Audit & Anti-Fraud Progress Report

1 April 2023 - 30 September 2023

1. INTRODUCTION

1.1 The purpose of this report is to present the performance of the Audit & Anti-Fraud Service for the period 1 April 2023 to 30 September 2023. It covers the areas of work undertaken, progress with implementing audit recommendations and information on current developments in the service area.

1.2 Internal Audit provides an independent continuous review of key and high-risk activities across the Council. It is important that the effectiveness of the work of Internal Audit is monitored and reported in order to comply with the requirements of the Accounts & Audit Regulations 2015 and to provide the necessary assurance on the adequacy of the Internal Audit service. This report contributes toward meeting these requirements.

2. INTERNAL AUDIT RESOURCES AVAILABLE

2.1 The Internal Audit function is an in-house service supplemented by specialist IT skills from an external provider. Internal Audit also supports the Council's CIPFA trainee programme. Internal Audit relies upon the co-operation of directorates and service level management to enable us to undertake the planned reviews.

2.2 The Internal Audit Team is fully staffed, including one post that is being covered by a Fixed Contract. We are focusing our resources on the areas that management has agreed can take place and will provide the necessary evidence to support the Corporate Head of Audit, Anti-Fraud & Risk Management's annual assurance statement.

2.3 The 2023/24 Audit Plan consisted of 65 audits (of which 12 are schools/children's centres), 6 audits have been postponed, cancelled or combined, and two have been added since the plan was agreed.

3. INTERNAL AUDIT KEY PERFORMANCE INDICATORS

3.1 Internal Audit's performance for 2023/23 against key indicators is shown in Table 1. Post audit survey results are summarised in paragraph 3.3.

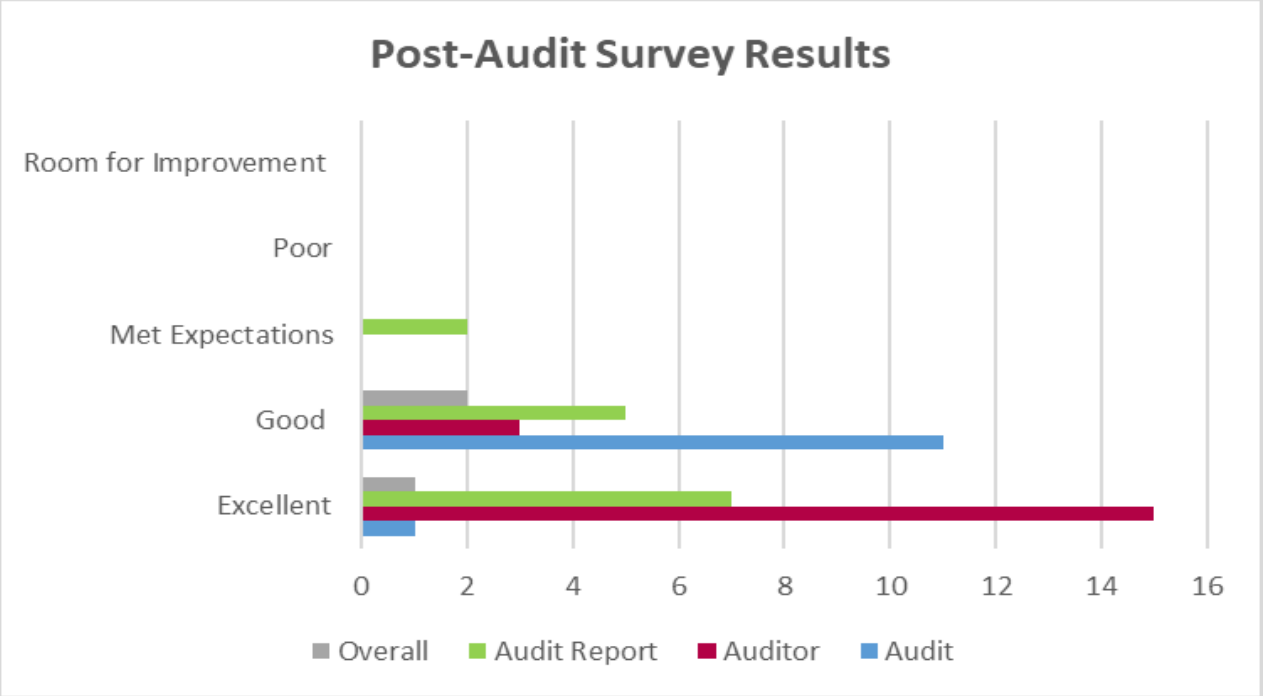
Objective	KPIs	Targets	Actual
Cost & Efficiency *To ensure the service provides Value for Money*	1) Percentage of planned audits completed to final/draft report stage 2) Average days between the end of fieldwork & issue of the draft report.	1) 90% by year end 2) Less than 15 working days	1) 18% complete or at draft report stage 2) 7 days
Quality *To ensure recommendations made by the service are agreed and implemented*	1) Percentage of high and medium recommendations made which are agreed 2) Percentage of agreed high and medium priority recommendations which are implemented	1) 100% 2) 90%	1) 100% 2) 62% - fully implemented** 13% - partially implemented
Client Satisfaction *To ensure that clients are satisfied with the service and consider it to be good quality*	1) Results of Post Audit Questionnaires 2) Results of other Questionnaires 3) No. of Complaints / Compliments	1) Responses meeting or exceeding expectations 2) Satisfactory 3) Actual numbers reported	1) 100% met expectations (96% exceeded expectations or excellent) 2) N/A 3) None

** See paragraph 6.2 for explanation

Table 1

3.2 As at 30 September 2023 a total of 18 internal audit reviews have been started from the 2023/24 Plan, 9 have been completed and a further three are at draft report stage. In addition 8 reviews carried forward from the 2022/23 annual plan were finalised.

3.3 Post-Audit Survey results from 1 April 2023 to 30 September 2023 continue to show that overall expectations of auditees are met or exceeded with 96% responding that expectations were exceeded, see bar chart below.



4. SUMMARY OF INTERNAL AUDIT WORK

4.1 Progress with 2023/24 planned audits is summarised in Table 2 below and detailed in Appendix 2.

2023/24 Audit Plan Stage of Audit Activity	**Number of assignments**	**Percentage of revised plan**
Scoping/TOR agreed	13	21
Fieldwork in progress	6	10
Draft report issued	3	5
Completed	9	14
Total work completed and in progress	**31**	**50%**
Original Plan	65	
Additional requests	2	
Cancelled or Postponed	5	
Total Revised Plan	**62**	

Table 2

4.2 The table shows 50% of the planned assignments have been completed, scoped/terms of reference agreed, or are work in progress.

4.3 Details of changes to the original audit plan are shown in Table 3 below. It is expected that there will be a degree of change to the audit plan that is agreed in April as the financial year progresses and priorities and risks change. There are also some deferral requests that in themselves raise concerns about the local control environment, for example, where the reason relates to the absence of systems due to the cyber attack or other cause, the absence of key staff due to organisational change or repeated deferral requests. Additional information will be provided to future Audit Committee meetings once consultation with management has been completed.

Cancelled reviews	**Reason for Cancellation**
Energy & Carbon Management - Hackney Schools	A reevaluation by Internal Audit & the Auditee has identified that the risks to the process are not significant and therefore the audit is not relevant at this time.
Integrated Learning Disabilities Service, ILDS	A recent independent review carried out. Action plan of review has led to an ongoing 3 year Transformation programme. Transformation Board Action Plan to be shared with Internal Audit
Postponed reviews	**Reason for Deferral**
Leasehold major works debt recovery	System availability and resource constraints
Procurement of Homecare	The audit has been deferred since 2021/22 pending progression of the procurement tender process.
Elections	Recent announcements. Resources/ Capacity and the timing of the implementation of new legislation
Additional reviews	**Reason for Addition**
The Garden School	Hackney Education Request
Changing Places Fund Grant	Management Request. Grant Usage Validation & Certification

Table 3

4.4 Each completed audit is given an overall assurance grading. These are categorised as ‘Significant’, ‘Reasonable’, ‘Limited’ or ‘No’ assurance. The assurances given this year are included in Appendix 3. For those audits finalised this year, including 8 carried forward from the 2022/23 plan, the assurance levels are set out in Table 4.

