateral intrusion. Whilst the code is not law, it will be taken into account by the ICO and the courts when deciding whether the Data Protection Act (2018) has been complied with.

10.7. Where social media or internet sites are used to investigate the sale of counterfeit goods officers should consider Note 239 on 'Covert Internet Investigations, e-Trading' of the OSC Procedures and Guidance which states: 'CHIS authorisation is only required for the use of an internet trading organisation such as eBay when a covert relationship is likely to be formed. The use of disguised purchaser details in a simple, overt, electronic purchase does not require a CHIS authorisation, because no relationship is usually established at that stage'.

11. TRAINING

11.1. Officers conducting surveillance operations or using a CHIS must have an appropriate accreditation or be otherwise suitably qualified or trained. Authorising Officers will have received training that has been approved by the SRO.

11.2. All training will take place at reasonable intervals to be determined by the SRO but it is envisaged that an update will usually be necessary following legislative or good practice developments or otherwise every 12 months.

11.3. A log will be kept recording all training received by Authorising Officers and other officers involved in RIPA. This training log will be stored alongside the Central RIPA Register.

12. THE INSPECTION PROCESS AND OVERSIGHT

12.1. On the 1st September 2017, The Office of Surveillance Commissioners, The Intelligence Services Commissioner's Office and The Interception of Communications Commissioner's Office were abolished by the Investigatory Powers Act 2016. The Investigatory Powers Commissioner's Office (IPCO) is now responsible for the judicial oversight of the use of covert surveillance by public authorities throughout the United Kingdom.

13. FURTHER GUIDANCE

13.1. This policy must be read in conjunction with current Home Office guidance.

Full Codes of Practice can be found on the Home Office website

https://www.gov.uk/government/collections/ripa-codes

Further information is also available on Investigatory Powers Commissioner's Office website

https://www.ipco.org.uk/

Legal advice can be obtained from Legal Services, contacts:
Grant Deg Assistant Director, Legal Services Grant.Deg@lbhf.gov.uk

Appendix 1 - PROCEDURE FOR AUTHORISING RIPA APPLICATIONS AND SEEKING JUDICIAL APPROVAL

1 DIRECTED SURVEILLANCE: CRIME THRESHOLD

We can only authorise the use of **directed surveillance** for the following purposes:

- **To prevent or detect criminal offences:**
  - **that are punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months imprisonment**

  OR
  - **that relate to underage sale of alcohol and tobacco under the following legislation:**
    - **S146 of the Licensing Act 2003 (sale of alcohol to children)**
    - **S147 of the Licensing Act 2003 (allowing the sale of alcohol to children)**
    - **S147A of the Licensing Act 2003 (persistently selling alcohol to children)**
    - **Section 7 of the Children and Young Persons Act 1933 (sale of tobacco, etc to persons under 18)**

We cannot authorise the use of directed surveillance for the purpose of preventing **disorder** unless this involves a criminal offence, whether on summary conviction or on indictment, punishable by a maximum term of at least 6 months imprisonment. (e.g. affray).

On the RIPA Application Form **you must**:

1 State you are investigating a criminal offence; and

2 Identify the relevant offence and statute which is either punishable with 6 months imprisonment or is related to underage sales of alcohol or tobacco.

Note: that if it becomes clear during an investigation the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the Crime threshold the authorisation **must** be cancelled.

Lesser Offences

In a case where the surveillance has been authorised to investigate a specific offence which meets the threshold, but the evidence obtained is used to substantiate offences which fall below the threshold it will be up to the court to decide whether to admit the evidence obtained.

CHIS

Conduct or use of a CHIS can only be authorised where it is necessary for the purpose of preventing or detecting crime or of preventing disorder.

The Authorisation does not take effect until the court has made an order approving the grant of the authorisation. The court has the power to refuse to approve the authorisation and to make an order quashing the authorisation**.**

To obtain legal advice call Legal Services for advice:
Janette Mullins, Acting Chief Solicitor (Litigation and Social Care):
020 8753 2744

2 PROCEDURE

1. Obtain URN from Mohammed Basith, RIPA Coordinator.
2. Submit Application Form (Appendix 3) to Authorising Officer:
    a. Andy Hyatt: Tri Borough Head of Fraud
    b. Valerie Simpson: Strategic Lead for Environmental Health and Regulatory Services
    c. Matthew Hooper: Chief Officer for Safer Neighbourhoods & Regulatory Services

If approval is granted the form to be signed and dated but the **authorisation will not be activated until judicial approval is obtained.**

3. Complete FORM ANNEX A
   This will contain a brief summary of the circumstances of the case but the RIPA authorisation form **must** contain all the information necessary to make application.

4. Telephone the court: Contact Maureen Robertson (Court bookings Manager) on 020 3126 3080 to arrange a date/time to attend. The application will be heard by a district judge in chambers.

Court details:
Westminster Magistrates Court, 181 Marylebone Road
London, NW1 5BR
Email: westminster.mc@hmcts.gsi.gov.uk

Applications will usually be heard at Westminster Magistrates at 10:00am and you must be at court by 9:30am to allow the Legal Adviser to check the application before it goes to court. Go to Court Office on first floor and explain you have a RIPA Judicial Approval Application.

5. Take with you:
   1 Both the original and a copy of RIPA Authorisation form
   2 Copy of authority to make application
   3 Two copies of partly completed Form Annex A

6. Hearing
   Sign in with the Court usher; give him/her the above documents; explain a RIPA Judicial approval application and if you wish to swear on oath or Affirm. Stand in witness box.

   - Take, oath or Affirm; identify yourself, name, post, employer
   - Explain you are the investigating officer who has made the application to AO
   - Identify, the AO, Name and post and give date of authorisation
   - State that you wish to obtain Judicial Approval for Directed Surveillance under S38 Protection of Freedoms Act 2012 and that you have partly completed Form Annex A

- The Magistrate will consider the following matters:

(a) that the person who granted the authorisation was entitled to do so;
(b) for directed surveillance that the application meets the crime threshold test;
(c) that at the time the authorisation was granted there were reasonable grounds for believing that the surveillance described in the authorisation was—
(i) **Necessary,** for the purpose of preventing or detecting crime or of preventing disorder

(ii) **Proportionate** to what was sought to be achieved by it; and

(d) that there remain reasonable grounds for believing those things at the time the court considers the application.

Necessity and Proportionality

It is still the case that the Authorising Officer must be satisfied that the surveillance is **necessary** for the purpose of "the prevention or detection of crime or the prevention of disorder". This goes beyond the prosecution of offences and includes actions taken to prevent, end or disrupt the commission of criminal offences. But before authorising surveillance the Authorising Officer must be satisfied that officers are investigating an identifiable criminal offence.

The guidance for Magistrates states authorisation will not be **proportionate** if it is excessive in the overall circumstances of the cases. The fact that a suspected offence may be serious will not alone justify surveillance.

No activity should be considered **proportionate** if the information which is sought could be reasonably obtained from other less intrusive means. The risk and proportionality of interfering with the privacy of people not connected with the investigation must also be weighed and, where possible, steps taken to mitigate it.

The Magistrates' guidance suggests that following element of proportionality should be considered:

- Balancing the size and scope of the proposed activity against the gravity or extent of the perceived crime or offence:
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- Recording, as far as reasonably practicable, what other methods have been considered and why they were not implemented.

7. **Outcome**

- Application granted and will be effective from date of order.
- Application refused.

- Application refused AND quash authorisation – but must give the Council at least 2 days notice from date of refusal to allow us to make representations.

Court will keep one copy of Annex Form A and one copy of Application.

- Provide Mohammed Basith with a copy of Application Form and a copy of Form Annex A within five days of approval.
- Note review date and provide copy of review and/or cancellation forms to Mohammed Basith.

ANNEX A - RIPA ACCEPTANCE FORM

Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local authority:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of subject:.....

.....

.....

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

.....

.....

.....

.....

.....

.....

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer:.....

Authorising Officer/Designated Person:.....

Officer(s) appearing before JP:.....

Address of applicant department:.....

.....

Contact telephone number:.....

Contact email address (optional):.....

Local authority reference:.....

Number of pages:.....

Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Magistrates' court:.....

Having considered the application, I (tick one):

☐ am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

.....

.....

.....

.....

.....

Reasons

.....

.....

.....

.....

.....

.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court:

Appendix 2 – ROLES AND RESPONSIBILITIES

Senior Responsible Officer (SRO)

The SRO is responsible for:

- The integrity of the process in place within the Council for the management of CHIS and Directed Surveillance;
- Ensuring compliance with the Acts and Codes of Guidance;
- Ensuring that a sufficient number of Authorising Officers are, after suitable training on RIPA and this Policy, duly authorised to take action under this Policy;
- Oversight of the reporting of errors to the relevant Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- Engagement with the Investigatory Powers Commissioner's Office (IPCO) inspectors when they conduct their inspections, where applicable; and
- Where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

Authorising Officer

- The officers named as Authorising Officers in Section 3.4.3 of this Policy shall be the only officers within the Council who can authorise applications under RIPA in accordance with the procedures set out in this Policy.
- Authorising Officers must ensure that staff who report to them follow this Policy and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this Policy.
- Each of the Authorising Officers can authorise applications, for onward consideration by a Magistrate. Each Authorising Officer may authorise renewals and cancellations, and undertake reviews, in relation to any investigation carried out, or proposed to be carried out, by officers.
- Authorising Officers must have current working knowledge of human rights principles, specifically those of necessity and proportionality.
- Authorising Officers must retain RIPA related documents for a period of 3 years. However, where it is believed that the records could be relevant to

pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.

- The officer who authorises a RIPA application should also carry out the review, renewal and cancellation. If the original Authorising Officer is not available to undertake the review, renewal or cancellation, this can be undertaken by any other Authorising Officer.

- Authorising Officers must attend training as directed by the SRO.

RIPA Coordinator

The RIPA Coordinator is responsible for:

- The overall management and oversight of requests and authorisations under RIPA;

- Retaining a copy of the application and authorisation together with any supplementary documentation and notification of the approval given by the authorising officer and maintaining a central RIPA records file matrix entering the required information as soon as the forms/documents are received in accordance with the relevant Home Office Code of Practice;

- The issuing of a unique reference number to each authorisation requested under RIPA (this must be before the application has been authorised);

- Reviewing and monitoring all forms and documents received to ensure compliance with the relevant law and guidance and this Policy and informing the Authorising Officer of any concerns;

- Chasing failures to submit documents and/or carry out reviews/cancellations;

- Providing an annual report and summary on the use of RIPA to the Head of Community Safety;

- Organising a corporate RIPA training programme; and

- Ensuring corporate awareness of RIPA and its value as a protection to the council is maintained.

Head of Community Safety (HoCS)

- The Head of Community Safety will report on the use of RIPA to the Hammersmith & Fulham Council Community Safety and Environment

Policy and Accountability Committee annually, and to other panels and committees (where appropriate).

Appendix 3 - RIPA APPLICATION FORM

Application for use of directed surveillance - GOV.UK (www.gov.uk)

Appendix 4 - RIPA REVIEW FORM

Review of use of directed surveillance - GOV.UK (www.gov.uk) & Reviewing the use of covert human intelligence sources (CHIS) - GOV.UK (www.gov.uk)

Appendix 5 - RIPA RENEWAL FORM

Renewal form for directed surveillance - GOV.UK (www.gov.uk) & Renewal of authorisation to use covert human intelligence sources - GOV.UK (www.gov.uk)

Appendix 6 - RIPA CANCELLATION FORM

Cancellation of use of directed surveillance form - GOV.UK (www.gov.uk) & Cancellation of covert human intelligence sources (CHIS) - GOV.UK (www.gov.uk)

Appendix 7 - COURT AUTHORISATION LETTER

Appendix 7 - COURT AUTHORISATION LETTER.doc

amAppendix B

London Borough of Hammersmith & Fulham

Regulation of Investigatory Powers Act 2000
Policy for Use of Direct Surveillance (Without Judicial Approval / "Non-RIPA")

H&F Version November 2019
1st Revision June 2020
2nd Revision July 2023

CONTENTS

1. INTRODUCTION

1.1. The Regulation of Investigatory Powers Act 2000 (RIPA) provides a statutory framework for police and public authorities to use surveillance data, where necessary and proportionate, for the purpose of preventing or detecting crime. RIPA regulates the use of these powers in a manner that is compatible with the Human Rights Act.

1.2. The purpose of RIPA is to protect the privacy rights of local residents but only to the extent that those rights are protected by the Human Rights Act.

