London Borough of Hammersmith & Fulham

Community Safety and Environment Policy and Accountability Committee

Agenda

Wednesday 11 November 2020
6.30 pm
Online - Virtual Meeting

MEMBERSHIP

Administration	Opposition
Councillor Bora Kwon (Chair) Councillor Iain Cassidy Councillor David Morton Councillor Ann Rosenberg	Councillor Victoria Brocklebank-Fowler

CONTACT OFFICER: Amrita Gill
Committee Co-ordinator
Governance and Scrutiny
☎: 07776672845
E-mail: amrita.gill@lbhf.gov.uk

THIS MEETING WILL BE HELD REMOTLEY

It will be streamed via YouTube on: https://youtu.be/jjWAECcpHag

To ask a public question about any of the items on the agenda, you will need to register to speak at the meeting.

To do this, please send an email to amrita.gill@lbhf.gov.uk by 12pm on Thursday 5th November 2020

Date Issued: 03 November 2020

London Borough of Hammersmith & Fulham

Community Safety and Environment Policy and Accountability Committee

Agenda

11 November 2020

Item **Pages**

1. APOLOGIES FOR ABSENCE

2. ROLL CALL AND DECLARATIONS OF INTEREST

To confirm attendance, the Chair will perform a roll call. Members will also have the opportunity to declare any interests.

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 Audit, Pensions and Standards Committee.

3. MINUTES 4 - 11

To approve the minutes of the previous meeting and discuss any matters arising.

4. PUBLIC PARTICIPATION

This meeting is being held remotely via Microsoft Teams. If you would like to make a comment or ask a question about any of the items on the agenda, either via Teams or in writing, please contact: amrita.gill@lbhf.gov.uk

5. THE FORMATION OF THE GANGS VIOLENCE AND EXPLOITATION UNIT 12 - 22

This report provides an overview of the of Council's new Gangs Violence and Exploitation Unit.

6. UPDATE ON COUNCIL'S USE OF INVESTIGATORY POWERS (RIPA AND IPA) 23 - 87

This report is to give Members the opportunity to scrutinise the Council's conduct in relation to directed surveillance, covert human intelligence sources (CHIS) and communications data.

London Borough of Hammersmith & Fulham

Community Safety and Environment Policy and Accountability Committee

Minutes

Wednesday 16 September 2020

PRESENT

Committee members: Councillors Bora Kwon (Chair), Iain Cassidy, David Morton, Ann Rosenberg and Victoria Brocklebank-Fowler

Other Councillors: Councillors Wesley Harcourt (Cabinet Member for the Environment), Stephen Cowan (The Leader of the Council), Adronie Alford, Amanda Lloyd-Harris and Andrew Brown

Officers: Ian Hawthorn (AD Environment Special Projects and Highways), Bram Kainth (Chief Officer - Public Realm), Anvar Alizadeh (Group Manager Structures), Matt Hooper (Chief Officer - Safer Neighbourhood), Monica Roucou (Community Action and Engagement Officer)

Guests: Adam Matan, Lorraine Ainscow-Searle, Maria Doulton (Police and Crime Commission) Tim Abbott, Rufus Foster, Joey - Le Gresley (H&F Consultants) David Rowe (TfL) Superintendent Mark Lawrence (Metropolitan Police)

A number of residents also attended to ask public questions on Item 5.

1. APOLOGIES FOR ABSENCE

There were no apologies for absence.

2. ROLL CALL AND DECLARATIONS OF INTEREST

The Chair carried out a roll call to confirm attendance. There were no declarations of interest.

3. MINUTES

RESOLVED
That, the minutes of the meeting held on the 20th July were approved.

4. PUBLIC PARTICIPATION

The Chair noted that the Committee had received a lot of questions and comments on the Hammersmith Bridge item. To address the main concerns in a manageable way, representative questions were chosen to cover the top issues and concerns. The questions and answers can be found under Item 5, Hammersmith Bridge.

5. HAMMERSMITH BRIDGE

Bram Kainth (Chief Officer - Public Realm), provided a presentation on Hammersmith Bridge and noted the following key updates:

- The bridge was closed to pedestrians, cyclists and river traffic on 13th August 2020.
- Sensors positioned throughout the bridge alerted engineers to a rapid increase in the size of dangerous micro-fractures in the cast iron pedestals.
- There had been a significant financial impact of Transport for London's (TfL's) emergency budget and resulted in the £25m existing budget being reduced to £17m.
- TfL were unable to commit to any further resources until the outcome of further negotiations with the government.
- The Leader sent two letters to the Prime Minister, seeking the government's engagement and financial support.
- The secretary of state announced a taskforce to review the engineers plans on 9th September 2020 and the first meeting was held on 16th September 2020.
- Design concept for full stabilisation and strengthening were being finalised and this would cost £46m.
- The Council was also exploring detailed design options for a temporary bridge for pedestrians and cyclists and this could take up to 9 months, costing £27m.
- Full restoration and strengthening, including stabilisation works would cost £141m and up to £163m for a quicker option.
- The Council was exploring a number of proposals for a ferry service.
- The Council had requested TfL to put on extra bus services on routes 533 and 378 to address school transport concerns.
- TfL were also exploring a point to point coach services for school children.
- Alternative walking and cycling routes had been identified by Council officers and measures on how to improve these routes were being explored.
- A temporary road bridge proposal was assessed by TfL in November 2019; however, this was rejected due to key reasons highlighted in the presentation.
- It was noted that immediate urgent stabilisation measures were being developed to reopen the bridge to pedestrians, cyclists and river traffic.

Councillor Stephen Cowan (The Leader of the Council) addressed the committee and gave an update on the work of the taskforce. The first

taskforce meeting was held on 16th September 2020 to review the engineer's reports. The taskforce was Chaired by Baroness Vere of Norbiton and included representatives from the Council, TfL, the London Borough of Richmond Upon Thames, Network Rail and the Department for Transport The Leader provided details of the discussions that were had at the taskforce meeting and noted that everyone involved in the taskforce was keen to open a safe fully functioning bridge to pedestrians, cyclists and motor vehicles as soon as possible. The Council would to go to tender with TfL when assurances on finances were provided by the government.

The Leader stressed the urgent need for short term mitigating actions and noted that he wrote to Baroness Vere on the 15th September 2020 setting out some of the main challenges faced by members of the public due to the closure of the bridge. The Council was working closely with the taskforce on proposals for short term alternatives which included a ferry service or a temporary road crossing.