Assurance Level	**2023/24**	**2022/23**	**2021/22**
No	0	0	1
Limited	2	0	0
Reasonable	7	7	8
Significant	6	17	5
Not Applicable	0	0	0
Total	**15**	**24**	**14**

Table 4

4.5 Where Internal Audit work identifies areas for improvement, recommendations are made to manage the level of risk. These are categorised as ‘High’, ‘Medium’ or ‘Low’ priority. The numbers of High and Medium recommendations issued up to 30 September 2023 are shown in Table 5.

Categorisation of Risk	Definition	Number 2023/24 Plan	Number 2022/23 Plan not previously reported
High	Major issues that we consider need to be brought to the attention of senior management.	2	3
Medium	Important issues which should be addressed by management in their areas of responsibility.	16	17
	Total	**18**	**20**

Table 5

5. SCHOOLS

5.1 The results of schools' audits are reported to Hackney Education (HE) within the Children's and Education Directorate. In addition, progress with the implementation of agreed recommendations from 2018/19 to the current date are regularly followed up and reported.

5.2 The schools audit programme focuses on the existence of, and compliance with key financial controls and the adequacy of governance arrangements.

6. IMPLEMENTATION OF RECOMMENDATIONS

6.1 In order to track the Council's response to improving the control environment, progress with implementation of agreed internal audit recommendations is tracked. The results of this work for the 'High' priority recommendations from audits undertaken from 2020/21 that were due to be implemented by 30 September 2023 are presented in Table 6.

Directorate	Implemented/ No longer relevant	Partially Implemented	Not implemented /No response	Not Yet Due	Total*
AHI	1	0	0	0	1
Children & Education	0	0	0	0	0
Climate, Homes & Economy	8	2	4	2	14
Finance & Corporate Resources	0	0	0	0	0
ICT	0	0	0	1	0
Chief Executive's	0	0	0	0	0
Corporate	1	0	0	0	1
Total number	10	2	4	3	16
Percentage (%)*	62%	13%	25%	n/a	100%

* Does not include "Not Yet Due"

Table 6

6.2 The Council's target for 2023/24 is 90% of 'High' priority recommendations should be implemented in accordance with agreed timescale. Audit followed up 16 'High' priority recommendations, the implementation rate currently stands at 62% fully implemented, with a further 13% partially implemented.

6.3 Of the 90 'Medium' priority recommendations followed up 54% were assessed as implemented and 20% partially implemented. Details are shown in Table 7.

Directorate	Implemented /No longer relevant	Partially Implemented	Not implemented /No Response	Not yet due	Total*
Adults, Health & Integration	7	2	0	0	9
Children & Education	1	0	1	2	2
Climate, Homes & Economy	32	3	13	6	48
Finance & Corporate Resources	0	7	4	4	11
ICT	0	0	0	7	0
Chief Executive's	7	0	0	0	7
Corporate	2	6	5	0	13
Total number	49	18	23	9	90
Percentage (%)	54%	20%	26%	n/a	100%

* Does not include "Not Yet Due"

Table 7

6.4 Recommendations made during school audits are followed up in the same way as for other recommendations. In circumstances where audits are categorised as 'No' or 'Limited' assurance, or where the school fails to provide progress updates with implementation of 'High' category recommendations, a follow up review is scheduled.

Recommendation Priority	Implemented/ No longer relevant	Partially Implemented	Not implemented/ No Response	Not yet due	Total*
High	1	1	1	1	3
Medium	60	6	28	6	94
Total Number	61	7	29	7	97
Percentage (%)	63%	7%	30%	n/a	100%

* Does not include "Not Yet Due"

Table 8

7. DEVELOPMENTS WITHIN INTERNAL AUDIT

7.1 The Audit & Anti Fraud Service has substantially recovered from the cyber attack and the Covid-19 pandemic. The ongoing effects of these exceptional events does continue to impact the ability to audit some Council services, as set out at paragraph 4.3 of this report.

7.2 The delivery of the planned ICT audits is now progressing after significant interruption due to the necessary response to the cyber attack in October 2020. One audit from the 2022/23 plan has been completed, audit fieldwork is progressing on other reviews and terms of reference are in place.

7.3 Internal Audit activity must be carried out in accordance with the Public Sector Internal Audit Standards (PSIAS). These include a requirement to undertake a regular internal assessment of the service, and a periodic External Quality Assessment (EQA), which should take place at least every 5 years. The most recent EQA review was undertaken in August 2023, it was overdue because of the pandemic and then the cyber attack. The report is in the process of being finalised and can be shared with the Audit Committee membership when it is available. Because the timing of the EQA report does not coincide with the Audit Committee timetable a summary of the issues that have been raised at draft stage are attached to this report as Appendix 7.

The status of the 10 recommendations that have been raised for Internal Audit to consider at the draft report stage are as follows:

- 4 recommendations have been implemented and are complete;
- 2 recommendations are advisory and will not be implemented;
- 2 recommendations have been agreed and will be implemented by 31 March 2024;
- One recommendation has been agreed and is in the process of being implemented;
- One recommendation is subject to further consideration before the draft report is agreed.

The actions arising from the EQA will be added to the Internal Audit Quality and Improvement Plan to ensure that the service continues to meet the highest standards.

8. ANTI FRAUD SERVICE

8.1 Investigation activity has been fully resumed following the disruption caused by the pandemic, which severely curtailed some areas of work. Some impacts continue to be felt following the cyber attack and, more significantly, from backlogs that have built up in the criminal justice system since early 2020.

8.2 Statistical information relating to the work of the Anti-Fraud Teams is shown at Appendix 4.

9. CONCLUSIONS

9.1 This report provides details of the performance of the Council's Internal Audit and Anti Fraud Services. It provides assurance that the service is being delivered to meet statutory responsibilities and is continually seeking to improve the standard of its service.

9.2 A greater level of audit resource than usual continues to be focussed on reviews that have been deferred from previous years due to the cyber attack and the pandemic, and those that will provide evidence to support the Corporate Head of Audit, Anti-Fraud & Risk Management's annual assurance statement.

Internal Audit Annual Plan *Progress to 30 September 2023 (including 2022/23 audits completed in the current year)*					
Code	**Description**	**High Priority**	**Medium Priority**	**Audit Assurance**	**Status**
2022/23 Audits					
Corporate / Cross Cutting					
2232LBH01	AGS Co-ordination 2023/24	N/A	N/A	**Reasonable**	Final Report
ADULTS, HEALTH & INTEGRATION					
2223AHI04	Safeguarding Adults	0	4	**Reasonable**	Final Report
CHILDREN & EDUCATION					
Children & Families					
2223CE01	LAC Incidentals				Draft Report
2223CE04	No Recourse to Public Funds	0	2	**Significant**	Final Report
FINANCE & CORPORATE RESOURCES					
Financial Management					
2223FCR05	Pensions	0	3	**Significant**	Final Report
Revenues & Benefits					
2223FCR10	NNDR/Business Rates	0	2	**Significant**	Final Report
ICT					
22233ICT04	Homeworking Support	0	3	**Reasonable**	Final Report
CLIMATE, HOMES & ECONOMY					
Housing					
2223CHE01	Cranston TMO	3	5	**Limited**	Final Report

Code	Description	High Priority Recs	Medium Priority Recs	Audit Assurance	Status
2023/24 Audits					
Corporate / Cross Cutting					
2324LBH01	AGS Co-ordination 2024/25				Q4
2324LBH02	Climate Change/Zero Tolerance				WiP
2324LBH03	Organisational Culture				Q4
2324LBH04	Equal Pay				WiP
2324LBH05	Gifts & Hospitality	1	1	**Reasonable**	Final Report
2324LBH06	Public Interest Reports (PIRs) Lessons Learnt				Q4/Pending Scrutiny Deep Dive
Chief Executive's					
2324CEX01	Recent Election Act				Deferred
2324CEX02	Internal Communications - Google Contacts				Draft Report
2324CEX03	Matrix ICT Contract (Digital Market Place)				Q3/ToR
Adults, Health & Integration					
Adult Services/Public Health					
2324AHI01	Integrated Learning Disabilities Service (ILDS)				Cancelled
2324AHI02	Procurement of Homecare				Deferred
2324AHI03	Public Health Commissioned Services - Substance Misuse				Q3
2324AHI04	Direct Payments Financial Assessment Process				Q3
2324AHI05	Residential Care				Q3
2324AHI06	Mortuary				Q4
2324AHI07	Supporting Families Programme Grant	0	0	**Reasonable**	Quarterly
2324AHI08	DLUHC Changing	0	0	**Reasonable**	Quarterly