1.3. The Council may only engage the Act when performing its 'core functions'. For example, a Local Authority conducting a criminal investigation would be considered to be performing a 'core function', whereas the disciplining of an employee would be considered to be a 'non-core' or 'ordinary' function.

1.4. In addition, surveillance may only be authorised under RIPA **when investigating criminal offences which are punishable by a *maximum term* of at *least 6 months imprisonment* ("the serious crime threshold").** This test was introduced by the Government following concerns that local authorities had been using directed surveillance techniques in less serious investigations, for example, to tackle dog fouling or checking an individual resides in a school catchment area.

1.5. Local Authorities have an obligation to deal with Anti-social behaviour (ASB) which involves the day-to-day incidents of crime, nuisance and disorder that make many people's lives a misery. This varies from vandalism, to public drunkenness or aggressive dogs, to noisy or abusive neighbours.

1.6. The victims of ASB can feel helpless and in many cases, the behaviour is targeted against the most vulnerable in our society. Even what is perceived as 'low level' ASB, when targeted and persistent, can have devastating effects on a victim's life.

1.7. To protect residents from ASB it may be necessary for Council Officers to conduct covert surveillance that does not satisfy the serious crime threshold and cannot be authorised by RIPA. For example, graffiti, criminal damage and urinating in public areas can have a real impact on the residents.

1.8. To enable the Council to support victims it is recognised that it may be necessary for the Council to conduct covert surveillance that does not satisfy the serious crime threshold and cannot be authorised by RIPA.

1.9. In addition, the Council as a Licensing Authority may need to carry out surveillance of licensed premises in order to promote the four licensing objectives.

1.10. On rare occasions it may also be necessary for Council Officers to conduct covert surveillance when carrying out a Disciplinary Investigation of an employee.

1.11. Officers of the London Borough of Hammersmith & Fulham who want to undertake directed surveillance which does not meet the "serious crime threshold" must therefore do so in accordance with this policy.

1.12. Nonetheless, when considering covert surveillance which is outside of RIPA, Council Officers should have regard to the Council's RIPA policy, the Directed Surveillance Code of Practice and the OSC Procedures and guidance (see section **15**).

1.13. In addition, Officers should have regard to the fact that covert surveillance undertaken without RIPA approval, comes with risks e.g.

- evidence unlawfully obtained may be ruled inadmissible and could result in the case collapsing;
- a complaint to the RIPA Tribunal;
- a complaint to the Local Government Ombudsman;
- a claim for damages; or
- adverse publicity.

1.14. Investigating and Authorising Officers **must** take account of these risks when considering non RIPA surveillance.

2. DIRECT SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES

2.1. Part II of Chapter II RIPA deals with Direct Surveillance and Covert Human Intelligence Sources. It covers intrusive surveillance, directed

surveillance and use and conduct of Covert Human Intelligence Sources (known as “CHIS”) who are more recognisable as agents, informants or undercover officers. The provisions aim to regulate the use of these investigative techniques and to prevent the unnecessary invasion of the privacy of individuals, essentially to a strike a balance between private and public rights. Please note the Council does not use CHIS powers (see 2.3 below).

2.2. Surveillance

2.2.1. Surveillance

Surveillance has a broad definition in the Act. It includes:

a) Monitoring, observing or listening to persons, their movements, conversations or other activities or communication. “Persons” includes limited companies, partnerships and cooperatives as well as individuals;

b) Recording anything monitored, observed or listened to in the course of surveillance; and

c) Surveillance by or with the assistance of a surveillance device.

2.2.2. Covert Surveillance

Covert surveillance is *surveillance*:

“Carried out in a manner calculated to ensure that persons who are subject to the surveillance are unaware that it is taking place”.

Note: Surveillance which is carried out in the open and is not hidden from the persons being observed does not need to be authorised under RIPA.

2.2.3. Intrusive Surveillance

Local authorities **cannot** carry out or authorise intrusive surveillance in any circumstances. ***Intrusive surveillance*** is surveillance:

a) Carried out in relation to anything taking place on any residential premises or in any private vehicle; and

b) Which involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device; or

c) Is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being present on the premises or in the vehicle, where the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

Surveillance will not be intrusive if it is carried out by means of a surveillance device designed principally for the purpose of providing information about the location of a vehicle.

2.2.4. Directed Surveillance

RIPA provides that ***directed surveillance*** is surveillance, which is covert and not intrusive and is undertaken:

a) For the purpose of a specific investigation or a specific operation;

b) In such a manner likely to result in obtaining ***private information*** about any person (whether or not one specifically identified for the purposes of the investigation or operation); and

c) Otherwise than by way of an immediate response to events or circumstances where it would not be reasonably practical for an authorisation to be sought.

2.2.5. **P*rivate information*** is any information relating to a person's private or family life including his or her relationships with others. The term is broadly interpreted and may include business or professional activities. The fact that covert surveillance is carried out in a public place or on business premises does not mean that it cannot result in obtaining personal information. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be

an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites.

2.2.6. When conducting covert test purchase operations at more than one establishment, it is not necessary to construct an authorisation for each premise to be visited but the intelligence must be sufficient to prevent "fishing trips". Premises may be combined within a single authorisation provided that each is identified at the outset. Necessity, proportionality and collateral intrusion must be carefully addressed in relation to each of the premises. It is unlikely that authorisations will be considered proportionate without demonstration that overt methods have been attempted and failed.

2.3. Covert Human Intelligence Sources ('CHIS')

2.3.1. It is Council policy of H&F not to use covert human intelligence sources. It is important that officers understand when the RIPA provisions regarding CHIS come into play so that they can avoid such circumstances.

RIPA defines a person as a CHIS if:

a) They establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c) below;

b) They covertly use such a relationship to obtain information or to provide access to any information to another person; or

c) They covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

2.3.2. A person who reports suspicion of an offence is not a CHIS and they do not become a CHIS if they are asked if they can provide additional information, e.g. details of the suspect's vehicle or the time that they leave for work. It is only if the person reporting suspicion establishes or maintains a personal relationship with another person for the purpose of covertly obtaining or disclosing information that they become a CHIS.

2.3.3. If you believe that using a CHIS is essential for your investigation and you want the Council to depart from the usual policy of not using covert personal relationships you should discuss this with an Authorising Officer.

2.3.4. Officers are advised to consult paragraphs 2.17 to 2.26 of the Covert Human Intelligence Sources Revised Code of Practice 2018 which provides further information on when human source activity will meet the definition of a CHIS.

3. POLICY FOR THE CONDUCT OF SURVEILLANCE NOT AUTHORISED BY RIPA

3.1. Following the introduction of the "serious crime threshold" the legal protection offered by RIPA is no longer available in cases where the criminal offence under investigation is not punishable by at *least* 6 months imprisonment.

3.2. However, this does not mean that it will not be possible to investigate lesser offences or other non-criminal matters with a view to protecting the victim or stopping the offending behaviour or that surveillance cannot be used in such investigations.

3.3. The statutory RIPA Code of Practice on covert surveillance makes it clear that routine patrols, observation at trouble 'hotspots', immediate response to events and overt use of CCTV are all techniques which do not require RIPA authorisation.

3.4. It is recognised that in order to protect residents from serious instances of ASB it may be necessary exceptionally for Council Officers to conduct covert surveillance that does not satisfy the serious crime threshold and cannot be authorised by RIPA. On rare occasions it may also be necessary for Council Officers to conduct covert surveillance when carrying out a disciplinary investigation of an employee.

3.5. The Office of Surveillance Commissioners guidance, for example, points out in relation to the Police use of intrusive surveillance for the protection of repeat burglary victims and vulnerable pensioners that "the fact that particular conduct [by the authority] may not be authorised under RIPA...does not necessarily mean that the actions proposed cannot lawfully be undertaken, even though without the protection that

an authorisation under the Acts would afford". The Investigatory Powers Tribunal has provided clear advice in its judgement in *Addison, Addison & Taylor v Cleveland Police* that where no authorisation is capable of being granted in such circumstances, "it will behove a police force to follow a course similar to that adopted here; i.e. a procedure as close as possible to that which would be adopted if an authorisation could be obtained from a "relevant Authorising Officer".

3.6. For this reason, the Council have adopted this policy and procedure for "non-RIPA" covert surveillance. All "non-RIPA" surveillance must be carried out in accordance with this policy.

4. AUTHORISING OFFICERS

4.1. RIPA provides that responsibility for authorising directed surveillance, use of a CHIS lies, within a local authority, with a **'Director, Head of Service, Service Manager or equivalent'.**

4.2. The following Officers are empowered to act as Authorising Officers for applications for "non-RIPA" surveillance:

- Andy Hyatt: Tri Borough Head of Fraud
- Valerie Simpson: Strategic Lead for Environmental Health and Regulatory Services
- Matthew Hooper: Chief Officer - Safer Neighbourhoods & Regulatory Services

4.3. Authorising Officers should not be responsible for authorising investigations in which they are directly involved.

4.4. All Authorising Officers must have current working knowledge of human rights principles, specifically those of necessity and proportionality.

4.5. All Authorising Officers are required to attend the necessary training in accordance with section 16 of this policy.

5. NECESSITY AND PROPORTIONALITY

5.1. A local authority is required to show that an interference with an individual's right to privacy is justifiable, to the extent that it is both ***necessary and proportionate***.

5.2. Directed Surveillance can only be authorised where the Authorising Officer believes, in the circumstances of a particular case, that it is ***necessary*** for the purpose of preventing or detecting crime or of preventing disorder.

5.3. ***Proportionality*** is a key concept of RIPA. The Authorising Officer must also believe that the directed surveillance or use of a CHIS is *proportionate* to what it is sought to achieve. In effect, any intrusion into individual's privacy should be no more than is absolutely necessary.

5.4. The authorisation should demonstrate how an Authorising Officer has reached the conclusion that the activity is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate (the proverbial 'sledgehammer to crack a nut').

5.5. The following elements of proportionality should be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; and
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

6. COLLATERAL INTRUSION

6.1. As part of this process an assessment should be made of the risk of what is termed '*collateral intrusion'* - intrusion into the privacy of persons other than those that are the subjects of investigation. Measures should be taken, wherever possible, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation.

6.2. If collateral intrusion is inevitable, publication of the material/evidence obtained must be carefully controlled. If the evidence is used in court

proceedings, if may be possible to deal with collateral intrusion by appropriate submission.

7. AUTHORISATION PROCEDURE

7.1. The Home Office has produced model forms to assist with the requirements of the authorisation process. Copies of the forms, adapted for use by the Council, are attached at Appendices 2-4.

7.2. Authorisation must be obtained in relation to each separate investigation. All applications for authorisations, and the authorisations themselves, must be in writing.

7.3. A Council Officer seeking to carry out surveillance outside of RIPA must complete the Non-RIPA Application Form attached to this policy (Appendix 2).

7.4. In completing the form, the officer must have regard to this policy and address the issues of Necessity and Proportionality and “collateral intrusion”.

7.5. The form must be passed to one of the Authorising Officers who is empowered to authorise applications made by staff.

7.6. The Authorising Officer will consider the application and will decide whether or not to authorise the surveillance applying the principles set out in this policy.

7.7. The “Non-RIPA” surveillance must not begin before the date the application is signed by the Authorising Officer.

7.8. The authorised application form must be forwarded to the RIPA Coordinator, Mohammed Basith, who will keep a central record of all RIPA and “non-RIPA” surveillance.

7.9. A monthly review of the authorisation must be conducted to assess the need for the surveillance to continue. The Investigating Officer will submit a review form to the Authorising Officer. The results of the review should be recorded on the central register.