The Chair explained that she had received some written questions from members of the public in advance of the meeting and speakers would also be invited to ask a question or make a comment to address the main areas of concerns as follows:

Q1: Can officers address if an emergency bridge or temporary crossing is planned and if so, what the timeline for implementation is?

In response the Chair explained that during the meeting we had heard about the various options for a temporary crossing therefore this question had already been addressed. She asked officers to outline the different options that were being explored for an emergency bridge or a temporary crossing, including timelines and requested that this be published as soon as possible.

Action: Bram Kainth

Q2*: I am a resident of Hammersmith and Fulham and have children who go to school on the other side of the river, and their commuting time has gone up significantly by bike each time they need to get across. We are very concerned that they will not be able to continue to get across by bike once it starts getting dark earlier due to security concerns. Does the Council have a viable solution within the next few weeks?*

In response Bram Kainth (Chief Officer - Public Realm), noted that the Council sympathised with all members of the public who were adversely affected by the closure of the bridge. He explained that the bridge was closed for the safety of the public and this remained the Council's top priority. To ensure that these concerns were mitigated in the short term, officers had requested a full audit on all the alternative pedestrian and cycle routes so lighting along these could be improved.

The Leader apologised for the level of disruption caused by the closure of the bridge. The Council was working with the taskforce to explore a number of options and find an immediate solution by the time the days got shorter. This would be addressed as one of the key priorities at the next taskforce meeting

and further details of the Council's plans should be available to members of the public in the coming weeks.

Q3: Many residents raised concerns over the safety of the alternate cycling and walking routes that people are now taking. There were concerns about insufficient lighting of these routes – particularly as the days are getting shorter, the dangers of increased traffic, and winter weather conditions. Are there plans to address these issues and are there plans for an alternative, safe pedestrian crossing?

In response Bram Kainth (Chief Officer - Public Realm) explained that this question had already been addressed in the response to the previous question. The concerns relating to the safety of the alternative routes would be passed on to the engineers as a priority.

Councillor Victoria Brocklebank-Fowler felt that the Beckett Rankine proposal to construct a temporary bridge adjacent to Hammersmith Bridge to allow motorised traffic to cross the River Thames until the main structure could be restored was the most popular option amongst residents locally. She asked why this had not gone ahead. Bram Kainth, referring back to the presentation provided the key reasons why the Beckett Rankine proposal had been rejected by TfL in October/November 2019.

Q4: Why is a temporary ferry service which can be organised within days not in place?

Bram Kainth (Chief Officer - Public Realm) reiterated that whilst the Council was looking at various options outlined in the presentation to address the concerns expressed, the Council's number one priority remained the safety of the public. He explained that options for a ferry service were actively being explored. The decision, whether to proceed with a ferry service would be taken by the taskforce within the coming weeks.

The Leader apologised to the members of the public for all the issues they were currently experiencing. He felt that a ferry service was the most appropriate short-term solution and noted that there was a broad consensus at the taskforce meeting that this was a priority and needed to be addressed urgently.

Q5: The existing bridge should be urgently and as cost effectively as possible replaced with a modern one with the existing facade perhaps attached to retain something of the history of the bridge.

In response the Leader explained that the costs and timescales for building a new bridge were similar to restoring the existing bridge. In addition, it was concluded by engineers at the initial taskforce meeting that the bridge could be fully restored. The Council's primary responsibility was to restore the existing bridge so that it was fit for purpose. However, options for a modern bridge had also been explored. These discussions would continue with the taskforce to find the quickest and most effective solution for the members of the public.

Q6: My son's school journey has doubled in time and we're really feeling the impact of the closure of the bridge. How can we as members of the public feel confident that this will be resolved urgently?

The Leader explained that one of the key objectives of the taskforce related to the urgency of developing a plan to safely reopen the bridge to the members of the public. One of the key challenges for the Council was to identify funding to restore the bridge. However, since the intervention of the Prime Minister, the Council welcomed the Government's full engagement to help move this forward. In addition, formal meetings with the taskforce would take place on a weekly basis. Reassurances were provided that the engineers would be reviewing the lighting along the alternative routes as a matter of urgency.

Q7: Can the Council publish the recent engineers reports and associated correspondence, given that so much about the bridge construction is already in the public domain?

Bram Kainth (Chief Officer - Public Realm) noted that the engineer's reports had not been released to the public for security reasons inline with TfL's policy. The Leader added that all the technical information had been shared with the relevant authorities and the government.

Councillor Victoria Brocklebank-Fowler noted the impact the closure of the bridge had on the residents of the borough and queried whether active steps had been taken to offer acknowledgement of the current situation. In response the Leader confirmed that a letter had been sent to all residents on the 16th September 2020 apologising about the inconvenience, the of the bridge had caused to many residents in the borough.

Councillor Iain Cassidy asked for further clarification to be provided as to why the Beckett Rankine proposals were not taken forward by TfL. Bram Kainth provided a detailed overview of the various challenges faced by the implementation of these proposals and outlined the technical reasons why these had not been successful.

Councillor Ann Rosenberg asked if a structural survey was commissioned by the Cabinet responsible between 2010-2014. Councillor Andrew Brown explained that the administration at the time continually assessed the condition of the bridge. However, at the time there were no serious concerns discovered regarding the structural integrity of the bridge.

Councillor Andrew Brown thanked all the officers for their hard work towards the actions taken to date for the interest of public safety. He sympathised with the significant impact the closure of the bridge had on the lives of many local residents in 2019 for motorised vehicles and 2020 for pedestrians and cyclists.

Councillor Andrew Brown requested detailed timelines of the studies and investigations that had been commissioned by the Council, included in the Leader's letter to local residents on 16th September 2020.

Action: Bram Kainth

RESOLVED:
That, the Committee noted and commented on this item.

6. POLICE AND CRIME COMMISSION REPORT

Matt Hooper (Chief Officer - Safer Neighbourhood) provided a presentation on the Policing and Crime Commission's (PCC's) final recommendations. It was noted that the Commission was created in November 2018. Since then, members of the Commission had undertaken a huge amount of field work, interviews and research to inform their final report. The report set out 35 'ambitious recommendations, each one evidence-led and designed to make residents safer, less fearful and better informed'. The report served as a resource and benchmark and included 7 headline recommendations as follows:

1. Crime communication infrastructure
2. A new H&F crime helpline
3. Disbanding existing resident engagement structures
4. New recommended groups, committee and roles
5. Prioritise pupil safety
6. New H&F youth commission
7. Addressing drug and alcohol misuse

In total 33 actions were proposed for the Council, Metropolitan Police and other organisations. 18 of these were supported, 12 were partially supported and 3 were not supported. The 3 actions that were not supported for either legislative or financial reasons were; a new H&F crime helpline, disbanding existing resident engagement structures and addressing drug and alcohol misuse.