	Places Fund Grant				
Children & Education					
Children & Families					
23243CE01	Development of Children & Family Hubs (Advisory)				Ongoing
2324CE02	Joint Agency Funding - Children with Complex Needs				Q3/Scoping
2324CE03	Foster Care Payments				Q3
2223CE04	CFS Residential Placements - LAC				Q3
Education & Schools					
2324CE05	Schools Overview Report 2019/20 - 2022/23	0	0	**Significant**	Final Report
2324CE06	Cost of Children in Alternative Provision				WiP
2324CE07	Falling School Roll Numbers				Q3/ToR
2324CE08	Traded Services				Q3/ToR
2324CE09	Unregistered Settings				Q4
Schools					
Primary Schools & Children's Centres					
2324SCH01	Colvestone Primary				WiP
2324SCH02	New Wave Federation	0	3	**Significant**	Final Report
2324SCH03	Viridis Federation				Q3/ToR
2324SCH04	Jubilee Primary & Fernbank Nursery School	0	2	**Reasonable**	Final Report
2324SCH05	Shoreditch Primary School (Formerly Whitmore Primary)				Q3
2324SCH06	Baden Powell Primary School				WiP
2324SCH07	Simon Marks Primary School				Q3/ToR
2324SCH08	Benthal Primary School				Draft Report
2324SCH09	St.Pauls with St.				Q4

	Michaels Primary School				
Secondary Schools					
2324SCH10	Cardinal Pole Secondary	1	8	**Limited**	Final Report
2324SCH11	The Urswick Secondary				WiP
2324SCH12	Clapton Girls Academy - Scrutiny	0	1	**Significant**	Final Report
2324SCH13	The Garden School				Q4
FINANCE & CORPORATE RESOURCES					
Financial Management					
2324FCR01	Risk Management				Q4
2324FCR02	Main Accounting System				Q3/ToR
23243FCR03	Accounts Payable				Q3/ToR
2324FCR04	Pensions				Q3/ToR
2324FCR05	VAT Compliance on Income				Q3/ToR
2324FCR06	Service Payroll				Q/4
2324FCR07	Fleet Management				Draft Report
Procurement					
2324FCR09	Reprocurement of Expiring Contracts				WiP
2324FCR10	Energy & Carbon Management in Hackney Schools				Cancelled
Revenues & Benefits					
2324FCR11	Money Hub				WiP
Strategic Property					
2324FCR12	Commercial Property Income				Q3/ToR
ICT					
2324ICT01	3 year ANA				n/a
2324ICT02	ICT Governance				Q4
2324ICT03	ICT Asset Management				ToR

2324ICT04	Key IT Systems & theirFunctionalty Post Cyber Attack				Q/4
2324ICT05	Cloud Platform				WIP
2324ICT06	FOI				Q4/ToR
2324ICT07	Follow-up of Recommendations				Q/4
2324ICT08	Assurance on New Systems, Repairs, Asset Management & Community Safety				Q4
Climate, Homes & Economy					
Housing					
2324CHE01	Rent Arrears - Incl. Effect of UC on Tenant Arrears				Q4
2324CHE02	Complaints Handling - Housing				Q3
2324CHE03	Right to Buy Scheme				Q3
2324CHE04	Leasehold Major Works- Debt Recovery				Deferred
2324CHE05	Wenlock Barn TMO				ToR
2324CHE06	Downs TMO				Q4
Public Realm					
2324CHE07	Use of Infrastructure Levy/Section 106				ToR
2324CHE08	Planning Enforcement				Q3/ToR
Regeneration					
2324CHE10	Business Grants Review - Additional Restrictions Grant (ARG)	0	1	**Significant**	Final Report

The **Overall Assurance** given in respect of an audit is categorised as follows:

Level of assurance	Description	Link to risk ratings
Significant	Our work found some low impact control weaknesses which, if addressed, would improve overall control. However, these weaknesses do not affect key controls and are unlikely to impair the achievement of the objectives of the system. Therefore we can conclude that the key controls have been adequately designed and are operating effectively to deliver the objectives of the system, function or process.	There are two or less medium-rated issues or only low rated or no findings to report.
Reasonable	There are some weaknesses in the design and/or operation of controls which could impair the achievement of the objectives of the system, function or process. However, either their impact would be less than critical or they would be unlikely to occur.	No more than one high priority finding &/or a low number of medium rated findings. Where there are many medium rated findings, consideration will be given as to whether the effect is to reduce the assurance to Limited.
Limited	There are some weaknesses in the design and / or operation of controls which could have a significant impact on the achievement of key system, function or process objectives but should not have a significant impact on the achievement of organisational objectives. However, there are discrete elements of the key system, function or process where we have not identified any significant weaknesses in the design and / or operation of controls which could impair the achievement of the objectives of the system, function or process. We are therefore able to give limited assurance over certain discrete aspects of the system, function or process.	There are up to three high-rated findings. However, if there are three high priority findings and many medium rated findings, consideration will be given as to whether in aggregate the effect is to reduce the opinion to No assurance.
No	There are weaknesses in the design and/or operation of controls which [in aggregate] have a significant impact on the achievement of key system, function or process objectives and may put at risk the achievement of organisation objectives.	There are a significant number of high rated findings (i.e. four or more).

* The overall assurance provided on reviews of Hackney Schools and Tenant Management Organisations (TMOs) differs slightly to the above (Appendix 3). To conclude an overall significant assurance rating requires three or less medium-rated issues, this is due to the wide coverage of risk and control areas during School & TMO reviews.

Anti-Fraud Service:

Statistical Information 1 April 2023 to 31 March 2023

1. Investigations Referred

The Anti-Fraud service has received 249 referrals during the 2023/24 year to date, which is broadly comparable with the rate of referrals during the previous 12 month period.

Group	Department	Number of Cases Referred in Period	Number of Cases Closed in Period	Cases Currently Under Investigation	Referrals 2023/24 YTD	Referrals 2022/23
Climate, Homes & Economy (CHE)	Climate, Homes & Economy	6	7	10	6	23
	Tenancy Fraud	119	99	400	119	278
	Parking	43	69	40	43	142
Children's & Education	Children's	2	2	0	2	5
	No Recourse to Public Funds (NRPF)	67	69	29	67	64
	Hackney Education	3	2	5	3	2
Adults, Health & Integration	Adults, Health & Integration	3	2	3	3	4
Finance & Corporate Resources (F&CR)	Finance & Resources	4	1	8	4	5
	Covid19 Business Grants	0	1	0	0	2
Chief Executive's Directorate	Chief Executive's Directorate	2	1	1	2	2
Total		249	253	489	249	527

Table 1

Note 1: Fraud reporting is provided at Group Directorate level, with additional detail being provided for areas that have been the subject of a dedicated counter-fraud response (Tenancy, Parking, Covid grants and NRPF).

Note 2: Cases closed/under investigation may include those carried forward from previous reporting periods.

2. Fraud Enquiries

Investigative support is provided to other bodies undertaking criminal enquiries, including the Police, Home Office and other Local Authorities. The team also supports other LBH teams to obtain information where they do not have direct access and it is available under the Data Protection Act crime prevention and detection gateways. AAF no longer provides a dedicated service to DWP to support their investigations, but an alternative mechanism has been made available to DWP which does not have a resource cost for Hackney.

Source	Number of Cases Referred in period	Number of Cases Closed in period	Cases Currently Under Investigation	Referrals 2023/24 YTD	Referrals 2022/23
Internal	16	17	0	16	19
Other Local Authority / Housing Association	61	63	0	61	65
HMRC	14	15	0	14	6
Police	22	24	0	22	21
Immigration	8	8	0	8	2
DWP	9	9	0	9	4
Other	7	8	0	7	5
Total	137	144	0	137	122

Table 2

3. National Fraud Initiative (NFI) Matches

The NFI is a biennial data matching exercise; the majority of datasets were most recently received in January 2023 (with the Council Tax matches being received a little later). Matches are investigated by various LBH teams over the 2 year cycle, AAF investigates some matches and coordinates the Council's overall response. The total number of matches includes a number of recommended cases that are identified as high priority, participants are expected to further risk assess the results to determine which are followed up.