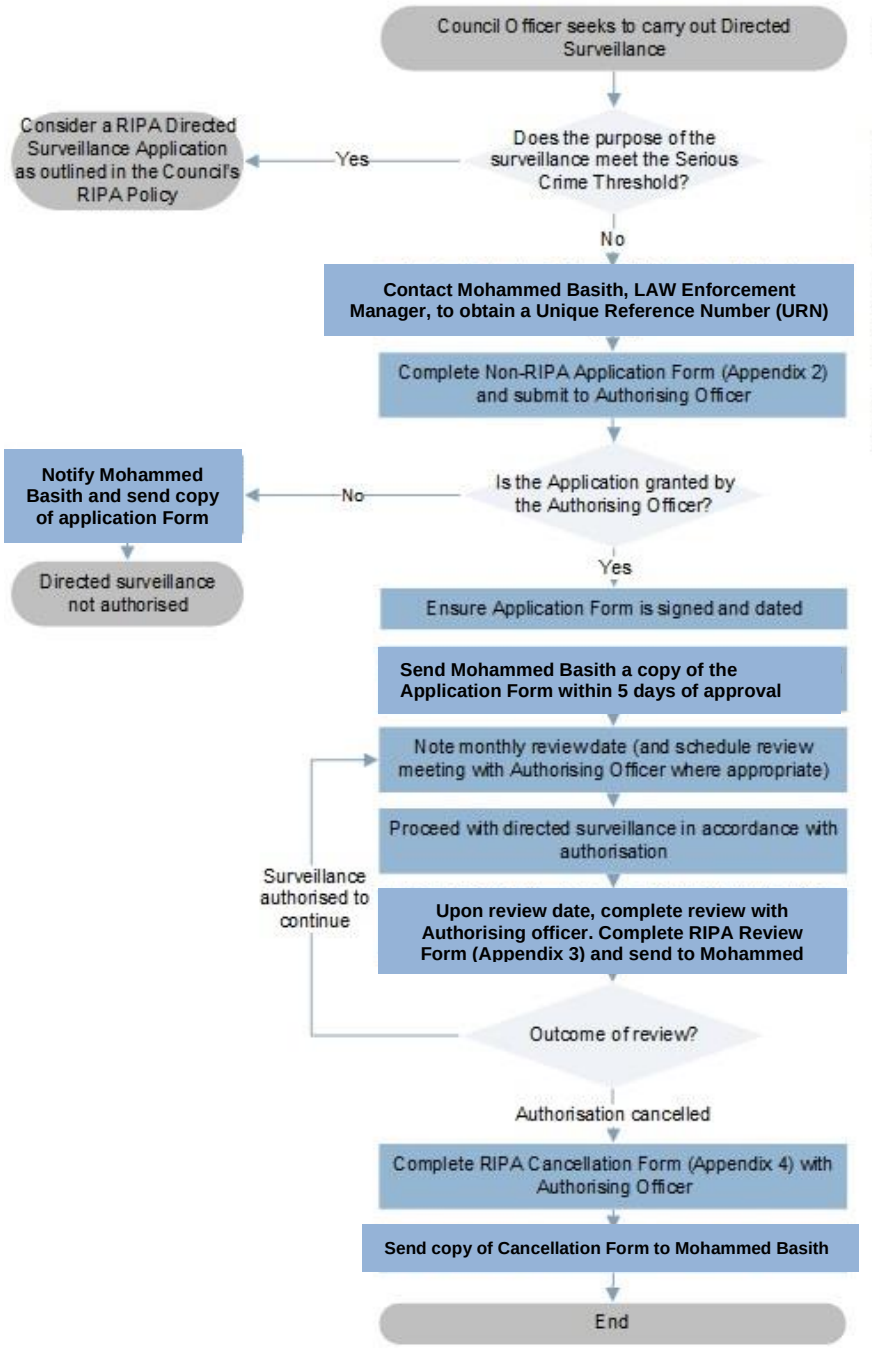
7.10. Authorisation for “non-RIPA” surveillance will last **3 months** unless cancelled or renewed and must be cancelled when no longer necessary or proportionate.

7.11. An Investigating Officer, in liaison with the Authorising Officer, must cancel an authorisation if he or she is satisfied that the activity no longer meets the criteria on which it was based.

7.12. The SRO in conjunction with the RIPA Coordinator is responsible for ensuring compliance with this procedure and will report on the use of “Non-RIPA” surveillance annually to Members.

8. DURATION OF AUTHORISATIONS – REVIEW, RENEWAL AND CANCELLATIONS

H&F Non-RIPA Application Process Map



Directed Surveillance

8.1. An authorisation for directed surveillance will last **3 months** unless cancelled or renewed (on a month by month basis) and must be cancelled when no longer necessary or proportionate.

8.2. Regular reviews of all authorisations must be undertaken to assess the need for the directed surveillance to continue. The results of the review should be recorded on the central register.

8.3. Authorisations can be renewed before the date on which they would cease to have effect provided that they continue to meet the relevant criteria. The renewal takes effect on the day on which the authorisation would have expired and continues for **3 months** (or 12 months for CHIS authorisations) according to the type of activity. Details in relation to any renewal should also be included in the central register.

8.4. An Authorising Officer must cancel an authorisation if he or she is satisfied that the activity no longer meets the criteria on which it was based. As before, details of this should be recorded in the central register.

9. CENTRAL RECORD OF AUTHORISATIONS

9.1. The Council must hold a centrally retrievable record of all applications for RIPA and "non-RIPA" surveillance that must be retained for a period of at least 3 years from the ending of an authorisation. This should include the unique reference number ('URN') of the investigation and details of the authorisation, review, cancellation and any renewal.

9.2. The central record is maintained by Mohammed Basith, RIPA Coordinator. Copies of all relevant documentation relating to applications should therefore be emailed to mohammed.basith@lbhf.gov.uk.

10. SENIOR RESPONSIBLE OFFICER (SRO)

10.1. The Act also requires the Council to have an SRO who is responsible for ensuring compliance with the Act and Code of Guidance and the integrity of the process in place within the authority to acquire communications data. Bram Kainth, Executive Director of Place acts as

the SRO for the Council.

11. REPORTING

11.1. The Head of Community Safety will report on the use of RIPA (including "non-RIPA" surveillance) annually to the Hammersmith & Fulham Council Community Safety and Environment Policy and Accountability Committee.

11.2. The SRO may, after consultation with the Authorising Officers, make changes to the list of Authorising Officers as they consider appropriate in accordance with the requirements of RIPA.

12. HANDLING AND DISCLOSURE OF MATERIALS AND DOCUMENTS

12.1. The Authorising Officer should retain all RIPA (and "non-RIPA") related documents for a period of 3 years. However, where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.

12.2. A copy of all completed RIPA (and "non-RIPA") forms including applications (whether granted or refused), authorisations, reviews, renewals and cancellations, must be forwarded by the Authorising Officer to the RIPA Coordinator.

12.3. Material obtained or produced during the course of an investigation should be processed, stored and destroyed in accordance with the requirements of the Data Protection Act 2018, the Freedom of Information Act 2000, any other legal requirements, including those of confidentiality, and the Council's policies and procedures currently in force relating to document retention.

12.4. All RIPA (including "non-RIPA") records, whether in original form or copies must be kept in secure locked storage when not in use.

12.5. All electronic copies of RIPA (including "non-RIPA") records, as well as the Central RIPA register, must be stored and shared in accordance with point 13.3. and password protected.

12.6. If there is any doubt regarding information handling and confidentiality, advice should be sought from the RIPA Coordinator or the SRO.

13. CCTV

13.1. The general usage of the Council's CCTV system is not affected by this policy. However, if Council officers want to use the Council's CCTV cameras for covert surveillance covered by RIPA then they must have a RIPA or Non RIPA authorisation. The Police and Transport for London (TfL) are the only other organisation permitted to use the Council CCTV for RIPA purposes.

14. SOCIAL MEDIA

14.1. Officers conducting online investigations should consult Note 289 on 'Covert Surveillance of Social Network Sites' of the OSC Procedures and Guidance.

14.2. Officers conducting online investigations should also consult paragraphs 3.10 - 3.17 of the Home Office Covert Surveillance and Property Interference Code of Practice 2018.

14.3. Officers checking Facebook, Instagram, Flickr and other forms of social media as part of an investigation, need to be aware that such activity may be subject to RIPA either as directed surveillance or deploying a CHIS (see paragraph 3.3.1 above for the definition of a CHIS) and the Council do not authorise the use of CHIS. Browsing public open web pages where access is not restricted to "friends", followers or subscribers is not covert activity provided the investigator is not taking steps to hide her/his activity from the suspect. The fact that the suspect is or may be unaware of the surveillance does not make it covert. However, any surveillance activity carried out in a manner which is calculated to ensure that a person subject to surveillance is unaware that surveillance against them is taking place is activity which is covert and officers will need to consider obtaining a RIPA or NON-RIPA authorisation. Similarly, repeat viewing of "open source" social media sites may constitute directed surveillance. This should be considered on a case by case basis and officers will need to consider obtaining a RIPA or NON-RIPA authorisation.

14.4. Officers must not covertly access information on social media which is not open to the public, for example by becoming a "friend' of a person on Facebook, or communicating via social media with the suspect as this type of activity conducted in a covert manner would engage the CHIS

provisions which the Councils do not authorise. An example of non-permitted covert surveillance is the creation of a fake profile. However, this may not apply if the only interaction avoids establishing a relationship by only doing the minimum required to make a test purchase (as per paragraph 10.7 below).

14.5. The gathering and use of online personal information by the Council will engage Human Rights particularly the right to privacy under Article 8 of the European Convention on Human Rights. To ensure such rights are respected the data protection principles in the Data Protection Act 2018 must also be complied with.

14.6. Where online surveillance involves employees then the Information Commissioner's Office's (ICO) Employment Practices Code (part 3) will apply. This requires an impact assessment to be done before the surveillance is undertaken to consider, amongst other things, necessity, proportionality and collateral intrusion. Whilst the code is not law, it will be taken into account by the ICO and the courts when deciding whether the Data Protection Act (2018) has been complied with.

14.7. Where social media or internet sites are used to investigate the sale of counterfeit goods officers should consider Note 239 on 'Covert Internet Investigations, e-Trading' of the OSC Procedures and Guidance which states: 'CHIS authorisation is only required for the use of an internet trading organisation such as eBay when a covert relationship is likely to be formed. The use of disguised purchaser details in a simple, overt, electronic purchase does not require a CHIS authorisation, because no relationship is usually established at that stage'.

15. FURTHER GUIDANCE

15.1. This policy must be read in conjunction with:

- the Council's RIPA policy which gives more detail about directed Surveillance and CHIS
- current Home Office guidance

Full Codes of Practice can be found on the Home Office website

https://www.gov.uk/government/collections/ripa-codes

Further information is also available on Investigatory Powers Commissioner's Office website

https://www.ipco.org.uk/

Legal advice can be obtained from Legal Services, contacts:
Grant Deg Assistant Director, Legal Services Grant.Deg@lbhf.gov.uk

Appendix 1 – ROLES AND RESPONSIBILITIES

Senior Responsible Officer (SRO)

The SRO is responsible for:

- The integrity of the process in place within the Council for the management of CHIS and Directed Surveillance;
- Ensuring compliance with the Acts and Codes of Guidance;
- Ensuring that a sufficient number of Authorising Officers are, after suitable training on RIPA and this Policy, duly authorised to take action under this Policy;
- Oversight of the reporting of errors to the relevant Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- Engagement with the Investigatory Powers Commissioner's Office (IPCO) inspectors when they conduct their inspections, where applicable; and
- Where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

Authorising Officer

- The officers named as Authorising Officers in Section 3.4.3 of this Policy shall be the only officers within the Council who can authorise applications under RIPA (including "non-RIPA") in accordance with the procedures set out in this Policy.
- Authorising Officers must ensure that staff who report to them follow this Policy and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this Policy.
- Each of the Authorising Officers can authorise applications, for onward consideration by a Magistrate. Each Authorising Officer may authorise renewals and cancellations, and undertake reviews, in relation to any investigation carried out, or proposed to be carried out, by officers.
- Authorising Officers must have current working knowledge of human rights principles, specifically those of necessity and proportionality.

- Authorising Officers must retain RIPA (including “non-RIPA”) related documents for a period of 3 years. However, where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.

- The officer who authorises a RIPA (including “non-RIPA”) application should also carry out the review, renewal and cancellation. If the original Authorising Officer is not available to undertake the review, renewal or cancellation, this can be undertaken by any other Authorising Officer.

- Authorising Officers must attend training as directed by the SRO.

RIPA Coordinator

The RIPA Coordinator is responsible for:

- The overall management and oversight of requests and authorisations under RIPA (including “non-RIPA”);

- Retaining a copy of the application and authorisation together with any supplementary documentation and notification of the approval given by the authorising officer and maintaining a central RIPA records file matrix entering the required information as soon as the forms/documents are received in accordance with the relevant Home Office Code of Practice;

- The issuing of a unique reference number to each authorisation requested under RIPA, including “non-RIPA” (this must be before the application has been authorised);

- Reviewing and monitoring all forms and documents received to ensure compliance with the relevant law and guidance and this Policy and informing the Authorising Officer of any concerns;

- Chasing failures to submit documents and/or carry out reviews/cancellations;

- Providing an annual report and summary on the use of RIPA (including “non-RIPA”) to the Head of Community Safety;

- Organising a corporate RIPA training programme; and

- Ensuring corporate awareness of RIPA (including “non-RIPA”) and its value as a protection to the council is maintained.