Superintendent Mark Lawrence, relating to recommendation 3, noted that Ward Panels were functioning across the borough, some more well attended and more productive than others, but these cannot be disbanded. These were driven by The Mayor's Office for Policing and Crime (MOPAC) and the central Neighbourhood Unit. Again, representation could always be increased, and everyone was welcome to join. It was crucial to deliver a consistent engagement strategy across London and Ward Panels formed part of that. However, the Metropolitan Police Service (MPS) recognised the validity and importance of the Ward Action Groups recommended in this report and made a commitment to ensure Ward Panels and Ward Action Groups work together to achieve the best outcomes.

Councillor Sue Fennimore (Deputy Leader) praised the sheer amount of work that had gone into the PCC. She thanked everyone that was involved in the Commission to bring forward these recommendations for an important and invaluable piece of work.

The Chair also thanked the members of the Commission for taking their time to address the Committee.

Councillor Victoria Brocklebank-Fowler asked Councillor Sue Fennimore to clarify what her views were on the recommendations included in the report. In response Councillor Sue Fennimore noted that she was grateful for all the work carried out by the Commission to produce these recommendations. All recommendations would be presented at Cabinet for consideration in November 2020 at which point it would be collectively determined which ones would be taken forward.

Councillor Victoria Brocklebank-Fowler asked for further clarification to be provided on whether Council officers were involved in responding to the recommendations. In response Matt Hooper noted that the Council worked in collaboration with the Police to jointly agree and respond to the recommendations proposed by the independent Commission.

Lorraine Ainscow-Searle (Police and Crime Commission) asked why the recommendation to consider working with the Police to adopt a diversion scheme for drug users such as that operating in Thames Valley was not supported. Matt Hooper explained that this was a significant programme of work which due to current resource and funding restrictions, the Council was not in a position to deliver at this time. However, the Council had agreed to extend the funding for the resilience project, and this would be made available post 2021.

Councillor Victoria Brocklebank-Fowler provided a summary of concerns regarding the arrangements for Ward Panels and the Ward Action Groups set up across the borough. However, noted that she was in favour of some of the other recommendations outlined in the report.

Councillor David Morton commented that he was the Chair for the Ward Action Group in Avonmore and Brook Green. He felt that these had worked extremely successfully and there was good integration between Council officers, Police and the Safer Neighbourhood team. Additionally, he provided a summary of the improvements that could be made in future to ensure these continued to work well.

Adam Matan (Police and Crime Commission) noted that the Commission had worked very closely with residents and key stakeholders to collate their views and action some of the challenges that were faced in the borough. He was pleased with the recommendations that had been submitted to the Council and hoped that these were implemented to achieve a practical solution for crime going forward.

Summing up the discussions, the Chair thanked everyone in attendance for their contributions, and efforts that had gone into developing the proposed recommendations

RESOLVED:
That, the Committed noted the recommendations of the Policing and Crime Commission (PCC) and the H&F officer responses.

Meeting started: 6:30pm
Meeting ended: 9:30pm

Chair .....

Contact officer: Amrita Gill
Committee Co-ordinator
Governance and Scrutiny
☎: 07776672845
E-mail: amrita.gill@lbhf.gov.uk

London Borough of Hammersmith & Fulham

Report to: Community Safety & Environment Policy & Accountability Committee

Date: 11/11/2020

Subject: The formation of the Gangs Violence and Exploitation Unit (GVEU)

Report of: Gideon Springer -Strategic Lead for Safer Streets

Summary

This report provides an overview of the of LBHF's new Gangs Violence and Exploitation Unit. It outlines our progress with resourcing the team, the developing operating model and the work we intend to undertake within the wider council and strategic partnerships to reduce the harm caused to our young people who are at risk from gangs, violence and other forms of exploitation.

In order to do this effectively there is a need to look holistically at the way we deal with vulnerable young people. This approach will also include the involvement of those within Children's Services, Housing, the Voluntary Sector and employment to provide a better future for our young people.

Recommendations

1. For the Committee to note and comment on the report.

Wards Affected: All

H&F Priorities

Please state how the subject of the report relates to our priorities – delete those priorities which are not appropriate

Our Priorities	Summary of how this report aligns to the H&F Priorities
• Building shared prosperity	*Supporting vulnerable young people away from gangs, violence and exploitation, back into education and employment.*
• Creating a compassionate council	Providing a service that intervenes, to improve the lives of the most vulnerable young people in the borough.
• Doing things with local residents, not to them	Working with communities to enable them to support vulnerable young people

Hammersmith & Fulham Council

Contact Officer(s):

Name: Matthew Hooper
Position: Chief Officer - Safer Neighbourhoods & Regulatory Services
Environment Department
Telephone020 8753 5809
07450 964 681
Email: matthew.hooper@lbhf.gov.uk

Background Papers Used in Preparing This Report

None.

---

1. Proposed Outcomes

As part of earlier corporate discussions relating to gangs, youth violence and exploitation the following outcomes framework was proposed as an approach to help organise our workstreams. The work of the new Gangs Violence and Exploitation Unit will fall mostly into the 'Protection' outcome: But will aim to work in partnership to address the other five outcomes outlined below:

1.1 Participation
Our communities particularly our young people, are engaged and active in designing young people's services

1.2 Community Support
Communities and families are well supported to tackle issues of exploitation and know where to look for help

1.3 Prevention
Our young people are provided with the best youth services in London which encourage positive activities and appeal to all

1.4 Early Intervention
All LBHF service provision is trauma informed and targeted at dealing with vulnerabilities early to reduce the impact of adverse experiences on our young people

1.5 Protection
We will use all available legislation to ensure our communities are protected from criminal behaviour

1.6 Community Resilience
Working with communities and the third sector to build an anti-violence culture

2. Performance Measures

The headline performance measures are proposed as follows:

2.1 Key Performance Indicators

- To reduce the number of violent crimes committed by young people;
- To reduce the number and seriousness of injuries caused by youth violence;
- To reduce the number of robberies and drug related offences committed by young people;

Once the team is fully in place, we will look at the previous levels of these offences with a view to setting clear targets, however the effect of the pandemic on all levels of crime and its continuing impact, will make it difficult to calculate smart targets in these areas at the current time with the pandemic second wave restrictions and possible further lock downs.