Type of Match	Number of Matches	Cases Under Investigation	Number Matches Cleared NFI2022/23	Number Matches Cleared NFI2020/21
Payroll	68	13	22	22
Housing Benefit	1008	3	814	32
Housing Tenants	1151	54	565	79
Right to Buy	506	0	65	0
Housing Waiting List	n/a	n/a	n/a	n/a
Concessionary travel / parking	825	3	625	292
Creditors	7180	0	43	8
Pensions	268	33	134	220
Council Tax (SPD)	13,134	212	881	n/a
Council Tax Reduction Scheme	n/a	n/a	n/a	n/a
Covid19 business grants	n/a	n/a	n/a	105
Other	26	1	15	n/a
Total	24,166	319	3,164	758

Table 3

Hackney has been able to participate more fully in the 2022/23 NFI matching than was possible in 2020/21 following recovery from the cyber attack in October 2020, although a lower level of disruption has persisted (hence the absence of some match categories from the table above).

Responsibility for investigating Housing Benefit matches passed to the DWP in 2014, Hackney has enabled DWP officers to directly access our Housing Benefit records, this has reduced the financial and resource burden on the Council.

4. Analysis of Outcomes

Investigations can result in differing outcomes from prosecution to no further action. Table 4 below details the most common outcomes that result from investigations conducted by the Anti-Fraud Teams.

Outcome	Reporting Period	2023/24 YTD	2022/23
Disciplinary action	0	0	1
Resigned as a result of the investigation	3	3	2
Referred to Police or other external body	1	1	3
Prosecution	5	5	3
Referred to Legal Services	9	2	8
Investigation Report/ Management Letter issued	4	4	7
Council service or discount cancelled	33	33	75
Covid business grants cancelled	1	1	3
Blue Badges recovered	20	20	66
Other fraudulent parking permit recovered	3	3	18
Parking misuse warnings issued	13	13	61
Penalty Charge Notice (PCN) issued	19	19	91
Vehicle removed for parking fraud	13	13	56
Recovery of tenancy	20	20	49
Housing application cancelled or downgraded	0	0	2
Right to Buy application withdrawn or cancelled	1	1	11

Table 4

The 5 prosecution outcomes listed above all relate to parking investigations. Three cases involved the use of a stolen Blue Badge and two cases involved the use of fraudulent visitor vouchers.

The Audit Investigation Team have been involved in 2 planning cases where criminal convictions had already been obtained but our follow up Proceeds of Crime work resulted in the award of confiscation orders totalling £311,200.31.

The investigations which led to the 3 staff resignations concerned 2 cases of misuse of a parking permit and one case involving irregularities in time recording.

5. Financial Losses as a Result of Fraud

The most apparent consequence of many frauds is a financial loss, however, it needs to be noted that it is not always possible to put a value in monetary terms. In many cases the direct financial loss accounts for only a small amount of the total cost of the fraud, with the additional amount comprising intangibles such as reputational damage, the cost of the investigation and prosecution, additional workplace controls, replacing staff involved and management time taken to deal with the event and its' aftermath.

The following are estimates of the monetary cost for some of Hackney's priority investigation areas based (where relevant) upon external benchmarking data to provide a realistic estimation of the cost of the irregularity:

5.1 Tenancy Fraud Team (TFT)

During the period April 2023 to september 2023 a total of 20 tenancies have been recovered by the TFT. Using the recognised measure for the estimated cost of each misused tenancy of £42,000 pa, this equates to a value of £840,000.

During this period one Right to Buy (RTB) applications was cancelled following investigation. Each RTB represents a discount of £127,900 on the sale of a Council asset, so the value of this work is a saving of £127,900 to the public purse.

5.2 No Recourse to Public Funds Team (NRPF)

An average weekly support package valued at c£387 is paid to each family supported (applicable to the 'service cancelled' category in Table 4). In the period April to September 2023, 33 support packages were cancelled or refused following AAF investigations. This equates to a saving in the region of £12,771 per week, if these had been paid for the full financial year it would have cost Hackney approximately £665,916

It is expected that more packages will be cancelled as a result of investigations carried out during this reporting period, once cases have been thoroughly evaluated.

5.3 Parking Concessions

The Audit Commission estimated the cost of each fraudulently used Blue Badge to be £100 (equivalent to on-street parking costs in the Hackney Central parking zone for less than 39 hours). Fees of £65 are also payable where a Penalty Charge Notice is issued as part of the enforcement process, or £265 if the vehicle is removed. In this period AIT recovered 23 Blue Badges or other parking permits, which equates to £2,300, and enforcement charges of £3,835 also arose.

The cost for these types of fraud is far greater in terms of the denial of dedicated parking areas to genuine blue badge holders and residents, and the reputational damage that could be caused to Hackney if we were seen not to be tackling the abuse of parking concessions within the borough.

5.4 Covid19 Business Grants

The investigations team has worked closely with the grant administration teams since March 2020 to assist with the grant verification process. This has identified multiple grant applications which were inaccurate, resulting in payment being withheld, and further cases where action is underway to recover payments that have already been made. One grant overpayment of £10,000 was resolved during this reporting period.

6. Matters Referred from the Whistleblowing Hotline

All Hackney staff (including Hackney Homes and Hackney Education) can report concerns about suspected fraud and other serious matters in confidence to a third party whistleblowing hotline. Other referral methods are available (and may indeed be preferable from an investigatory perspective), however, the hotline allows officers to raise a concern that they might not otherwise feel able to report. One fraud referral was received via the hotline in the reporting period.

7. Regulation of Investigatory Powers Act (RIPA) Authorisations

RIPA is the legislation that regulates the use of surveillance by public bodies. Surveillance is one tool that may be used to obtain evidence in support of an investigation, where it can be

demonstrated to be proportionate to the seriousness of the matter concerned, and where there is no other less intrusive means of obtaining the same information.

Because surveillance has the potential to be a particularly intrusive means of evidence gathering, the approval process requires authorisation by a nominated senior Hackney officer (Corporate Head of Audit, Investigations & Risk Management/Director/Chief Executive) and approval by a magistrate. Although Hackney will use its surveillance powers conferred by RIPA when it is appropriate to do so, no application has been made in the current financial year.

8. Proceeds of Crime Act (POCA) Investigations

POCA investigations can only be undertaken by accredited officers, as are currently employed by AAF. The Council is able to benefit financially from the use of POCA investigation powers. The amount awarded to the Council is greater in instances where the Council is both the investigating and prosecuting authority. The Council's investigation processes are supported by POCA in four principal ways: -

- Providing access to financial information in connection with a criminal enquiry, subject to approval by Crown Court by way of a **Production Order**.
- Preventing the subject of a criminal enquiry from disposing of assets prior to a trial, where these may have been obtained from criminal activity, by use of a **Restraint Order**, subject to Court approval.
- Recognising that offenders should not be able to benefit from their criminal conduct through the use of **Confiscation Orders**. These allow the courts to confiscate any benefit that a defendant may have received as a result of their crime.
- Under the confiscation process the courts are also able to ensure that victims are compensated for their loss by way of a **Compensation Order.**

Type of Order	Authorised in period	2022/23 YTD	2022/23
Production	6	6	3
Restraint	0	0	0
Compensation	0	0	0
Confiscation	1	1	0
Total	7	7	3

Table 5

The POCA incentivisation scheme splits the proceeds from orders between investigation, prosecution and judicial authorities, and the HM Treasury - so the amount reported here represents a part of the total benefit to the public purse arising from this work. It should be noted that funds awarded from successful POCA investigations can often be received some time after the investigation is reported.

9. Proactive counter-fraud plan for 2023/24

The content of the 2023/24 proactive counter fraud plan was reported in April, since when the following reviews have been started:

- Allocation of specific parking permits - terms of reference has been prepared;
- Entitlements to specific new grant programmes - work in progress
- Compliance with leave arrangements - work in progress

Delivery of the proactive counter-fraud plan is determined in part by the number and complexity of reactive investigations that are received.

Anti-Fraud and Corruption Policy

Audit & Anti-Fraud Division
October 2023

Anti-Fraud and Corruption Policy

Contents Page

Anti-Fraud and Corruption Policy

1. Introduction

1.1 The London Borough of Hackney employs over 4000 staff and has gross expenditure in the region of £1.2 billion. As with all large organisations, the size and nature of our services puts us at risk of loss due to fraud, corruption and irregularity both from within and outside the Council.[1]

1.2 The Council is committed to tackling fraud, corruption and irregularity and making sure that the opportunity for these to occur is reduced to the lowest possible level. Where there is the possibility of fraud, corruption or other irregularities, we will deal with such matters as outlined in the following paragraphs.

1.3 The Council has maintained its' anti-fraud capabilities in recent years and this has enabled the ongoing effective detection of, and response to, fraud and corruption. Dedicated teams are in place to tackle the highest priority issues. As a result Hackney has achieved significant savings and recovery of funds and assets, which contributed to the Council's reputation for sound internal control.