Head of Community Safety (HoCS)

- The Head of Community Safety will report on the use of RIPA (and “non-RIPA”) annually to the Hammersmith & Fulham Council Community Safety and Environment Policy and Accountability Committee, and to other panels and committees (where appropriate).

Appendix 2 – NON-RIPA APPLICATION FORM

Application for use of directed surveillance - GOV.UK (www.gov.uk)

Appendix 3 – NON-RIPA REVIEW FORM

Review of use of directed surveillance - GOV.UK (www.gov.uk)

Appendix 4 – NON-RIPA RENEWAL FORM

Renewal form for directed surveillance - GOV.UK (www.gov.uk)

Appendix 5 – NON-RIPA CANCELLATION FORM

Cancellation of use of directed surveillance form - GOV.UK (www.gov.uk)

APPENDIX C

London Borough of Hammersmith & Fulham

Investigatory Powers Act 2016
Policy for Use of Communications Data

February 2020

Reviewed July 2023

CONTENTS

1. INTRODUCTION

1.1. The Investigatory Power Act (IPA) 2016. The IPA builds on, and supersedes parts of, the Regulation of Investigatory Powers Act (RIPA) 2000. The IPA has granted law enforcement and public authorities updated powers to access communications data for legitimate purposes. It requires a local authority to follow a specific procedure and obtain independent authorisation before obtaining communications data.

1.2. The IPA does NOT allow local authorities to intercept communications (e.g. bugging of telephones etc.). Local authorities are NOT allowed to intercept the content of any person's communications or to access internet connection records for any purpose. It is an offence to do so without lawful authority.

1.3. Failure to comply with the IPA may mean the Council's actions are unlawful and amount to a criminal offence. It may also mean that evidence obtained would be inadmissible in court proceedings and jeopardise the outcome of the case, It could also lead to a claim for damages against the Council.

1.4. Officers of the London Borough of Hammersmith & Fulham who want to access communications data must do so in accordance with this policy.

2. WHAT IS COMMUNICATION DATA?

2.1. The term communications data embraces the 'who', 'when' and 'where' of communication but not the content. It is information about a communication whether it originated from the internet, the postal services, or a telecommunications service.

2.2. Communications data captures who an individual is communicating with, when and where they are communicating, as well as the type of communication and device used.

2.3. There are 2 types of communication data "Entity data" and/or "Events data".

2.3.1. Entity Data:

This relates to the association between an entity and a telecommunications service or telecommunications system or could be description and identification of an entity. Basically, data about a person or thing (such as a device) or information linking them.

For example:

- Billing information such as name, address and bank details of the subscriber
- Phone numbers or other identifiers linked to customer accounts
- Customer address provided to a communications service provider
- IP address allocated to an individual by an internet access provider
- Account holder details for an email account

Entity Data is less intrusive than Events Data and can be obtained for the prevention and detection of any crime.

2.3.2. Events Data:

This means any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunications system where the event consists of one or more entities engaging in a specific activity at as specific time.

For example:

- The type of communication, time sent and duration
- The fact that someone has sent or received an email, phone call, text or social media message
- The location of a person when they made a mobile phone call or the Wi-Fi hotspot their phone was connected to

Events Data can be ONLY be obtained for the prevention and detection of 'Serious Crime'. Which includes:

- A crime involving violence or substantial financial gain
- An offence that can attract a sentence of 12 months or more imprisonment
- An offence which involves, as an integral part of it, a breach of a person's privacy or the sending of a communication
- Offences committed by a corporate body

3. AUTHORISATIONS

3.1. No Council Officer may obtain any form of communication data **unless and until** they have obtained the proper authorisation.

3.2. This means that:

- An Approved Rank Officer (ARO) must be consulted;

- The application must be sent to the Council's Single Point of Contact (SPoC); and
- The application must be approved by the Office for Communication Data Authorisations (OCDA).

3.3. The following types of conduct may be authorised:

- Conduct to obtain communications data - including obtaining data directly or asking any person believed to be in possession of or capable of obtaining such data to obtain and disclose it; and/or
- Giving of a notice – requiring a telecommunications operator to obtain and disclose the required data.

Approved Rank Officer (ARO)

3.4. The following Council Officers are empowered to act as Designated Persons for applications for communications data:

- Andy Hyatt: Tri Borough Head of Fraud
- Valerie Simpson: Strategic Lead for Environmental Health and Regulatory Services
- Matthew Hooper: Chief Officer for Safer Neighbourhoods & Regulatory Services

Single Point of Contact (SPoC)

3.5. The National Anti-Fraud Network (NAFN) provides a SPoC service to the Council. All applications for communication data must be submitted to NAFN.

3.6. All forms to access communications data are covered by the online application process through NAFN.

3.7. Prospective applicants and are required to register on the NAFN Website.

3.8. Once registered, applications for the acquisition of communications data can be managed through the Focus 112 Portal.

Senior Responsible Officer (SRO)

3.9. The Act also requires the Council to have an SRO who is responsible for ensuring compliance with the Act and Code of Guidance and the integrity of the process in place within the authority to acquire communications data.

3.10. Bram Kainth, Executive Director of Place, acts as the SRO for the Council.

3.11. Further details of roles and responsibilities are set out in Appendix 1.

4. NECESSITY AND PROPORTIONALITY

4.1. A local authority is required to show that an interference with an individual's right to privacy is justifiable, to the extent that it is both ***necessary and proportionate***.

Necessity

4.2. Applications to obtain Communications Data should only be made where it is **necessary** for an "applicable **crime purpose**".

4.3. Applications can be made for **'entity data'** where the purpose of obtaining the data is for the **prevention and detection of crime or prevention of disorder.** This definition permits the obtaining of entity data for any crime, irrespective of seriousness or for preventing disorder.

4.4. Applications for **'events data'**, requires a higher threshold, and applications for this data should only be made were the purpose is the 'prevention and detection of **serious crime'** as outlined in section 2.3.2.

The application must explain:

- The crime or event under investigation;
- The person whose data is sought, such as a suspect AND description of how they are linked to the crime;
- The communications data sought, such as a telephone number or IP address, and how this data is related to the person and crime; **and**
- The link between these 3 points to demonstrate it is necessary to obtain communications data.

Proportionality

4.5. All applications for communication data must also demonstrate that the means of obtaining the information is **proportionate** to what it is sought to achieve.

4.6. In effect, any intrusion into individual's privacy should be no more than is absolutely necessary.

4.7. The applicant should demonstrate how they reached the conclusion that the activity is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate (the proverbial 'sledgehammer to crack a nut').

4.8. Applications should contain the following:

- An outline of how obtaining the data will benefit the investigation. The relevance of the data being sought should be explained and anything which might undermine the application;
- The relevance of time periods requested;
- How the level of intrusion is justified against any benefit the data will give to the investigation. This should include consideration of whether less intrusive investigations could be undertaken;
- A consideration of the rights (particularly to privacy and, in relevant cases, freedom of expression) of the individual and a balancing of these rights against the benefit to the investigation;
- Any details of what **collateral intrusion** may occur and how the time periods requested impact on the collateral intrusion, if applicable;
- Where no collateral intrusion will occur, such as when applying for entity data, the absence of collateral intrusion should be noted.

Collateral Intrusion

4.9. As part of this process an assessment should be made of the risk of what is termed '*collateral intrusion'* - intrusion into the privacy of persons other than those that are the subjects of investigation.

4.10. Measures should be taken, wherever possible, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation.

5. DURATION OF AUTHORISATIONS – REVIEW, RENEWAL AND CANCELLATION

5.1. An authorisation will be valid for a maximum of one month from the date of OCDA approval. This means that the conduct authorised should have been commenced or the notice served within that month. All authorisations and notices must relate to the acquisition or disclosure of information for a specific date or period.

5.2. Applications can be renewed before the date on which they would cease to have effect provided they continue to meet the relevant criteria. OCDA approval is required for all renewals. The renewal takes effect on the day on which the authorisation would have expired and continues for a one-month period.

5.3. Renewal may be appropriate where there is a continuing requirement to acquire or obtain data that will or may be generated in the future. The reasoning for seeking renewal should be set out by an applicant in an addendum to the application on which the authorisation or notice being renewed was granted or given.

5.4. A note should be made of the date and time of applications for renewal.

5.5. An Authorisation must be cancelled if at any time after they are given it comes to the Council's notice that it is no longer necessary or proportionate to what was sought to be achieved. The council is under a duty to notify NAFN immediately.

6. RECORD OF AUTHORISATIONS

6.1. Applications, authorisations, copies of notices, and records of the withdrawal and cancellation of authorisations, must be retained in written or electronic form for a minimum of 3 years and ideally 5 years. A record of the date and, when appropriate, the time each notice or authorisation is granted, renewed or cancelled.

6.2. All records are stored and retained by NAFN online for inspection by the Investigatory Powers Tribunal (IPT).

7. HANDLING AND DISCLOSURE OF MATERIALS AND DOCUMENTS

7.1. The ARO should retain IPA related documents for a period of 3 years. However, where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.

7.2. Material obtained or produced during the course of investigations subject to IPA authorisations should be processed, stored and destroyed in accordance with the requirements of the Data Protection Act 2018, the Freedom of Information Act 2000, any other legal requirements, including those of confidentiality, and the Council's policies and procedures currently in force relating to document retention.

7.3. All IPA records, whether in original form or copies must be kept in secure locked storage when not in use.

7.4. All electronic copies of IPA records, as well as the Central RIPA register, must be stored and shared in accordance with point 7.3. and password protected.

7.5. If there is any doubt regarding information handling and confidentiality, advice should be sought from the RIPA Coordinator or Legal Services.

8. ERRORS

8.1. Where any error occurs in the granting of an authorisation, or because of any authorised conduct, a record should be kept.

8.2. Where the error results in communications data being obtained or disclosed incorrectly, a report must be made to the IPC by whoever is responsible for it. E.g. The telecommunications operator must report the error if it resulted from them disclosing data not requested, whereas if the error is because the public authority provided incorrect information, they must report the error. The SRO would be the appropriate person to make the report to the IPC.

8.3. Where an error has occurred before data has been obtained or disclosed incorrectly, a record will be maintained by the public authority. These records must be available for inspection by the IPC.

8.4. A non-exhaustive list of reportable and recordable errors is provided in the Code of Practice.

8.5. There may be rare occasions when communications data is wrongly obtained or disclosed and this amounts to a “serious error”. A serious error is anything that “**caused significant prejudice or harm to the person concerned**” It is insufficient that there has been a breach of a person’s human rights.

8.6. In these cases, the public authority which made the error, or established that the error had been made, must report the error to the SRO and the IPC.

8.7. When an error is reported to the IPC, the IPC may inform the affected individual subject of the data disclosure, who may make a complaint to the IPT. The IPC must be satisfied that the error is a) a serious error AND b) it is in the public interest for the individual concerned to be informed of the error.

8.8. Before deciding if the error is serious or not the IPC will accept submissions from the Public Authority regarding whether it is in the public interest to disclose. For instance, it may not be in the public interest to disclose if to do so would be prejudicial to the prevention and detection of crime.

9. TRAINING

9.1. Officers requesting communication data should have an appropriate accreditation or be otherwise suitably qualified or trained. ARO's will have received training that has been approved by the SRO.

9.2. All training will take place at reasonable intervals to be determined by the SRO, but it is envisaged that an update will usually be necessary following legislative or good practice developments or otherwise every 12 months.

9.3. A log will be kept recording all training received by officers involved in IPA. This training log will be stored alongside the Central RIPA Register.

10. OFFENCES FOR NON-COMPLIANCE WITH IPA

10.1. It is an offence for a person in a public authority knowingly or recklessly to obtain communications data from a telecommunications operator or postal operator without lawful authority (section 11 of IPA 2016).

10.2. The roles and responsibilities laid down for the SRO and SPoC are designed to prevent the knowing or reckless obtaining of communications by a public authority without lawful authorisation. Adherence to the requirements of the Act and the Code, including procedures detailed in this Policy, will mitigate the risk of any offence being committed.

10.3. An offence is not committed if the person obtaining the data can show that they acted in the reasonable belief that they had lawful authority.

10.4. It is not an offence to obtain communications data where it is made publicly or commercially available by a telecommunications/postal operator. In such circumstances the consent of the operator provides the lawful authority. However, public authorities should not require, or invite, any operator to disclose communications data by relying on this exemption.