2.2 Qualitative Measures

- To identify, disrupt and enforce against specific gangs that operate in H&F;
- To identify and respond to young people 'associated' with gangs;
- To provide safe routes out of gang association;
- To identify and respond to the needs of females associated with youth violence;
- To establish and maintain a longer-term sustainable framework based on early intervention, disruption and prevention to ensure that young people involved in low level criminality are successfully diverted from more serious crime
- To provide support for victims.
- To provide support for the families of those exploited into gang activities.

3. The Experience of Vulnerable Young People Within Hammersmith and Fulham

Some young people in the borough (and nationally) have been conscripted into gangs and gang culture by organised crime leaders. It is our duty to safeguard young people from this and prevent others from being drawn into this form of criminal activity. We also need to ensure that those who are the perpetrators of this form of exploitation are brought to justice.

Our number one priority is to keep people safe and our residents need to know that we are doing everything in our power to prevent their children and young people being victimised and exploited by those involved in organised crime. In order to address these issues we have created the borough’s first ever dedicated unit to tackle gangs, violence and exploitation.

In addition to the very real harms caused by gang activity, fear of crime and gangs is pervasive and something which must be tackled. We will be tough on gangs, but as a compassionate council, we will also be tough on the causes of gangs, which means addressing the underlying issues.

This will involve a significant amount of joint working at a senior level to ensure that Hammersmith & Fulham develops leading practice in relation to establishing new early intervention approaches, improving case management and bringing about reductions in the number of young people involved in violent incidents.

4. The Gangs Violence and Exploitation Unit (GVEU)

The Leader of the council was instrumental in developing this ground-breaking agreement between the Council and the Metropolitan Police. Hammersmith and Fulham will fund Police Officers to work together with specialist council staff to bring the full weight of criminal legislation to bear on gangs and gang leaders operating in the borough. Whilst at the same time delivering greater initiatives to engage with and divert vulnerable young people away from gangs, violence and exploitation.

This new dedicated Unit will consist of 11 LBHF employed officers and 6 Metropolitan Police Officers (17 FTEs). The total annual cost of the unit is £983,000.

The GVEU will lead a strategic portfolio of work to deliver Hammersmith & Fulham's approach to supporting young people out of gangs, violence and exploitation. This will involve a significant amount of joint working at a senior level to ensure that Hammersmith & Fulham develops leading practice in relation to establishing new early intervention approaches, improving case management and bringing about reductions in the number of young people involved in violent incidents.

5. Progress in establishing the Gangs Violence and Exploitation Unit.

Approval for the recruitment to the GVEU was received in June 2020, interviews were held on 25th & 26th August. We have now recruited the Team Leader and 3 of the 4 Gangs Workers. They took up their posts in mid September 2020 when the GVEU became operational. The final Gangs Worker post has been offered to a candidate and they are in the process of being recruited.

The next phase of recruitment for the 4 ASB Coordinators is currently underway, interviews are taking place late October and early November. This will be followed by the final stage to recruit the Researcher and Analyst Posts in November.

Police have identified 4 officers to work in the GVEU and 2 officers who will work alongside them but focus on operational delivery with the Youth Offending Team. The contract for these posts has now been agreed with the Metropolitan Police.

Office space for the GVEU has been identified within 145 Kings Street and this will form the physical base for the team. The team will start to carry out business critical work in the Borough in the first week of November.

The terms of reference and operating procedures for the team are being developed through stakeholder consultation and a series of workshops. It is envisaged that the team will operate alongside the Youth Offending Team and Family Assist to identify vulnerable young people who do not yet reach the threshold for statutory intervention but are nevertheless at risk from gangs, violence or exploitation.

By intervening with these children at an early stage, the GVEU will be able to work with them, their and third sector providers to divert them away from risky behaviour. GVEU Officers will utilise some of the services already available within the Borough but will also work in a different way with the community to support vulnerable young people and develop different approaches.

6. Operating Model

Framework

- The GVEU We will work in conjunction with all departments within the Council and does not replace any of the existing services. The police are part of the GVEU and will be co-located in 145 King Street
- Every vulnerable young person referred to or identified by the Unit will be evaluated in relation to the level of risk and given a RAG status. Progress with that young person will be monitored via monthly multi-agency casework conferences.
- If GVEU in conjunction with other agencies feel that risk / criminal activity is increasing (change in RAG status) a multi-agency decision will be made about who is best placed to work with the young person.
- GVEU workers will work with a broad range of cases – this could be the most high-risk or young people that are coming to the attention of the CJS but who are not currently engaged by any statutory agency. The ultimate aim will be to support the young person into education, employment, training, and any other pathways likely to work for that individual.
- We will work with social landlords when young people are coming to their attention due to GVE issues and work with them around enforcement and support.
- When our efforts to support and divert a young person have not been successful and all options have been exhausted, we will consider all enforcement options such as tenancy action, injunctions, Closure Orders etc. This work will be carried out in conjunction with the police and relevant agencies will be consulted. Enforcement action does not mean that support will be withdrawn.
- We will have an analyst and business support role to assist the unit. The analytical work will be crucial to developing the work of the unit and informing us where we need to focus our work.

Other deliverables:

- The GVEU will look to operate a duty service similar to other operational areas of the council where the mailbox and phone line are staffed
- We will develop online reporting tools similar to ASB and hate crime whereby a family / person can refer to us about concerns they may have about GVE issues so they can seek assistance. We will work with Children's / Family Services re: any safeguarding concerns and we can signpost the family / person / offer support. Additionally, there will be a reporting tool for people to report issues of concern around gangs, violence and exploitation. We will make it clear this should be reported to the police if an emergency and give

details of services available. This will help to develop the local intelligence picture around this area of work.