1.4 An important part of this approach is having an established anti-fraud and corruption policy, which is used to advise and guide Members, staff and persons working for/with the Council on our approach to the serious issues of fraud and corruption. This document provides an overview of the Council's approach in this matter and includes a 'Fraud Response Plan' which provides more detailed guidance on how to deal with fraud and corruption (see Appendix 1).

1.5 The main message is that the Council expects all Members, employees and workers to be fair and honest, and to give Audit and Anti Fraud service any ~~all reasonable~~ help, information and support that is needed to deal with fraud and corruption. Employees in this context relates to direct employees as well as other 'workers', including agency and contract staff, consultants, staff employed in Hackney maintained educational establishments, volunteers, etc.

1.6 This Anti-Fraud & Corruption Policy and supporting documents apply to the whole of the Council, including Hackney Education and schools and nurseries maintained by the London Borough of Hackney.

1.7 This policy supersedes all previously published Anti-Fraud and Corruption Strategies and will take immediate effect. It is the responsibility of the Audit and Anti-Fraud Service to make sure that this document is reviewed regularly to ensure it remains effective. Any enquiries about this policy should be directed to the Corporate Head of Audit, Anti-Fraud and Risk Management. Future revisions to this policy should be approved by the Council's Audit Committee.

[1] For the purposes of this document 'fraud & corruption' is an all encompassing term which should also be taken to include, dishonest financial irregularity/misappropriation, theft, etc.

2. Approach

2.1 The Council's approach to minimising the risk of loss due to fraud, corruption and irregularity is: -

a) to develop and maintain a culture of honesty and openness, and to oppose fraud, corruption and irregularity within the Council and in its relationship with outside individuals and organisations; and

b) to have a series of comprehensive and inter-related procedures and arrangements in place designed to prevent, frustrate and deter fraud, corruption and irregularity or, where they occur, to detect and take effective action against any attempted or actual fraud, corruption or irregularity affecting the Council.

2.2 The Audit and Anti Fraud Service will investigate cases of fraud and corruption. Employees are expected to comply with the spirit as well as the letter of the laws and regulations that are relevant to their Council duties. Those who commit fraudulent and corrupt actions are liable to face disciplinary action which may result in dismissal for gross misconduct. We may also refer such matters to the police and will support criminal prosecutions where this is appropriate.

3. Culture

3.1 The Council believes that the maintenance of a culture of honesty and openness is an important component in tackling fraud, corruption and irregularity.

3.2 To be effective, the Anti-Fraud and Corruption Policy and supporting arrangements set out in Section 4, need to apply within an overall culture within the Council which positively promotes the highest standards expected of those who represent it and makes it absolutely clear that the Council will not tolerate dishonesty on the part of any of its Members or employees or any persons/organisations involved in any way with the Council.

3.3 To encourage this culture the Council has adopted a range of interrelated policies, codes, arrangements and procedures which ensures all Members, employees or any persons/organisations involved in any way with the Council are

- ➢ fully aware of our cultural and ethical values and the conduct that is expected;
- ➢ required to comply with these standards when working for the Council, and also away from work to the extent that their actions may compromise the Council's values, including the aim of minimising fraud and corruption.~~and in agreement with, the culture the Council seeks to maintain, the values and conduct expected of persons working for or involved with the Council, including the Council's aim of keeping fraud & corruption to the lowest possible level~~

3.4 Responsibility for the creation of an anti-fraud culture rests jointly with all those involved in the Council in providing political direction, determining policy, and providing management and supervision. The Council expects that Members and

employees at all levels will actively promote an anti-fraud and corruption culture through:

- Endorsing and publicising the Council's Anti-Fraud and Corruption Policy,
- Being an example to others by ensuring adherence to legal requirements and the Council's internal rules and regulations, (e.g. Codes of Conduct, Financial Procedure Rules, Contract Standing Orders, Using Systems & Data Policy, etc.)
- Organising effective induction and training which should include briefings regarding expected standards of conduct, and references to anti-fraud and corruption arrangements
- Encouraging the reporting of any suspicions of fraud, corruption or deliberate irregularity by Members, employees, the public or any other third party with whom the Council works in providing services
- Treating seriously any suspicions reported to them and dealing sensitively with the person reporting the information
- Dealing swiftly and robustly with those who defraud the Council or who act corruptly
- Raising any concerns they may have regarding fraudulent or corrupt activity and maintaining effective internal control arrangements designed to combat fraud, corruption and irregularity.

4. Our Written Rules

4.1 The Council has in place a number of rules, codes of conduct and policies to ensure that financial, operational and organisational procedures are properly controlled. These are an important part of our internal control process, and it is important that all Members, employees and workers know about them.

4.2 The most important of these are as follows: -

- Constitution
- Financial Procedure Rules
- Financial Standing Orders
- Contract Standing Orders
- Code of Conduct for Council Employees
- Code of Conduct for Schools & Educational Settings
- Code of Conduct for Members
- Gifts & Hospitality Procedure
- Anti-Fraud & Corruption Policy
- Anti-Money Laundering Policy
- Anti-Bribery Policy
- Whistleblowing Policy
- Using Systems and Data Policy
- Information Sharing Policy
- Records Management Policy
- Scheme for Financing Schools and Schools Financial Procedures Manual

4.3 Individual departments have also introduced their own measures, which are designed to control their activities. Examples include schemes of delegation, accounting control procedures and procedural/operational manuals.

4.4 Managers in the individual departments must ensure that all employees and other workers have access to these procedures/manuals and receive suitable training.

4.5 Members, employees and workers must make sure that they read and understand the rules, code of conduct and policies that apply to them, and act in line with them.

4.6 Any Member, employee or worker who does not adhere to the rules, codes of conduct or policies may be subject to formal action, including disciplinary or legal action.

5. Expected Behaviour

5.1 All people and organisations that are in any way associated with Hackney Council are expected to be honest and fair in their dealings not only with the Council, its clients and customers but also in their dealings outside of the Council.

5.2 The Council expects Members and employees to lead by example in these matters.

5.3 The Code of Conduct for Council Employees forms part of the contract of employment, and it requires employees and workers to always work in accordance with the Anti-Fraud and Corruption Policy.

5.4 Council employees have an important part to play in combating fraud and corruption and they are expected to warn and provide information to Audit and Anti Fraud service if they suspect a case of fraud or corruption. Guidance on reporting such matters is available in the Council's Fraud Response Plan attached as Appendix 1. The Council's Constitution sets out that it is the responsibility of all Council officers to provide a full explanation and any information or document under their control, or access to any premises, facilities or systems, which is required for the purposes of an Internal Audit investigation. This expectation applies to not only the Council, but also associated bodies and partners including: -

i. organisations to which the Council has given grants;
ii. organisations with whom the Council contracts; and
iii. partner organisations in any scheme for which the Council has responsibility as lead body.

There is a requirement to include these access arrangements in written agreements with external partners.

5.5 The Audit and Anti Fraud service will deal with all referrals fairly ~~and confidentially~~ and as far as possible we will not reveal the names of the people who reported the matter to us. However, confidentiality cannot be guaranteed under all circumstances. For example, if an investigation leads to a prosecution and the person who reported the matter is required to give evidence in court. Section 6 below and the Council's Fraud Response Plan attached at Appendix 1 gives more advice on this issue for

both managers and staff. Our Anti Bribery Policy (Appendix 2) sets out the Council's approach to minimising the risk of corruption and bribery.

5.6 The Nolan Committee sets out the seven guiding principles that apply to people who serve the public. The Council has developed its working culture with these principles in mind. These principles are set out in Appendix 3.

5.7 Managers are expected to deal fairly and quickly with anyone who has or is suspected of committing fraud or acting corruptly. We may refer such matters to the police if we reasonably believe that a criminal offence has taken place.

6. Preventing Fraud and Corruption

6.1 The Council's approach is that steps should be taken to minimise the threat of ~~beat~~ fraud and corruption, we must prevent it from happening in the first place. It is essential that there are clear rules and procedures, within which Members, employees, consultants and contractors can work. These include the main rules, codes of conduct and policies set out in Section 4.2 above.

6.2 We will regularly review and update our written rules.

6.3 Managers are responsible for ensuring that suitable levels of internal check are included in working procedures, particularly financial procedures. It is important that duties are organised so that no one person can carry out a complete transaction without some form of checking process being built into the system.