11. FURTHER GUIDANCE

11.1. This policy must be read in conjunction with current Home Office guidance.

Full Codes of Practice can be found on the Home Office website

https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice

Note the current code is dated November 2018 and will be updated to be fully up to date with changes in legislation.

Legal advice can be obtained from Legal Services, contact:
Janette Mullins, Chief Solicitor (Litigation and Social Care), 0208 753 2744

APPENDIX 1 – ROLES AND RESPONSIBILITIES

Obtaining communications data under the Act involves five roles:

- Applicant;
- Approved rank officer (ARO);
- Single point of contact (SPoC);
- Authorising agency (OCDA); and
- Senior Responsible Officer in a Public Authority (SRO).

Applicant

- A person involved in conducting or assisting an investigation or operation within the Council who makes an application in writing or electronically to obtain communications data.

Approved Rank Officer (ARO)

- A person who is a manager at service level or above within the Council. The ARO's role is to have an awareness of the application made by the Applicant and convey this to the SPoC.

- The ARO does not authorise or approve any element of the application and is not required to be "operationally independent".

- The AROs for the Council are identified in section 3.4. of this Policy and shall be the only officers within the Council who act as an ARO in accordance with the procedures set out in this Policy.

- ARO's must ensure that staff who report to them follow this Policy and do not obtain communication data without first obtaining the relevant authorisations in compliance with this Policy.

- ARO's must have current working knowledge of human rights principles, specifically those of necessity and proportionality.

- ARO's must attend training as directed by the SRO.

Single Point of Contact (SPoC)

- An individual trained to facilitate the lawful obtaining of communications data and effective co-operation between a public authority, the Office for Communications Data Authorisations (OCDA) and telecommunications and postal operators. To

become accredited an individual must complete a course of training appropriate for the role of a SPoC and have been issued the relevant SPoC unique identifier.

- The Council is a member of the National Anti-Fraud Network (NAFN) and use NAFN's shared SPoC service. NAFN is an accredited body for the purpose of providing data and intelligence under the IPA for all public bodies.

Authorising Agency (OCDA)

- The independent body responsible for the authorisation and assessment of all Data Communications applications under the Act.

- They undertake the following roles:
    - Independent assessment of all Data Communications applications;
    - Authorisation of any appropriate applications; and
    - Ensuring accountability of Authorities in the process and safeguarding standards.

Senior Responsible Officer (SRO)

- A person of a senior rank, a manager at service level or above within the Public Authority.

- The SRO is identified at section 3.10 of this Policy responsible for:

    - The integrity of the process in place within the public authority to obtain communications data;
    - Engagement with authorising officers in the Office for Communications Data Authorisations (where relevant);
    - Compliance with Part 3 of the Act and with the Code of Practice, including responsibility for novel or contentious cases;
    - Oversight of the reporting of errors to the IPC and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
    - Ensuring the overall quality of applications submitted to OCDA;
    - Engagement with the IPC"s inspectors during inspections; and
    - Where necessary, oversight of the implementation of post-inspection action plans approved by the IPC.

Head of Community Safety (HoCS)

- The Head of Community Safety will report on the use of IPA to the Hammersmith & Fulham Council Community Safety and Environment Policy

and Accountability Committee annually, and to other panels and committees (where appropriate).

LONDON BOROUGH OF HAMMERSMITH & FULHAM

Report to: Social Inclusion and Community Safety PAC

Date: 24/07/2024

Subject: Annual Performance Report for the Law Enforcement Team

Report author: Mohammed Basith, Law Enforcement Manager

Responsible Director: Neil Thurlow Director of Public Protection

SUMMARY

This report provides PAC with an update following the previous meeting focusing on work of the Law Enforcement Team between December 2023 and May 2024.

There are no decisions required from this report.

RECOMMENDATIONS

For the group to note and comment on the report

Wards Affected: All

Our Values	Summary of how this report aligns to the H&F Values
Building shared prosperity	A cleaner, greener, safer borough increases opportunities for all
Creating a compassionate council	Working with our communities the LET is the front face of the council for many and the service offers help, support, and advice for all ensuring that everyone's problems are addressed
Doing things with residents, not to them	Residents are concerned around environmental crime, ASB and this affects how they feel and perceive the boroughs safety. Residents' safety and perceptions of safety are key attributes that the LET work towards addressing
Being ruthlessly financially efficient	We have brought together several services to create one larger, singular service with a wider parameter of powers
Taking pride in H&F	The LET service work hard to improve the environment of H&F creating a cleaner, greener

	borough
Rising to the challenge of the climate and ecological emergency	The service uses only electric vehicles and the default for staff is to walk with vehicles being used for specific matters only

Background Papers Used in Preparing This Report

None

DETAILED ANALYSIS

Background

1. In February 2024, the Law Enforcement Team (LET) presented performance data and achievements since the formation of the service in April 2021.

2. This report provides service information between 1 December 2023 to 31 May 2024.

3. Since 01 December 2023 to 31 May 2023, the LET has continued to deliver a highly visible front-line service 24/7, and this report provides further details of the work LET officers have undertaken.

Headlines of the LET's work for this period include:

4. Over 47,875 patrols – the service averages 261 patrols per day – with officers working to investigate and resolve service requests, monitor sites following incidents or to inspect locations following referrals for a range of issues from both internal or external partners and teams.

5. For the period of this report the LET team have received 2,914 service requests from residents and businesses, which have been investigated and resolved.

6. Most service requests are resolved without the need for enforcement due to the officer's ability to engage and educate however there are several more complex cases which require constant investigation, monitoring and enforcement activity which can take upwards of 21 to 28 days where legal processes are followed.

7. LET officers issued 870 fixed penalty notices for issues such as fly-tipping, littering and highway obstruction.

8. The Team continues to show a high visibility presence in all the housing estates and parks with 13,142 patrols in housing land, and 5645 patrols in parks. These patrols equate to 5,330 and 3,720 patrol hours respectively.

9. In addition, 11,620 hours of patrols have taken place in all highways and district centres across the borough.

10. Keeping our resident's safe remains a high priority for the Team, and as such, the LET officers have conducted 1,948 weapons sweeps during their patrols resulting in the removal of five knives from the streets. In addition to this, the LET have also recovered drugs, confiscated drug paraphernalia from individuals and on one occasion foiled a burglary from a commercial premises and returned the items to the business.

11. During this period, there were more reports of anti-social behaviour to the service compared to the previous period. There were 370 service requests in the North, 221 in Central, and 167 in South areas. This represents a 57% increase (from 457 last year to 758 this year) in reports to the LET compared to the same period last year. Residents are reporting issues more frequently to the LET and have mentioned that they prefer contacting the LET instead of the police because they feel that the LET responds faster and are more confident in the service as they believe the team can resolve the issues they report.

Service highlights (addresses anonymised where relevant):

12. Theft of, and theft from, motor vehicles:

13. In December and January, the LET supported our police colleagues in monitoring the car crime hotspots. This was part of the wider operation to detect and apprehend individuals who were breaking into cars to steal items in the Ravenscourt ward.

14. The LET worked with the local police team via the tactical tasking and coordination group to collaborate and deploy staff in the late evening and overnight when the incidents were most prevalent.

15. Following the month-long tasking, the issues have subsided considerably, and the LET continue to monitor areas where these concerns have been raised to minimise risk of these issues returning.

Estate ASB issues:

16. The North team and Police have been worked together to tackle an issue emanating from a property in the White city estate - the premises had seen its security measures breached by non-residents. These people were then gaining access to the loft space.

17. Responding to reports overnight – as residents contacted the team - the Night team responded, investigated and the persons present were asked to leave. Following compliance by those present the repairs team undertook works to prevent further access.

18. Those who were present were engaged with and advised how to seek housing support. Referrals were also made to Street Link – the Councils homeless partner – to ensure that they too were aware and were engaged.

19. Once the repairs were completed all residents were engaged and informed to contact the LET 24/7 should there be any further breaches.

20. **Appendix 1** provides further statistical information on service performance for the time of this report.

Updates on action assigned in the February PAC:

21. No actions were assigned.

Broader LET service headline updates:

Housing and homelessness:

22. The LET is actively enforcing issues across the borough with particular emphasis on issues at Housing sites and in parks where ASB and Crime have been reported.

23. Our work with the homeless and street-sleeping communities, along with our partner agencies, is ongoing. Since February, the LET team has been tasked with meeting biweekly to connect with the outreach staff at the mayor's homeless charity and visit various areas across the borough to locate and help street sleepers.

Anti-social behaviour:

24. Following concerns around anti-social use of e-bikes and e-scooters the Councils Community Safety Team, following consultation with residents, introduced a Public Space Protection Order - Thames Path Public Spaces Protection Order (PSPO) | London Borough of Hammersmith & Fulham (lbhf.gov.uk) – the LET, alongside the Met Police, are responsible for enforcing breaches of the PSPO.

25. Over the period of this report three joint operations have been conducted in Bishops Park with the local police team resulting in over a hundred engagements with cyclists and a fine being issued against a cyclist who breached the prohibitions of the PSPO.

Emergency response:

26. The LET continue to support the Council's emergency planning team and assisted with a large-scale evacuation of the residents from the immediate area surrounding the London Oratory School following the arson attack in December.

Violence Against Women and Girls:

27. The safety of all women and girls remains a priority for the Council as we continue to create a safe and equal place for everyone who lives, works, visits and studies in the borough. H&F take a zero-tolerance approach against all

forms of gender-based harassment and abuse, wherever it occurs and are take urgent steps to ensure women and girls feel safe in the borough.

28. To encourage wider participation and feedback for the consultation from the residents and visitors to the borough of the Street Harassment Public Space Protection order, LET officers provided high visibility engagement and reassurance patrols to residents and businesses within H&F's town centres and transport hubs during an eight-night operation, running from 18:00-00:00 every Friday and Saturday throughout December 2023. The patrols focused on night-time economy venues, which were expected to be busy and where there have previously been reports of sexual violence in public spaces. The operation was conducted by up to six identified officers each night during the operation period.

Joint work with the Metropolitan Police:

29. After a tragic suicide in the south of the borough in April, LET officers were first on the scene and helped to cordon off the area and secure it. They worked closely with the emergency response teams to assist in the delicate task of retrieving the individual, who was located at a height. Their collaboration allowed the emergency workers to provide immediate first aid, but despite their best efforts, they were unable to save the person.

30. After a stabbing incident in the northern part of the borough, the LET worked together with the Police immediately. The CSU Gangs team raised concerns about potential tensions in other areas in the southern part of the borough. As a result, the LET was assigned to collaborate with the Police to increase visibility in those areas. Following the joint efforts, no further incidents occurred. As there was no intelligence indicating that the issue would escalate further, the tasking was ended two weeks later.

31. Squatters took over a property in the South of the borough. The Police tasked the LET to monitor it overnight to establish whether it was still occupied. Through our interventions and monitoring, the Police were able to apply for, and obtain, a closure order on the premises. The closure order prevented an unauthorised music event (UME) taking place as, advertising was identified, and it was estimated that over 200 people were due to attend.

32. The LET continues to conduct fortnightly multi-agency operations in various wards across the borough. Invitations are being shared with Tenant and Resident Association leads and ward councillors to ensure they are aware of the work taking place.

Broader matters:

33. Following discussions at a previous PAC around how the LET officers engage with and/or support residents in mental health crisis on the borough we are pleased to confirm that all LET officers undertook mental health training in February 2024. This was done regardless of when officers had previosuly had training and will now form part of our officers annual training programme.

34. LET staff continue to assist with events in the borough. Over this period officers assisted in the marshalling of the FIFA Best awards in February and the Oxford-Cambridge boat race in March. There are more events LET will support with over the summer.

35. **Appendix 2** provides images of some of the above illustrating the LETs work.

Challenges faced by LET Staff

36. At a previous PAC meeting the service was asked whether officers have been affected by aggression whether verbal or physical.

37. The Council, and service, continue to support our staff proving appropiate PPE, training and aftercare to officers should they become a victim of such matters as they go about their duties. The LET continue to deliver the service to the best of their abilities and regularly receive compliments. Such incidents, as above, are thankfully very rare but they are a challenge for officers to undertake their work as they, and we, wish them to.

Service compliments

38. Over is period, LET has achieved several positive outcomes. The following news stories highlight some of these successes:

39. Following a patrol in December LET officers reunited a resident with her lost phone. The Resident commented *"I'd like to thank Abbas and Paulo for finding my phone at Beavor Lane. They're a credit to your unit and an example of what community law enforcement teams should be."*

40. Following the incident in April as highlighted in point 43, the Police Seargent contacted the LET with the following.