- We will publicise the GVEU via LBHF's social media.
- Where there is an intelligence picture being built of areas requiring outreach work due to congregation / ASB, the GVEU will deliver outreach work in these areas with the assistance of our partners - police, CCTV, NWS and Parks police
- The GVEU will work with the community via community groups, faith groups and TRA's to build on existing relationships and develop new ones. This will be for the purposes of encouraging families / young people to seek advice support and developing intelligence
- Developing the Council's response with our internal / external partners to our young people who are involved in County Lines activity – developing intelligence, response and assistance.
- We will be a part of the consultation meetings that have been developed for practitioners to seek assistance around GVE concerns and this will be done on a rotational basis by the GVEU workers.

7. Statistical Information

Appendix 1 below sets out some of the critical statistical information that sets the borough context for the GVEU in relation to the following three core factors: (1) first time entrants to the criminal justice system, (2) re-offending data, (3) the recommendations of the Lammy Review and data on disproportionality within the youth offending cohort in H&F.

Appendix 1

1. First Time Entrants into the Criminal Justice System

Historically, Hammersmith and Fulham Borough has seen higher rates of first time entrants into the Criminal Justice System than the National Average and the London Average.

However, this rate now lies below both the London average of 264 per 100,00 and the National average of 215 per 100,00 of local 10-17-year olds. The actual number of FTE's dropped by 2 from 31 to 29 (rounded).

Hammersmith and Fulham remain favourably at 4th place in our YOT 'family' for 2018/19 FTEs.

However as can be seen from the below charts Hammersmith and Fulham still have considerable challenges when it comes to Children and Young People sentenced to custody and Children and Young Peoples reoffending rates which remain higher than all those in our YOT family.

2. Children and young people sentenced to custody

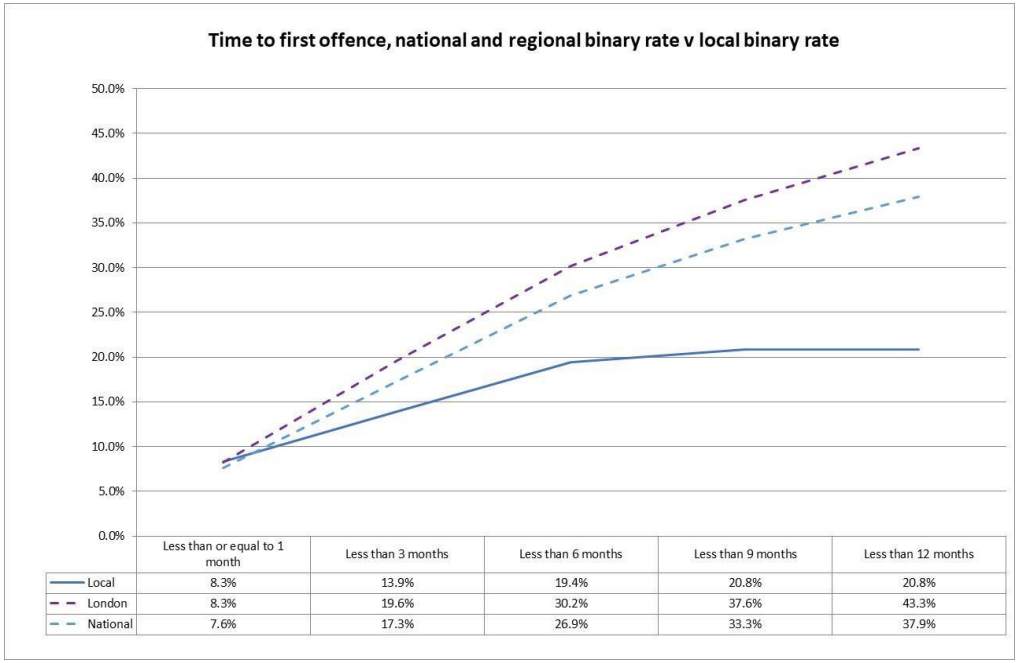
	Use of Custody - Baseline Apr 18 - Mar 19			Use of Custody - Latest Data Apr 19 - Mar 20		
	Number	**2018 Population**	**Rate per 1,000**	**Number**	**2018 Population**	**Rate per 1,000**
Hammersmith and Fulham	**7**	**14,086**	**0.50**	**11**	**14,086**	**0.78**
New YOT Family						
Camden	7	21,377	0.33	1	21,377	0.05
Wandsworth	3	22,363	0.13	1	22,363	0.04
Westminster	5	19,014	0.26	3	19,014	0.16
Islington	23	16,616	1.38	6	16,616	0.36
Kensington and Chelsea	5	11,706	0.43	2	11,706	0.17
Haringey	10	24,826	0.40	N/A	24,826	-
Greenwich	17	26,380	0.64	13	26,380	0.49
Southwark	8	24,912	0.32	9	24,912	0.36
Manchester	54	47,861	1.13	31	47,861	0.65
Merton	1	17,948	0.06	4	17,948	0.22
Family Average	**13**	**23,300**	**0.57**	**8**	**23,300**	**0.33**

3. Hammersmith and Fulham's Reoffending Data:

Apr 17 - Mar 18

	Reoffences per reoffender	Reoffences per offender	% Reoffending
Hammersmith and Fulham	**4.45**	**2.28**	**51.4%**
Camden	3.89	1.66	42.7
Wandsworth	3.67	1.64	44.7
Westminster	3.49	1.42	40.7
Islington	4.23	1.99	47.1
Kensington and Chelsea	2.61	0.85	32.7
Haringey	3.31	1.35	40.9
Greenwich	2.93	1.10	37.6
Southwark	4.36	2.02	46.3
Manchester	4.78	1.75	36.7
Merton	3.41	1.55	45.5
Family Average	**3.87**	**1.60**	**41.4**

Live Reoffending Data April 19-Mar 20



Hammersmith and Fulham data for the 12-month cohort Apr17-Mar18 shows the proportion of reoffenders increasing on the previous year, up from 46.7% to 51.4%. Hammersmith has the highest reoffending rate within its YOT family, and the rate lies above the London average 41.9% and the National average 38.4%.

Live reoffending data for the Apr19-Mar20 cohort has moved from 12.9% to 20.8% reoffenders since last quarter. From the current cohort total of 72 young people, 15 have reoffended (offences proven), while 6 more have offences pending which if all proven would increase the binary rate to 29.2%. Live reoffending data for 2019-20 is showing this rate as tracking below London and national rates, however this rate will not be finalised until January 2022

4. The Lammy Review

David Lammy MP published his final review into the treatment of, and outcomes for, Black, Asian and Minority Ethnic (BAME) individuals in the CJS in September 2017. H&F Youth Offending Service (YOS) contributed to this review.