6.4 Managers, in consultation with Human Resources, are responsible for ensuring that pre-employment screening checks appropriate to the nature of the post are carried out. These should include checks on identity, previous employment and permission to work in the UK, and may also include checks on qualifications, credit status and Disclosure & Barring Service checks. This applies to both permanent and temporary staff.

6.5 The Council is committed to working and co-operating with other organisations to prevent organised fraud and corruption. This may include being prepared to help and exchange information with other councils and organisations. This will be subject to any legal restrictions and the Council's own policies/procedures regarding the exchange of information.

6.6 The exchange of personal information will be properly controlled in line with appropriate legislation. The Audit & Anti-Fraud Service will adhere to and only exchange personal information in accordance with the Council's Information Sharing Policy and the Data Protection Act (DPA).

6.7 Confidential facilities are available for people to report fraud or corruption or give us information that may prevent the same. These include telephone hotlines, which members of the public as well as staff can use to give us information about specific services.

7. Whistleblowing

7.1 This section should be read in conjunction with the Council's Whistleblowing Policy, which sets out the types of concern that can be reported and is available on the intranet.

7.2 Although employees are expected to report their concerns, the Council recognises that this can be a difficult decision to make. If you report a concern in good faith you will have nothing to fear because you will be doing a service to the public and to the Council.

7.3 The Council will not tolerate any harassment or victimisation (including informal pressures) and will take appropriate action to protect you when you raise a concern in good faith. Any investigation into allegations that you raise of potential malpractice or wrongdoing will not influence or be influenced by any disciplinary, capability, redeployment or redundancy procedures that might separately apply to you.

7.4 The Council maintains an independent Whistleblower Hotline for staff provided by Navex that can be used if an individual feels unable to follow the standard reporting process set out at section 3.3 of the Fraud response Plan. To report a concern via the Whistleblowing Hotline please use this link or call **0800 890 011, followed at the prompt by the code 833 558 1923**. Contact details are also available from the Whistleblowing page on the Council's Intranet.

7.5 Concerns that are expressed anonymously will be considered, however, in our experience there is a greater likelihood of a successful investigation if the Audit and Anti Fraud Service are able to communicate directly with those who raise a concern.

7.6 Factors taken into account when deciding on appropriate investigation action would include: -

- The nature and seriousness of the issue raised
- The credibility of the concern
- The likelihood of confirming the allegation from attributable sources

7.7 If you make an allegation or raise a suspicion in good faith, but it is not confirmed by the investigations, no action will be taken against you. However, if during the investigation it is found that you made an allegation/raised a suspicion frivolously, maliciously or for personal gain, disciplinary action may be taken against you.

8. Detecting and investigating fraud and corruption

8.1 The Council's approach to detecting and investigating fraud and corruption is set out in the Council's Fraud Response Plan attached at Appendix 1. This also sets out the responsibilities upon all employees/workers to report their concerns, and what actions should be taken by employees/workers, managers and investigators.

8.2 The Council will take all steps available to us to recover any monies misappropriated from the Council.

8.3 The Audit and Anti Fraud service will communicate the outcomes of our investigations where appropriate (e.g. via internal bulletins and the press).

8.4 The External Auditor also has powers to investigate fraud and corruption.

9. Suspicions of Money Laundering

9.1 This section should be read in conjunction with the Council's Anti-Money Laundering Policy.

9.2 Money laundering is essentially the process by which the proceeds of crime and the true ownership of those proceeds are changed so that they appear to come from a legitimate source.

9.3 All employees have a clear obligation under the Terrorism Act 2000, the Proceeds of Crime Act 2002 (POCA) and the Money Laundering Regulations 2007 to report suspicions of money laundering and there can be severe penalties for individuals who fail to act in accordance with the legislation.

9.4 Employees must report any suspicions of money laundering to the Money Laundering Reporting Officer (MLRO) or Deputy Money Laundering Reporting Officer (DMLRO) (contact details at Appendix 1). Reporting suspicions in this way is essential to ensure that: -

- Suspected instances of money laundering are investigated properly
- There is a standard process for dealing with suspected cases of money laundering
- Individual's and the Council's interests are protected.

9.5 The MLRO or DMLRO will ensure that legislative requirements for investigating and reporting suspicions of money laundering are followed.

9.6 It is essential that employees do not do anything that could result in the suspect being alerted to the fact there is a suspicion regarding their activity or that the matter has been reported.

10. Fraud Awareness & Training

10.1 The Council recognises that the key to the continuing success of our anti-fraud culture depends upon maintaining a high level of fraud awareness among employees, workers and those who work with us.

10.2 The Council will provide training to support employees who use or manage internal control systems.

10.3 The Council will seek to ensure that the stance on fraud and corruption is widely publicised both internally and externally. All Members, employees, workers and other associated bodies/persons with whom the Council conducts its business will be

appropriately informed of this policy and the supporting framework as outlined in Section 4 above.

10.4 The Audit and Anti fraud service is committed to training and developing its staff who are involved in investigating fraud and corruption.

Document and version control

Document and version control	
Title of document	London Borough of Hackney Anti-Fraud & Corruption Strategy
Owner	Michael Sheffield
Job title of owner	Corporate Head of Audit, Anti-Fraud & Risk Management
Directorate	Finance and Corporate Resources
Approved by	Audit Committee
Publication date	tbc
For use by	All staff
Why issued	Corporate Policy
Review date	July 2025 (normal review will be biennial as minimum, with ad hoc review as necessary)

Version control details				
Version No.	**Author / editor**	**Version date**	**Approval date**	**Overview of changes**
V1.0	Michael Sheffield	1 June 2019	June 2019	
V2.0	Michael Sheffield	October 2023	tbc	Inclusion of officer and partner responsibilities as set out in the Constitution; Updated WB contact details; Clarity that staff can raise concerns with a more senior manager in the first instance if that is appropriate, and that managers must report concerns to AAF; Clarity on maintained school investigation remits.

Fraud Response Plan

1. Introduction

1.1 It is important that we do all we can to prevent and detect fraud to make sure that we can provide value for money services to residents and businesses within the Borough of Hackney honestly, efficiently.

1.2 Our Anti-Fraud and Corruption Policy sets out the principles we are committed to in relation to preventing, reporting, detecting and managing fraud/corruption and money laundering.

1.3 This fraud response plan sets out what employees and managers should do if they suspect fraud, corruption or money laundering.

1.4 It is the responsibility of the Audit & Anti-Fraud Service to investigate suspicions of fraud and corruption.

2. Definitions

Fraud:

The Fraud Act 2006 created an offence of fraud which can be committed in three separate ways: -

(i) False representation
A fraud will be committed if a person dishonestly makes a false representation and when doing so intends to make a gain or cause loss (or a risk of loss) to another.

(ii) Failing to disclose information
A fraud will be committed if a person dishonestly fails to disclose information where there is a legal obligation to do so and when doing so intends to make a gain or cause loss (or a risk of loss) to another.

(iii) Abuse of position
A person will commit fraud if they occupy a position in which they are expected to safeguard, or not act against, the financial interests of another person and they dishonestly abuse that position; and in doing so intend to make a gain or cause loss (or a risk of loss) to another.

Corruption:

The Bribery Act 2011 introduces three principle corruption offences:

(i) Bribing another person
An individual commits an offence if a financial or other advantage is offered, promised or given to another person for the improper performance of a function;

(ii) Being bribed
An individual commits an offence if a financial or other advantage is requested, agreed or received for the improper performance of a function;

(iii) Failure to prevent bribery
A corporate offence whereby the Council can be liable for the actions of those associated with it, if it has not taken reasonable steps to mitigate against this (see the Bribery Act Policy at Appendix 2 for details).

Money Laundering:

Money laundering, as defined in the Proceeds of Crime Act 2002 (POCA), is: -

(i) Concealing, disguising, converting or transferring criminal property, or removing it from the UK;

(ii) Entering into or becoming concerned in an arrangement which you know or should reasonably suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person;

(iii) Acquiring, using or possessing criminal property.

3. Procedures for Reporting Suspected Fraud and Corruption

3.1 We rely on our staff to help us to prevent and detect fraud and corruption or suspicions of money laundering. It is often members of staff who are in a position to spot any possible cases of fraud, corruption or money laundering at an early stage.

3.2 We require staff to tell us if they suspect fraud, corruption or money laundering.

3.3 We have specific reporting lines for fraud and corruption. You should first report the matter to your line manager or a more senior manager in your service area. If this is not appropriate, you should inform the Corporate Head of Audit, Anti-Fraud & Risk Management.