"I am the police sergeant who was on scene at the incident where a man fell from the 17th floor of XXXXXX House. I understand that the following officers from your Law Enforcement Team, including Christopher, were present at the scene; ET08, ET149, ET161, ET136, ET142 and ET145

I'd like to take this opportunity to extend my gratitude to all those who were involved, their involvement varied from being the first people on scene, to liaising with the local community and assisting the numerous emergency service personal on scene.

A traumatic incident like this is thankfully not an everyday occurrence, people can react differently or how they feel and react about these things can vary as time goes or are exposed to triggers which brings the memory back. I encourage you to check in on the welfare of your staff.

Please do pass on my thanks, their involvement helped manage and sooth what was an initial chaotic scene, bringing order and calm to the situation".

41. A College Park resident expressed gratitude to the LET for their assistance in handling a situation in February involving a neighbour with mental health issues. The resident wrote a thank-you note stating the following,

42. *“Dear LET, I wanted to express my gratitude to the 3 LET officers who turned up at the scene to support me in College Park, whilst I was suffering harassment from an aggressive and mentally unwell neighbour (who lives at the HMO at XXXXXX Rd) on Thursday 15 February. I had called 999 (on the advice of the neighbor’s Property Managers) at around 3 pm to seek help from both the Police and the Ambulance service. The Police did not arrive until 9 am the next morning (Friday 16th Feb), and by the way, they were very helpful when they did arrive. The Ambulance arrived later on the afternoon of Thurs 16th but were unable to help, mainly it seemed due to miscommunication with the Police. So, with the Emergency Services not being able to offer the help I needed to feel safe and manage the situation or to be able to attend the scene while the harassment was happening, I felt very much indebted to the outstanding skills and empathy shown, in particular, by Honorata Hawrylik and Magda Niedzwiedz. Skills applied not only with me, but also in the way they handled my neighbour who clearly is suffering with mental health problems, on top of his alcoholism. They were both firm and compassionate and quickly defused the situation which might well have escalated out of control.*

    Thank goodness for the Law Enforcement Team and in particular, from my experience on Thursday, to the women in that team.”

43. On 20 February 2024, LET attended SBG Station due to reports of amplified music being played, which was in breach of the PSPO. While on location, the LET officer enforced the PSPO and issued an FPN.

44. Whilst onsite, the LET officers were approached by a group of females stating they were being harassed by a male who was intoxicated. The LET officers approached and spoke to the male, who was verbally aggressive and abusive and smashed a glass bottle on the floor. LET Officers contacted CCTV and requested Police assistance. They waited near the male and diverted pedestrians away from the scene until the Police arrived at the location and arrested the male, as he was also wanted on other charges such as alleged assault and failure to attend court previously.

45. On 26 February 2024 2 Night team LET officers were patrolling at 22:45 around the Fulham Broadway area when they came across three males engaged in what initially appeared to be a fight on Harwood Road junction with Fulham Broadway. As they made their way towards the commotion it became increasingly apparent that it was an attempted robbery in progress. The LET officers immediately contacted CCTV control room and gave the operator a location and a quick description of what was unfolding. While speaking to CCTV, both perpetrators ran away along Harwood Road. The LET officers gave CCTV the direction of travel of the perpetrators and CCTV operator was able to pick them up on camera.

Police officers were informed, and these males were tracked in their vehicle to a local housing block where they were subsequently arrested for robbery, assault, and drink driving.

46. Following intensive work to reduce issues near Goldhawk Road area a resident wrote in May with the following *“The LET have been great and came to update me in person a week or so ago. It does seem to have helped a great deal already, as there's been a decrease in activity, although it hasn't completely stopped (per my 2 emails yesterday). The drug use in broad daylight on a street people walk their kids to school on really is quite shocking. They do seem to be the same faces, so hopefully with a bit more time and a bit more focus we can see this solved”.*

LIST OF APPENDICES

Appendix 1 - LET Performance Data
Appendix 2 - List of LET achievements and other taskings

Appendix 1 LET Performance Data

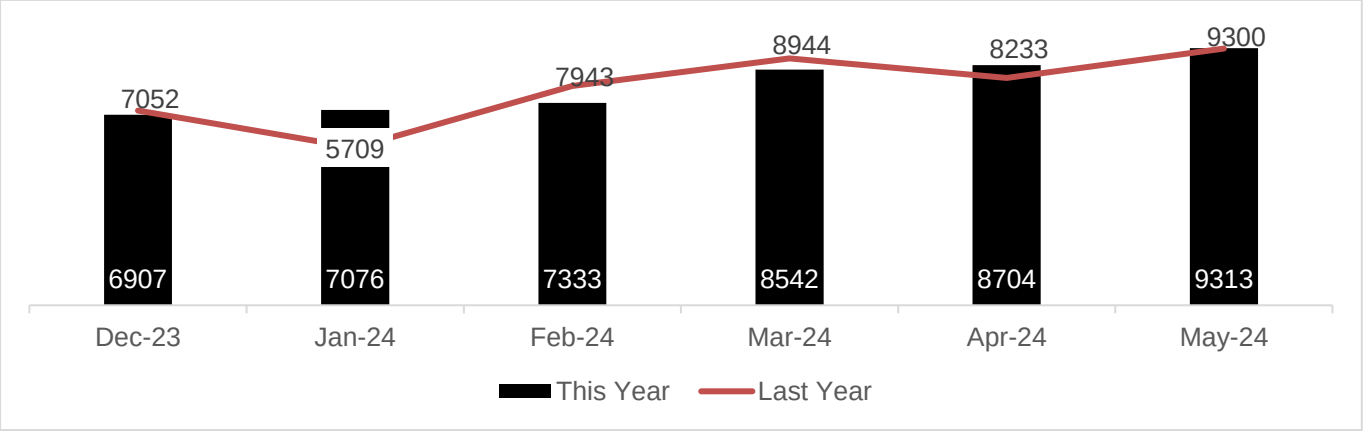
Appendix 1 contains performance data for the LET over the last financial year and for this reporting period with an annual comparison to the same time period 12 months ago.

The table below shows the full data for the financial years 2023 and 2024, as shown in Column A, and the data for the period of this report (December 2023 to May 2024), as shown in Column B.

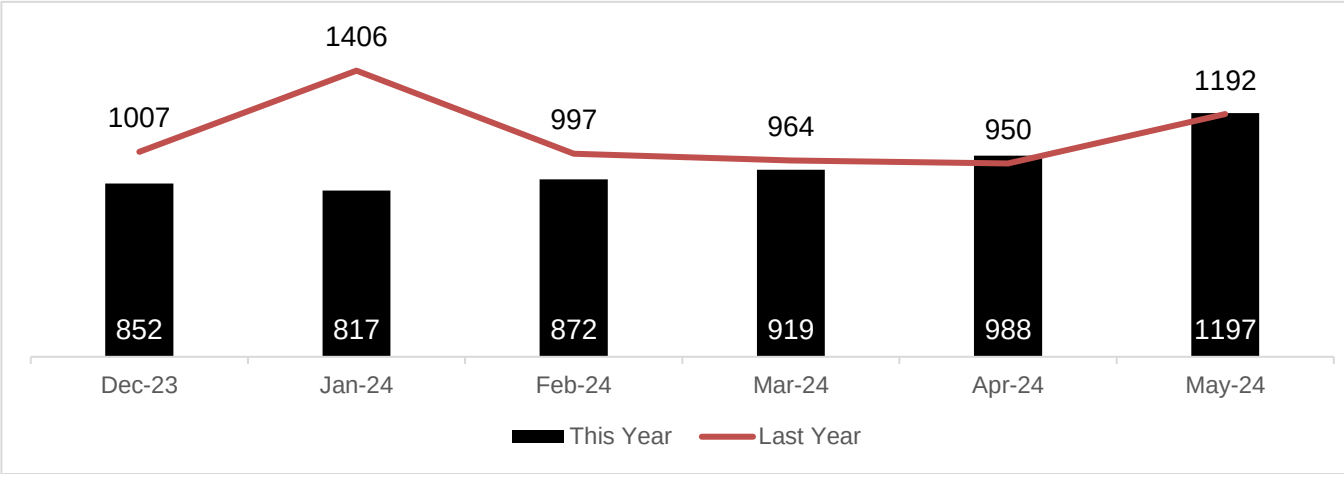
	2023/2024 A	December 2023 to May 2024 B
Total Investigations	5,924	2914
Total FPNs issued	2,054	870
Patrols in HRA estates and/or blocks	27,182	5645
Patrol hours in parks	5,573	3720
Patrol hours in estates and/or blocks	8,045	5330
Patrol hours in public realm	16,915	11620
Weapon sweeps	5,105	1948

For this report and all future ones, the data from sections 1.1 to 2.5 will consistently include data from the corresponding period in the previous year. This approach will provide direct comparison of like for like months allowing for comparible data performance.