The review aimed to 'make recommendations for improvement with the ultimate aim of reducing the proportion of BAME offenders in the criminal justice system' and covered the role of the CPS, courts system, prisons and young offenders institutions, the Parole Board, the Probation Service and Youth Offending Teams (YOTs).

The review highlighted that BAME people represent:

- 14% of the population;
- 25% of the prison population; and
- 40% of young people in custody.

Black people represent:

- 3% of the population;
- 12% of the prison population; and
- more than 20% of young people in custody.

The review also found that:

- Arrest rates are higher for BAME people;
- BAME people are more likely to plead not guilty;
- There is evidence of differential treatment - for example, BAME people are more likely to receive prison sentences for drug offences;
- BAME people report poor experiences of prison (including discrimination); and
- Young BAME people in prison through the youth system are less likely to have recorded mental health needs, learning difficulties or troubled family relationships, suggesting they have unmet needs.

The review identified that if BAME people were not disproportionately represented in our CJS there would be 9,000 fewer prisoners (equivalent of 12 average prisons). It also estimates the economic cost of this overrepresentation in the courts, prisons and probation service as £309 million a year.

YOTs were established in the Crime and Disorder Act (1998) with a view to reducing youth offending and reoffending. The Lammy review acknowledged the success of the youth justice system in reducing the numbers of children and young people overall but cited:

- The BAME proportion of young people offending for the first time rose from 11% year ending March 2006 to 19% year ending March 2016;
- The BAME proportion of young people reoffending rose from 11% year ending March 2006 to 19% year ending March 2016; and
- The BAME proportion of youth prisoners had risen from 25% to 41% in the decade 2006-2016.

5. The Hammersmith & Fulham Picture

Data

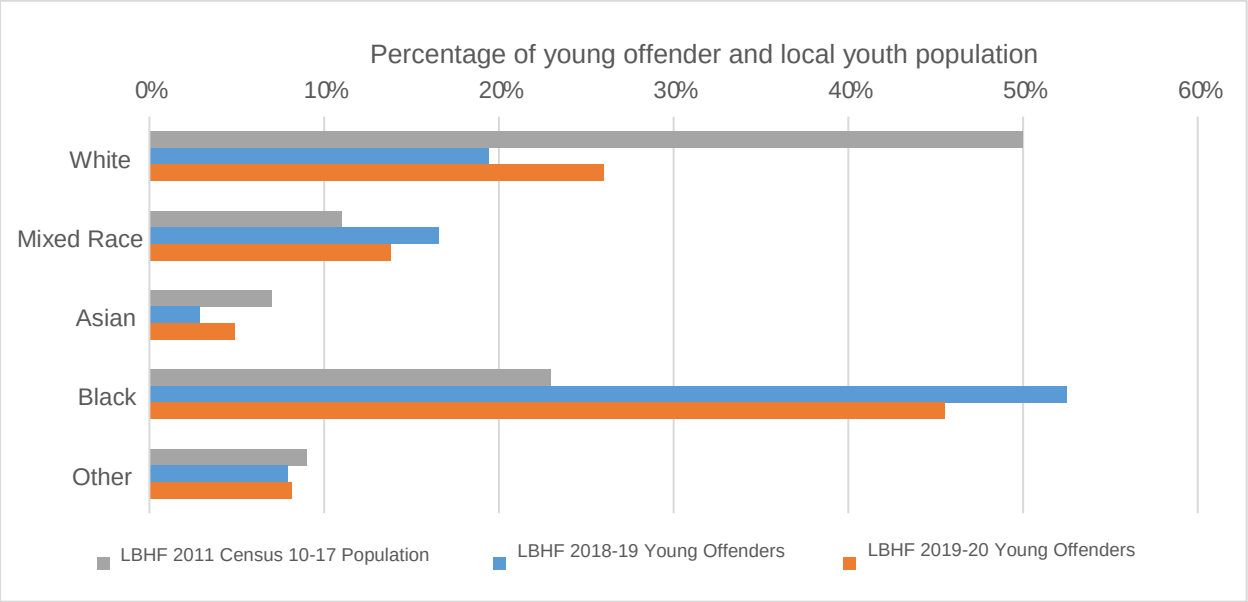


Figure 1 - H&F local youth population and young offender population by ethnicity

Figure 1 shows a significant overrepresentation of the Black group of young offenders compared to local youth population in H&F, while the White group is significantly under-represented. The Q4 period for 2019/20 shows that the overrepresentation of the Black group has decreased on the previous year. In H&F the rate of overrepresentation of BAME young people has been above the London and National rates. However, Q4 of 2019/20 saw the rate of overrepresentation reducing to below the London and National rates.

A recent stocktake of offences falling under the Youth Justice Board's (YJB) definition of serious youth violence robbery, violence against the person and drug offences showed Black and mixed heritage (Black and White) young people as overrepresented in this cohort. All recorded robbery offences in the year to March 2019 were committed by Black and mixed heritage children and young people.

- The live reoffending tracker 2019/20 shows of the current cohort of **73** young people **49** are BAME.
- Of the **8** young people currently in either a secure training centre (STC) or Young Offenders Institution (YOI) all bar **1** are Black or of mixed heritage.
- There are **54** young people open to the YOS currently of which **14** are LAC and **12** of whom are Black or mixed heritage.

Data from Children's Services also highlights that BAME children are overrepresented in terms of permanent school exclusions.

It is the aim of the GVEU to address his disproportionality by way of early intervention and diversion of young people who are involved or on the periphery of involvement with gangs Violence and exploitation. Within the Borough, this cohort is predominantly young BAME males who often see that they have no other option but to be drawn into this lifestyle.

The GVEU will work with young people to provide that alternative future and by working in partnership with all other statutory and non-statutory agencies operating within the Borough the team will start to affect the lives of these young people in a positive manner.

London Borough of Hammersmith & Fulham

Report to: Community Safety & Environment Policy & Accountability Committee

Date: 11/11/2020

Subject: Update on Council's Use of Investigatory Powers (RIPA and IPA)

Report of: Beth Morgan, Community Safety Policy and Service Development Officer

Responsible Director: Sharon Lea, Director, Strategic Director of Environment

Summary

- This report is to give Members the opportunity to scrutinise the council's conduct in relation to directed surveillance, covert human intelligence sources (CHIS) and communications data.