3.2 We also subscribe to an independent whistleblowers telephone hotline, which is run for us by an independent organisation, Navex. This allows concerns to be raised where the reporting person does not have confidence in the Council's internal arrangements for any reason. You can contact the whistleblowers hotline if you have information about a suspected case of fraud, corruption, money laundering and/or other irregularity but you do not feel able to follow the normal reporting procedures. Contact details are provided at Section 10 of this Fraud Response Plan.

3.3 The action that you take when you first find out about a suspected case of fraud, corruption, money laundering or irregularity might be vital to the success of any investigation that follows, so it is important that your actions are in line with the information given in this document.

4. Action by Employees

4.1 Under our Code of Conduct for Employees and Financial Procedure Rules, employees must report any suspected cases of fraud and corruption to their direct line manager, a more senior manager in your reporting line or, if that is not appropriate, to the

Corporate Head of Audit, Anti-Fraud and Risk Management. Reporting cases in this way ensures that: -

- Suspected cases of fraud and corruption are investigated properly;
- The Fraud Response Plan is carried out properly;
- There is a standard process for dealing with all suspected cases of fraud, corruption (including bribery) and money laundering;
- There is a corporate process for dealing with surveillance activity; and
- Individuals and the Council's interests are protected.

4.2 You should ensure that you are familiar with all of the rules, regulations, policies and procedures that are in place to assist you with your duties. You must not participate in fraudulent or corrupt acts.

4.3 If you suspect fraud, corruption or money laundering anywhere within the Council, you should do the following:

(i) Write down your concerns immediately. Make a note of all relevant details, such as what was said in phone or other conversations, the date, the time and the names of anyone involved.

(ii) In cases of suspected fraud or corruption, you must report the matter immediately to your line manager, a more senior manager in your chain of command or the Corporate Head of Audit, Anti-Fraud and Risk Management. Give that officer any notes you have made or any evidence you have gathered. Don't tell anyone else about your suspicions.

(iii) In cases of suspected money laundering, immediately advise the Corporate Head of Audit, Anti-Fraud and Risk Management, who is the Council's designated Money Laundering Reporting Officer (MLRO), or the Audit Investigation Manager (Deputy Money Laundering Reporting Officer, DMLRO). (See contact details at section 10 of this response plan.)

(iv) Help Audit & Anti-Fraud or another authorised organisations in any investigation.

4.3 Under **no circumstances** should you try to carry out an investigation yourself. This may damage any Audit & Anti-Fraud or subsequent investigation.

5. Action by Managers

5.1 If you find out about suspected fraud, corruption or money laundering in your work area, you should do the following: -

(i) Listen to the concerns of your staff and treat every report you receive seriously and sensitively. Staff should be encouraged to raise any concerns they have with their manager.

(ii) Make sure that all staff concerns are given a fair hearing. You should also reassure staff that they will not suffer victimisation because they have told you of their suspicions.

(iii) Get as much information as possible from the member of staff, including any notes and any evidence they have that may support the allegation. Do not interfere with any evidence and make sure it is kept in a safe place.

(i) Assess whether the suspicions are justified before you take the matter further.

5.2 **Do not** try to carry out an investigation yourself. This may damage any Audit & Anti-Fraud or subsequent investigation.

5.3 Report the matter immediately to the Corporate Head of Audit, Anti-Fraud and Risk Management. Do not tell anyone else about your suspicions.

5.4 Help Audit & Anti-Fraud or another authorised organisations in any investigation.

6. Audit & Anti-Fraud

6.1 Audit & Anti-Fraud is normally the appropriate unit to investigate cases of suspected fraud or corruption, so it is important that every suspicion is reported to the Corporate Head of Audit, Anti-Fraud and Risk Management.

6.2 The Corporate Head of Audit, Anti-Fraud and Risk Management, the Audit Investigation Manager and Investigators will work with managers to decide on the type and course of the investigation. This will include referring cases to the police where necessary. Where appropriate we will press for the prosecution of offenders.

6.3 If an investigation is likely to result in both a Police investigation and action under the Council's Disciplinary Policy & Procedure, then advice should be sought from the Corporate Head of Audit, Anti-Fraud and Risk Management and the Director of Human Resources & Organisational Development.

6.4 We will carefully consider ~~investigate~~ all referrals received to determine that the matters involved are appropriate for investigation, and to consider the potential for our enquiries to identify evidence and allow further action to be considered. Anonymous referrals will be assessed in the same way but they are often much harder to pursue so we would encourage anyone with concerns to refer the matter directly to the Corporate Head of Audit, Anti-Fraud and Risk Management if they do not feel they can raise the matter with their manager.

6.5 Experienced audit staff will manage fraud and corruption investigations. Any investigation that Audit & Anti-Fraud carries out will be in line with our procedures and legislation that applies to the conduct of these enquiries, including the Criminal Procedures and Investigations Act (CPIA) and the Police and Criminal Evidence Act (PACE).

6.6 Should surveillance be considered necessary during the course of an investigation this must be conducted in line with the Regulation of Investigatory Powers Act 2000 (RIPA) and the Council's own Surveillance and Communications Data policy. Failure to follow this policy could have severe consequences for the Council and only officers trained in this specialist area of investigations should carry out this activity. The Corporate Head

of Audit, Anti-Fraud and Risk Management is responsible for maintaining the Council's central record of RIPA authorisations.

6.7 Audit & Anti-Fraud will liaise with managers about the results of any investigation, and advise them what action they need to take.

6.8 If appropriate, feedback will also be provided to the person who initially raised the concerns.

7. Responsibilities if you are a worker who is the subject of an Audit & Anti-Fraud investigation

7.1 There is a responsibility on all officers of the Council, associated bodies or partner organisations (including organisations that the Council has provided grants to or contracted with) to provide any information, explanation or document under their control, or access to any premises, facilities or systems which is required in connection with any Audit & Anti-Fraud investigation.

7.2 Audit & Anti-Fraud investigations will be carried out in line with Divisional procedures and established best practice, and workers are required to cooperate with these arrangements.

7.3 Interviews with investigation subjects will ordinarily be audibly recorded, at the discretion of Audit & Anti-Fraud and in accordance with best practice and team procedures.

8. Actions Arising from Investigation

8.1 The Council's Anti-Fraud and Corruption Policy provides that dishonesty on the part of any Members, employees or any person or organisations involved in any way with the delivery of services to or on behalf of the Council will not be tolerated. Where fraud, corruption or irregularity is detected the Council will rigorously pursue appropriate action against the persons concerned including legal and/or disciplinary action, and wherever possible and deemed appropriate, we will take action to recover any losses suffered.

9. Schools

9.1 Hackney Council funds maintained schools and is also the ultimate employer of maintained school staff, even though staff are directly employed by the school governing body. The Council retains the right to investigate concerns of staff fraud, corruption and irregularity, the outcomes of these enquiries will be reported and it will be the responsibility of the school governing body to determine whether suspension, disciplinary or dismissal action in respect of their staff is appropriate.

10. Tenant Management Organisations (TMOs)

10.1 The Councils' statutory responsibility to properly administer its' financial affairs extends to the provision of housing services, including those provided by TMOs under the Right to Manage. Hackney retains its statutory obligations to ensure proper financial

administration including through provision of regular internal audit reviews and investigatory work if required.

11. Contact Details

Contact	Details
Council	
Corporate Head of Audit, Anti-Fraud and Risk Management (Money Laundering Reporting Officer) Michael Sheffield	Hackney Town Hall, Mare Street, London E8 1EA Tel: 020 8356 2505 Email: michael.sheffield@hackney.gov.uk
Audit Investigation Manager (Deputy Money Laundering Reporting Officer) Vinny Walsh	Hackney Town Hall, Mare Street, London E8 1EA Tel: 020 8356 2536 Email: vinny.walsh@hackney.gov.uk
External	
Navex Whistleblowing Hotline (Council's external hotline provider)	Tel: 0800 890 011, then at the prompt, 833-558-1923; alternatively reports can be made online by clicking here.
Protect (the whistleblowing charity)	The Green House 244-254 Cambridge Heath Road London E2 9DA Tel: 020 3117 2520 Website: https://protect-advice.org.uk/contact-protect-advice-line/

Anti Bribery Policy

Offences

The following offences were introduced as part of the Bribery Act 2011:

(i) **Section 1 - Bribing another person**

An individual commits an offence if a financial or other advantage is offered, promised or given to another person for the improper performance of a function;

(ii) **Section 2 - Being bribed**

An individual commits an offence if a financial or other advantage is requested, agreed or received for the improper performance of a function;

(iii) **Section 7 - Failure to prevent bribery**

The Council will be liable to prosecution if a person associated with it bribes another person intending to obtain or retain business or an advantage in the conduct of business for the Council. Organisations are liable to an unlimited fine if convicted for this offence.