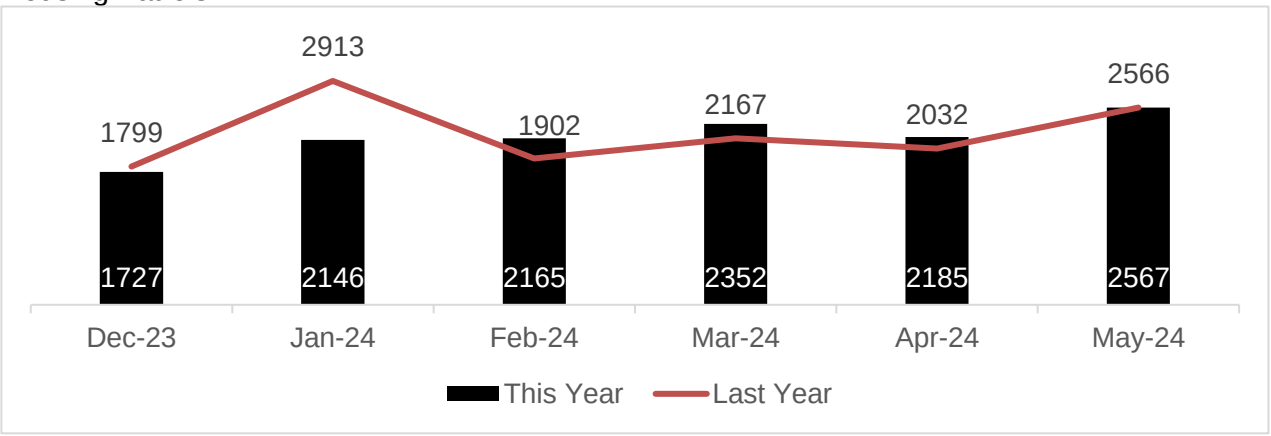
1.1 All LET Patrols



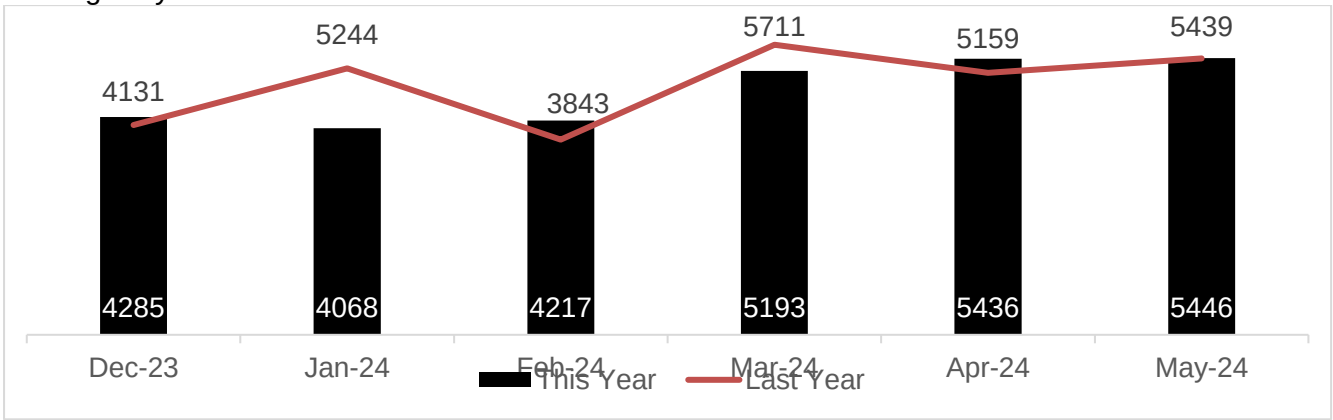
1.2 Park Patrols



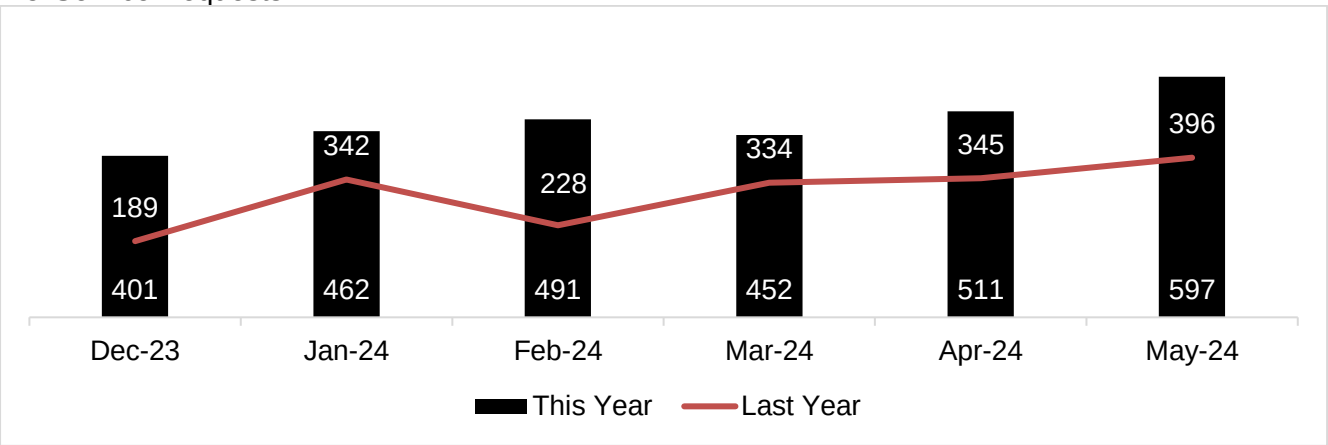
1.3 Housing Patrols



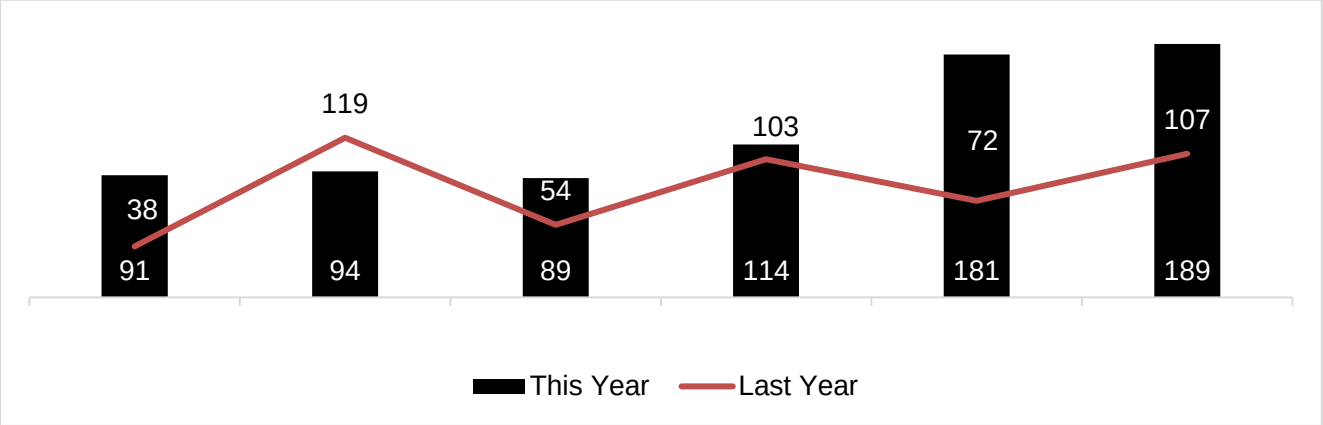
1.4 Highway and District Centre Patrols



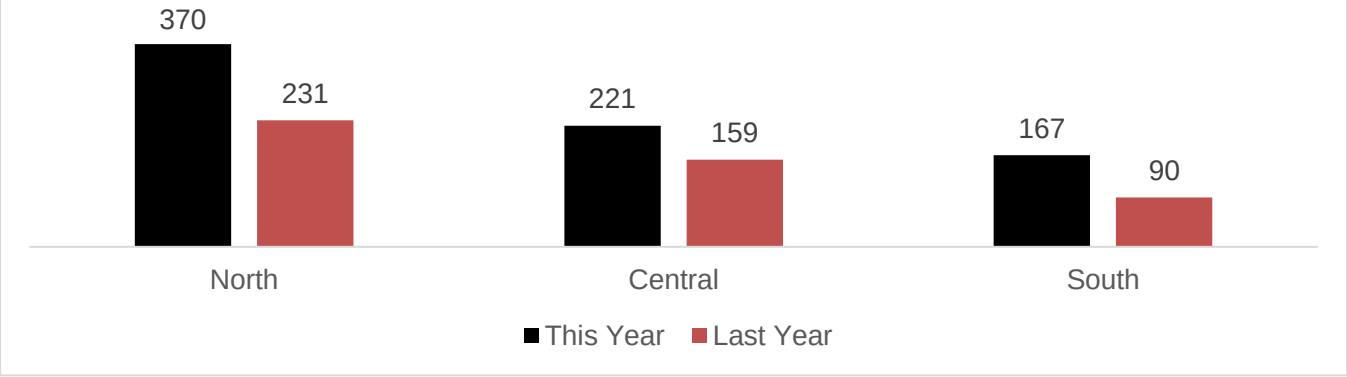
1.5 Service Requests



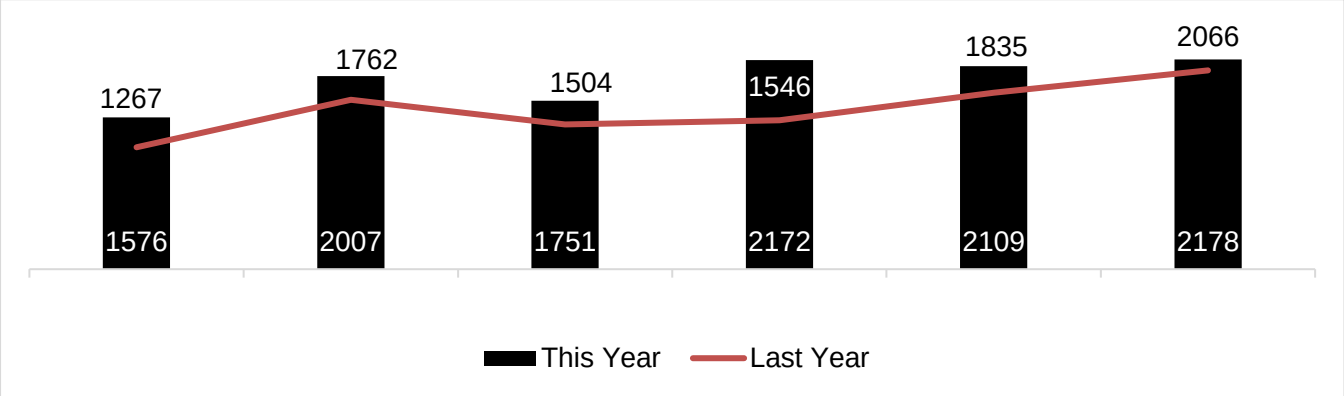
1.6 ASB Service Requests



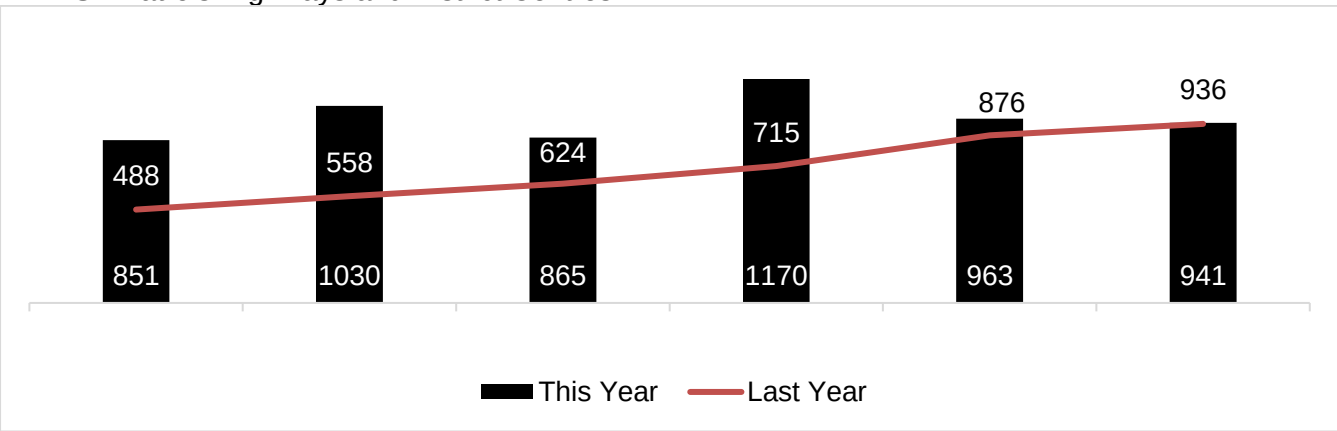
1.6 ASB Service Request by Location



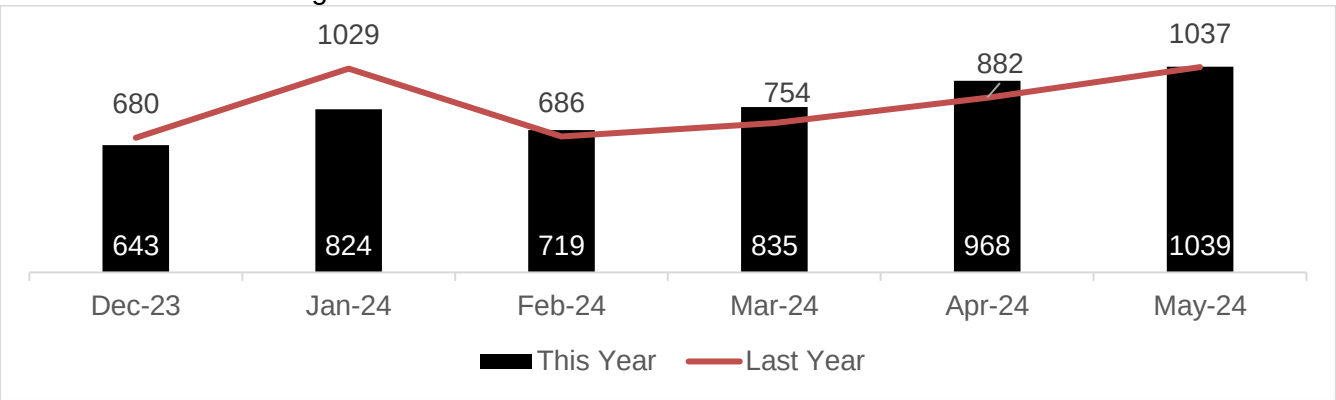
1.6 ASB Targeted Patrols



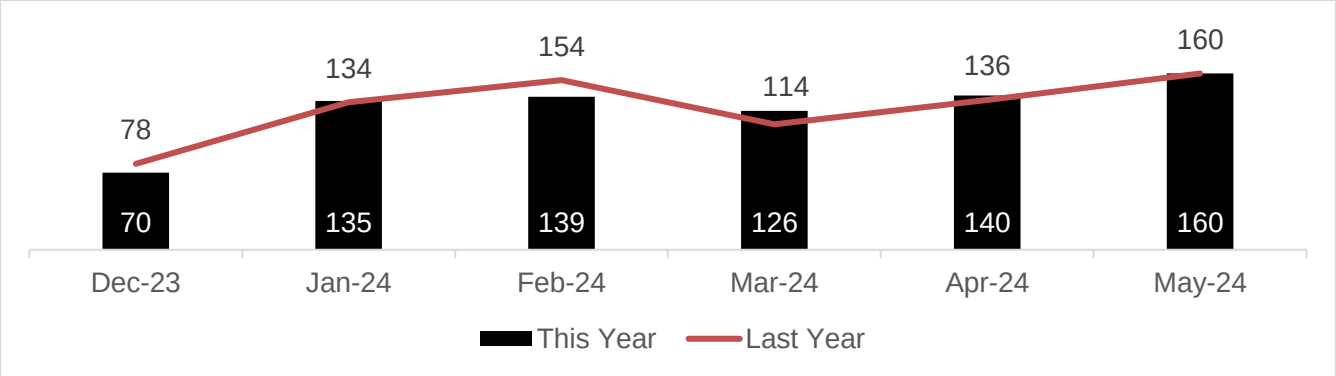
1.7 ASB Patrols Highways and District Centres