- The council must conduct directed surveillance, and use covert human intelligence sources, in accordance with the Regulation of Investigatory Powers Act (RIPA) and council policy.

- RIPA provides a statutory framework for police and public authorities to use investigatory powers, where necessary and proportionate, for the purpose of preventing or detecting crime or preventing disorder. RIPA regulates the use of these powers in a manner that is compatible with the Human Rights Act.

- The Investigatory Powers Act (IPA) 2016 provides a new legal framework for the acquisition of communications data, replacing Part I of Chapter 2 of RIPA.

- The council must access communications data in accordance with the Investigatory Powers Act 2016 and council policy.

- The council's use of covert surveillance was inspected by the Investigatory Powers Commissioner's Office (IPCO) in April 2020. The outcome of this inspection was positive and this report details the actions the council will take in response.

Recommendations

1. That Members review and comment on the council's RIPA (and IPA) policies and procedures and the use of RIPA and IPA functions by the council.

2. That members note the outcome of the IPCO inspection and provide any comments.

Wards Affected: All

H&F Priorities

Please state how the subject of the report relates to our priorities – delete those priorities which are not appropriate

Our Priorities	Summary of how this report aligns to the H&F Priorities
• Creating a compassionate council	The council uses investigatory powers, where necessary and proportionate, to address antisocial behaviour, crime and disorder which can have a devastating impact of the lives of residents in H&F.

Contact Officer(s):

Name: Beth Morgan
Position: Community Safety Policy and Service Development Officer
Telephone: 020 8753 3102
Email: Beth.Morgan@lbhf.gov.uk

Name: Stephen Gibbs
Position: Neighbourhood Wardens Manager (RIPA Coordinator)
Telephone: 020 8753 2645
Email: Stephen.Gibbs@lbhf.gov.uk

Background Papers Used in Preparing This Report

None

---

1. Background

- In January 2020, the Investigatory Powers Commissioner's Office (IPCO) communicated its intention to conduct an inspection of the council's use of covert surveillance in April 2020.

- 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'.

- Covert Human Intelligence Sources (CHIS) involve using an officer to establish or maintain a personal (or other) relationship with a person for the covert purpose of obtaining information, such as agents, informants or undercover officers. It is council policy not to use CHIS.

- The last inspection of Hammersmith & Fulham Council by the Office of Surveillance (OSC) took place in January 2017. Between October 2015 and July 2019 RIPA governance and functions in H&F were managed under a shared working arrangement with RBKC.

- Since then, H&F has implemented a new sovereign arrangement for the exercise of functions under RIPA, including developing and implementing sovereign RIPA policies, procedures and governance arrangements.

- Three separate policies have been developed since the last inspection and based on the councils' previous RIPA policy which cover:

a. Policy for Use of Direct Surveillance and Covert Human Intelligence Sources (Regulation of Investigatory Powers Act 2000) (**Appendix 1**)
b. Policy for Use of Direct Surveillance (without Judicial Approval / "Non-RIPA") (Regulation of Investigatory Powers Act 2000) (**Appendix 2**)
c. Policy for Accessing Communications Data (Investigatory Powers Act 2016) (**Appendix 3**)

- The council must report on the use of investigatory powers annually to the Community Safety and Environment Policy and Accountability Committee. The council's use of these powers since the last report are detailed below.

2. Frequency of Use:

2.1. Directed Surveillance (November 2018 – December 2019):

- Directed Surveillance refers to covert, but not intrusive, surveillance which is not an immediate response to events. 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 6 month or more custodial sentence, with the exception of offences relating to the underage sale of alcohol and tobacco).

Department	Authorising Officer	Number of applications	Reason
The Environment: Safer Neighbourhoods Division	Strategic Lead for Environmental Health and Regulatory Services	1	Illegal supply of controlled drugs

2.2. Non-RIPA Surveillance (November 2018 – December 2019):

- Local authorities have an obligation to deal with anti-social behaviour (ASB), which involves day-to-day incidents of crime, nuisance and disorder. Even what is perceived as 'low level' ASB, when targeted and persistent, can have a devastating effect on a victim.

- Therefore, in some cases it may be necessary for Council Officers to conduct covert surveillance that does not satisfy the serious “crime threshold” (criminal offences that are either punishable by at least 6 months’ imprisonment or are related to the underage sale of various prohibited items) and cannot be authorised by RIPA.

- 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.

Department	Authorising Officer	Number of applications	Reason
The Environment: Safer Neighbourhoods Division	Strategic Lead for Environmental Health and Regulatory Services	4	Intimidation/harassment; Illegal supply of controlled drugs (unknown suspects)

2.3. Communications Data (October 2018 – December 2019)

- 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.

- 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).

Department	Authorising Officer	Number of applications	Reason
The Environment: Trading Standards	Head of Fraud	1	Fraud

3. Inspection Report

- The Investigatory Powers Commissioners Office conducted an inspection of the council in April 2020.

- The feedback detailed in the inspection report was very positive and confirmed that the council has a good level of compliance with the legislation.

- In particular the report highlighted that:

- All recommendations made during the last inspection have been discharged;
- The council's RIPA policies had been revised, compliance with the policies is regularly checked, and an annual regime of RIPA training had been introduced;
- Quarterly meetings take place led by the RIPA Gatekeeper to critique the ongoing use of RIPA (this was noted as good practice);
- The directed surveillance authorisations reviewed were of good standard; and
- Robust processes are in place to securely retain surveillance products gathered as a result of covert activity (including a retention schedule to monitor the retention and destruction of this material).

3.1. Recommendations and Actions

- The inspector made five key recommendations in the report. The council has created an action plan to address each of these recommendations.

- Three of the recommendations related to additions to the council's investigatory powers policies. All the proposed changes have been made and the policies are attached as **Appendices 1-3**.

- A further recommendation related to establishing a process to review data retention and destruction. In response, the council has added data retention and destruction as a standing agenda item at the quarterly RIPA meetings.

- The final recommendation related to raising awareness of RIPA across the council (and, in particular, in service areas where RIPA considerations are not so immediately apparent). In response, the council has added RIPA awareness raising as a standing agenda item at the quarterly RIPA meetings.

List of Appendices:

Appendix 1 - Council Policy for Use of Direct Surveillance and Covert Human Intelligence Sources (Regulation of Investigatory Powers Act 2000)

Appendix 2 - Council for Use of Direct Surveillance (Without Judicial Approval / "Non-RIPA") (Regulation of Investigatory Powers Act 2000)

Appendix 3 - Council Policy for Accessing Communications Data (Investigatory Powers Act 2016)

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

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

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. 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 Stephen Gibbs, RIPA Coordinator. Copies of all relevant documentation relating to applications should therefore be emailed to Stephen.Gibbs@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. Sharon Lea, Strategic Director of Environment, 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:

Janette Mullins, Acting Chief Solicitor (Litigation and Social Care) 0208 753 2744

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 Stephen Gibbs, 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 Stephen Gibbs 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 Stephen Gibbs.

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

RIPA Applica

Appendix 4 - RIPA REVIEW FORM

RIPA Revie

Appendix 5 - RIPA RENEWAL FORM

RIPA Renev

Appendix 6 - RIPA CANCELLATION FORM

RIPA Cancell

Appendix 7 - COURT AUTHORISATION LETTER

Court Authori

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

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, Stephen Gibbs, 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.

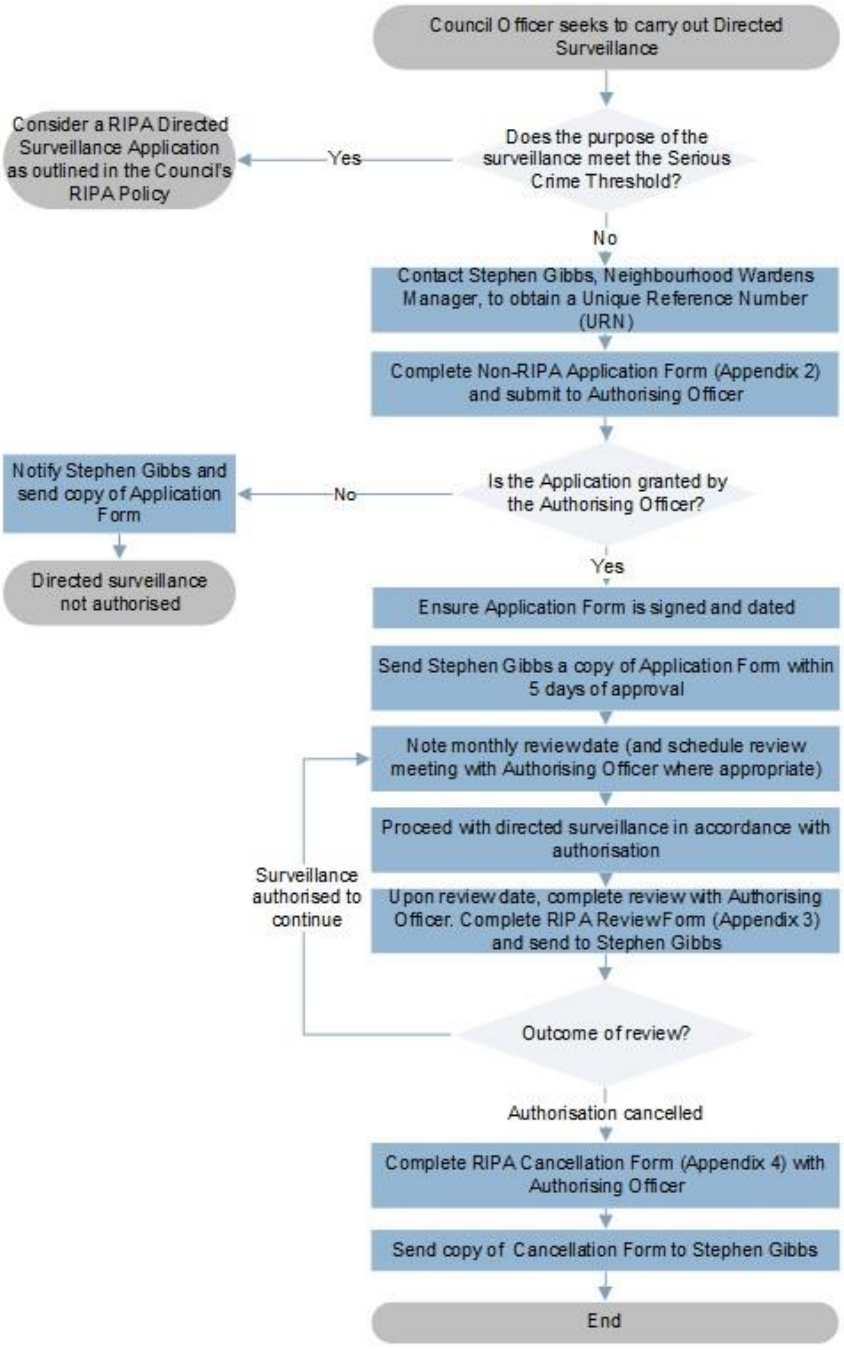
7.10. Authorisation for “non-RIPA” surveillance will last **3 months** unless cancelled or renewed and must be cancelled when no longer necessary or proportionate.

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



Officer should read RIPA Policy and "non-RIPA" Policy

Note: When considering covert surveillance which is outside of RIPA, Council Officers must have regard to the Council's RIPA Policy, the Directed Surveillance Code of Practice and the OSC Procedures and guidance.

Investigating Authorising Officers must take account of the risks outlined in the "non-RIPA" Policy when considering non-RIPA surveillance.

Surveillance must not be authorised under this policy if there is any likelihood of acquiring confidential information.

Note: Authorisation for non RIPA surveillance will last 3 months unless cancelled or renewed and must be cancelled when no longer necessary or proportionate.

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 Stephen Gibbs, RIPA Coordinator. Copies of all relevant documentation relating to applications should therefore be emailed to Stephen.Gibbs@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. Sharon Lea, Strategic Director of Environment

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:

Janette Mullins, Chief Solicitor (Litigation and Social Care) 0208 753 2744

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

Non-RIPA appl

Appendix 3 – NON-RIPA REVIEW FORM

Non-RIPA re

Appendix 4 – NON-RIPA RENEWAL FORM

Non-RIPA rei

Appendix 5 – NON-RIPA CANCELLATION FORM

Non-RIP

London Borough of Hammersmith & Fulham

Investigatory Powers Act 2016
Policy for Use of Communications Data

February 2020

CONTENTS

1. INTRODUCTION

1.1. The Investigatory Power Act (IPA) 2016 sets out how a local authority can access communication data. 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. Sharon Lea, Strategic Director of Environment, 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).