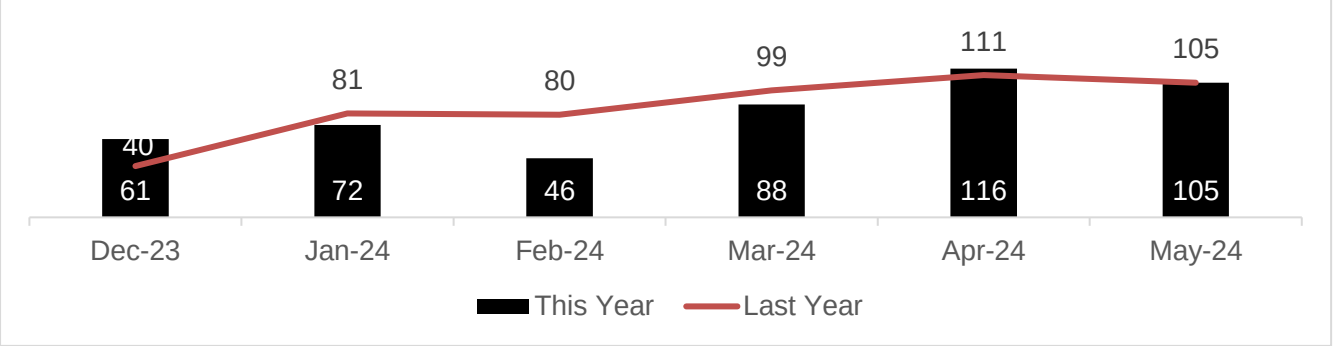
1.8 ASB Patrols Housing



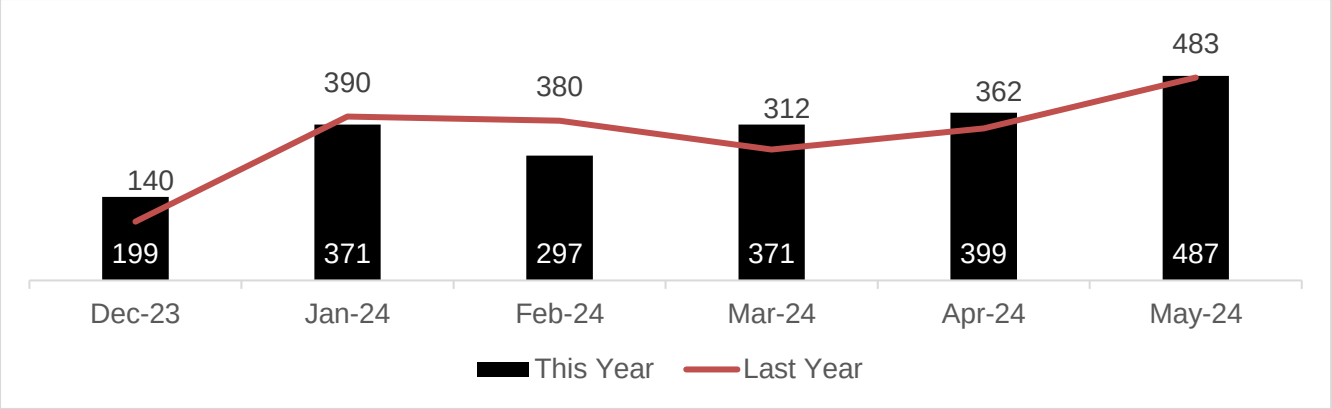
2.0 ASB Patrols Parks



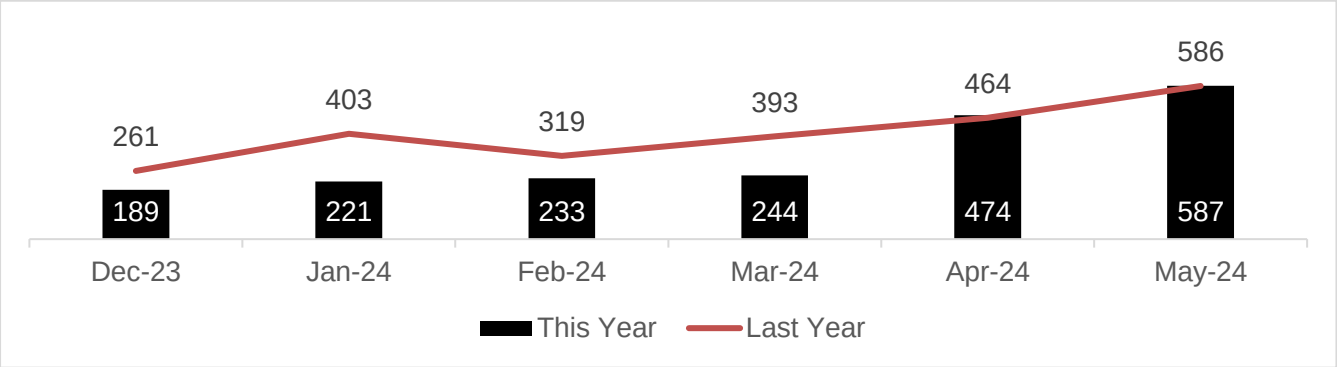
2.1 ASB Drink / Alcohol Monitoring & Interventions



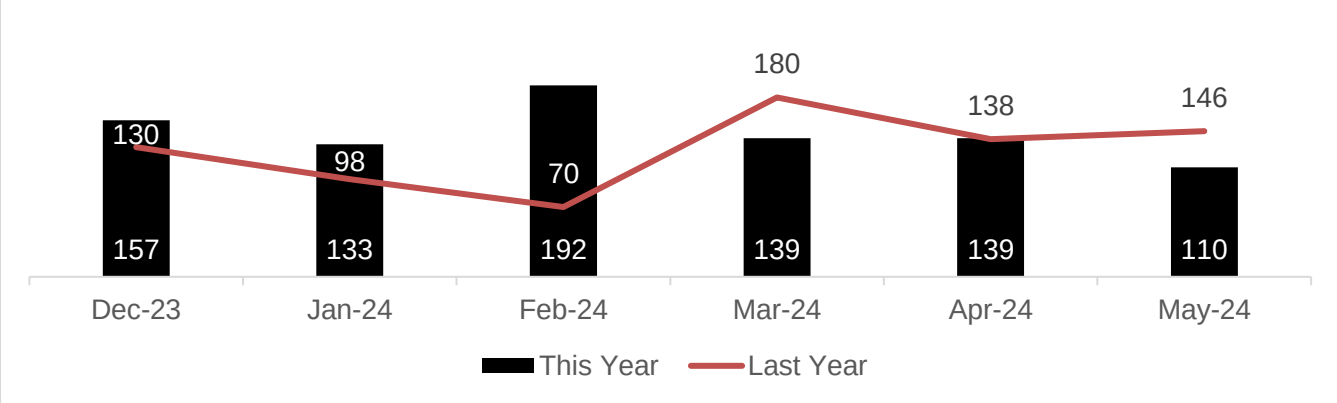
2.2 ASB Drugs Monitoring & Interventions



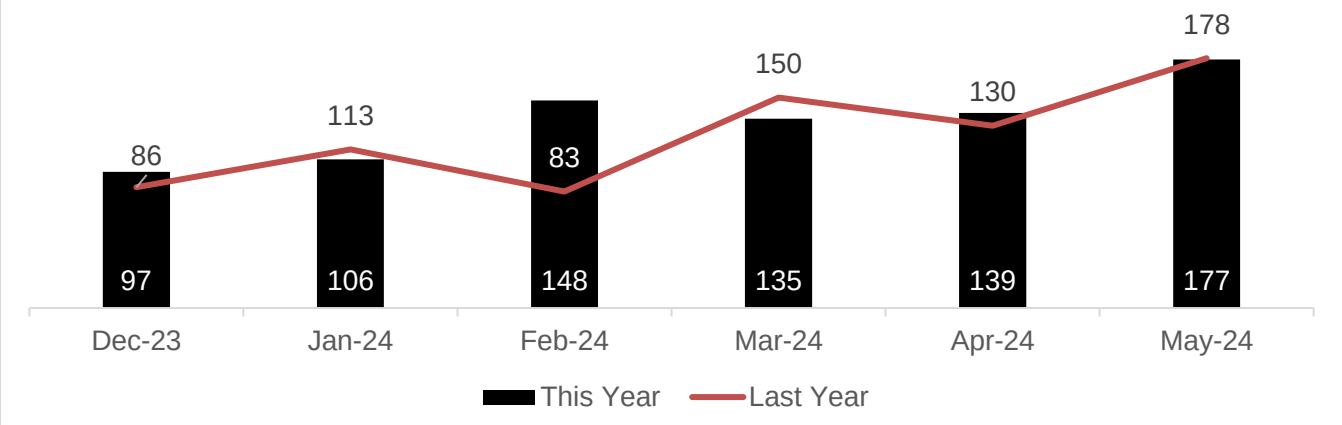
2.3 Weapons Sweeps



2.4 FPN by Month



2.5 Street Population (Engagement/Referral)

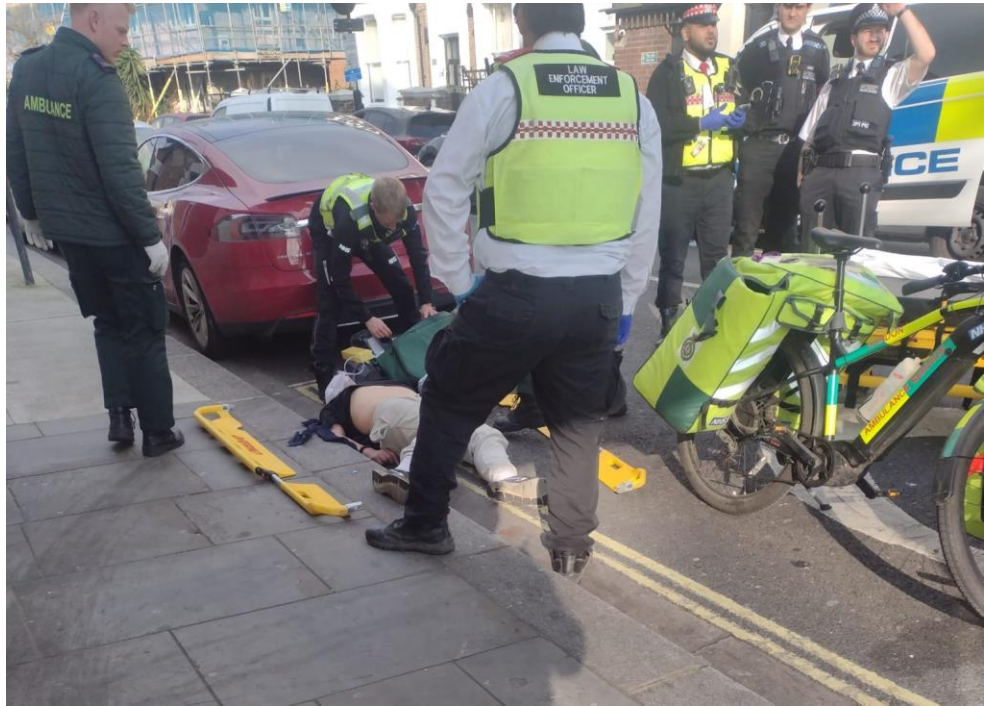



POLICE STAFF
POLICE STAFF
PCSO


ENFORCEMENT
OFFICER


CAUTION
WET FLOOR
20 Feb 2024, 1


4 02:16:42
CCTV IN OPERATION


AMBULANCE
LAW ENFORCEMENT OFFICER


NO DUMPING
CYCLE CRIME
Lock it
or lose it!
WARNING
£80
DO NOT FEED
THE PIGEONS
RUBBISH AND RECYCLING
COLLECTION TIMES


27

INVESTIGATOR'S
POCKET BOOK
h&f
Book serial number
Issued to:
Issued by:
Issue date:
Initials of issuing officer:


LAW ENFORCEMENT TEAM
CCTV
IN OPERATION
LAW ENFORCEMENT TEAM

An example of long term problem solving – the LET ward officers worked with a range of partners to clean up the junction of Wulfsan Street, W12 to create a cleaner, brighter and maintained area for the residents.