Council position

The Council has a zero tolerance approach to all forms of fraud and corruption, including bribery. We expect all people working for the Council (permanent and fixed term employees, agency workers and contractors) and other organisations that carry out functions on our behalf to act honestly and with integrity, and comply with the spirit as well as the letter of the laws and regulations that are applicable to their work.

Corporate Responsibilities

The Council can demonstrate a commitment to preventing bribery by following government advice based around six key principles. Adherence to these principles will provide a full organisational defence to any Section 7 offence in the event that a case of bribery does take place. The six principles are as follows:

1. <u>Proportionate procedures</u>

This policy sets out the Council's stance on bribery. Our Financial Procedure Rules, Contract Standing Orders, Code of Conduct, Anti-Fraud and Corruption Policy and Gifts and Hospitality Guidance set out the standards and detailed procedures that workers should follow. These procedures are proportionate with the bribery risks that the Council faces and the nature, scale and complexity of the activities that we undertake.

2. <u>Top level commitment</u>

The Council's senior management are committed to preventing bribery by persons associated with it. Honesty and integrity is one of the seven principles of working at Hackney, we require that anyone working for the Council does not place themselves in a position where their honesty and integrity can be questioned, must avoid conflicts of

interest, and must make decisions fairly (including the award of contracts and when making appointments).

3. Risk Assessment

The Council is committed to on-going risk assessment of potential external and internal risks, including bribery, financial irregularity and other events that would damage its reputation

4. Due diligence

The Council applies due diligence procedures, taking a proportionate and risk based approach, in respect of persons who perform or will perform services for or on behalf of the council, in order to mitigate identified bribery risks.

5. Communication (including training)

The Council seeks to ensure that its bribery prevention policies and procedures are embedded and understood throughout the organisation, and that training will be provided which is proportionate to the Council's risk of exposure to bribery.

6. Monitoring and review

All Council procedures that relate to the prevention of bribery will be monitored and reviewed, and improved where necessary.

Gifts and hospitalities

This policy is consistent with the Council's gifts and hospitality procedures. These require that the offer of gifts and hospitality must always be recorded and the offer will ordinarily be refused unless it is of token value. The Gifts and Hospitality procedure sets out the very limited circumstances where an offer may be accepted and the process that has to be followed. The procedure also sets out that even the restricted circumstances that could lead to an offer being accepted will never apply if the entity offering the gift or hospitality is a potential Council supplier or employee, or is seeking planning permission from the Council.

Facilitation payments

These are small bribes paid to facilitate routine government action. Facilitation payments are not acceptable under the Council's Anti-Fraud and Corruption arrangements.

The Seven Principles of Public Life

Selflessness

Holders of Public office should take decisions in terms of the public interest. They should not do so in order to gain financial or other material benefits for themselves, their family, or their friends

Integrity

Holders of public office should not place themselves under any financial or other obligation to outside individuals or organisations that might influence them in the performance of their official duties.

Objectivity

In carrying out public business, including making public appointments, awarding contract, or recommending individuals for rewards and benefits, holders of public office should make choices on merit.

Accountability

Holders of public office are accountable for their decisions and actions to the public and must submit themselves to whatever scrutiny is appropriate to their office.

Openness

Holders of public office should be as open as possible about all the decisions and actions that they take. They should give reasons for their decisions and restrict information only when the wider public interest clearly demands.

Honesty

Holders of public office have a duty to declare any private interests relating to their public duties and to take steps to resolve any conflicts arising in a way that protects the public interest.

Leadership

Holders of public office should promote and support these principles by leadership and example.

.....

Note

These principles are a direct extract from the Nolan Committee report

Surveillance and Communications Data

Policy and Procedures

Audit & Anti-Fraud Division
October 2023

INDEX

INTRODUCTION

Hackney Council is committed to making the Borough a place for everyone, this involves building a fair and safe community.

The aim of this policy document is to: -

- explain the scope of the Regulations of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act (IPA) 2016 in so far as they apply to work undertaken by London Borough of Hackney;
- provide guidance on the authorisation procedures to be followed;
- provide a framework for carrying out surveillance both within and outside RIPA; and
- ensure that all the legal obligations on the Council are met, in particular the Human Rights Act 1998

Officers will be clear about the purpose of the monitoring and be satisfied that the particular method of surveillance chosen is justified.

This policy document is based upon the requirements of RIPA and the Home Office Code's of Practice on Covert Surveillance and Covert Human Intelligence Sources. The Council's use of surveillance powers and Covert Human Intelligence Sources is governed by RIPA 2000, our ability to obtain communication data falls under the IPA 2016. All Hackney officers (or its agents) are required to understand and follow this policy when involved in any of the above activities. Links to the following Home Office Codes of Practice are available here, these include -

- Surveillance COP
- Communications Data COP
- Covert Human Intelligence

If any officer is unsure about any aspect of this policy document or surveillance in general they should contact the council's Corporate Head of Audit, Anti-Fraud and Risk Management at the earliest possible opportunity, for advice and guidance.

Audit & Anti-Fraud regularly coordinate training for officers who may need to use or approve surveillance powers. Any person wishing to apply for, or authorise, activity under RIPA must have completed the most recent training, and anyone who attends court to seek judicial approval for surveillance activity must be authorised to do so under section 223 of the Local Government Act 1972. Any use of the powers to obtain communications data under the IPA 2016 must be carried out through the National Anti-Fraud Network (NAFN), applicants must have completed the NAFN training and follow the requirements set out at Part 3 of this Policy.

All investigations that involve covert surveillance or requests for information relating to communications data are open to inspection and scrutiny by the Investigatory Powers Commissioners Office (IPCO) and are subject to review. The reviews will highlight inconsistencies and any necessary improvements needed to comply with the

legislation. It is essential, therefore, that all surveillance is appropriately authorised in accordance with this policy document.

RIPA regulates the use of a range of covert techniques by public authorities including local authorities. The more intrusive techniques such as interception can only be used by law enforcement and intelligence agencies.

Local authorities are only able to use the least intrusive types of investigatory techniques set out by RIPA and IPA, these include:

- directed surveillance e.g. covert surveillance in public places
- covert human intelligence sources e.g. informants, undercover officers, and
- acquisition of communications data.

Local authorities may only use these powers for preventing or detecting crimes which attract a maximum custodial sentence of 6 months or more or criminal offences relating to the underage sale of alcohol or tobacco.

The above techniques are described in more detail later in this policy document.

REGULATION OF INVESTIGATORY POWERS ACT 2000

PART 1 – DIRECTED SURVEILLANCE

1.1 What is Surveillance

Surveillance can involve monitoring, observing or listening to people. This includes their movements, conversations, activities or other communications or recording anything with a surveillance device.

Overt Surveillance takes place where the surveillance is not hidden, such as alerting the public to the use of CCTV in a public place. Overt surveillance does not require authorisation.

Covert Surveillance is where the person or people under observation are not aware that surveillance is taking place.

Directed Surveillance is covert in nature but is not intrusive. It shall also be undertaken for a specific investigation/operation, which is likely to result in private information about a person being obtained.

All directed surveillance carried out by Hackney officers must be authorised.

Intrusive Surveillance is covert surveillance which is carried out in relation to anything taking place on any residential premises or in a private vehicle and involves the presence of an individual on the premises, on the vehicle or is carried out by means of a surveillance device.

NB – Councils are not permitted to authorise intrusive surveillance. Hackney officers can only conduct intrusive surveillance if they are involved in surveillance with other enforcement agencies with higher authorisation powers (e.g. Police, HM Revenue & Customs, etc) in which case the authorisation would be obtained by the other agency.

In cases of surveillance on members of the public, it is clear that the Council is acting as a public authority. This means that the Human Rights Act and RIPA apply. In cases where an employee is under investigation, the Council's role is that of an employer and not a public authority. RIPA does not apply in these cases, although we will still follow the principles established by the legislation when undertaking surveillance for this reason. It is likely that any tribunal hearing employee cases involving surveillance will consider human rights issues when making decisions. Furthermore, if the employee is under investigation for a criminal offence, the Council will be able to obtain a RIPA authorisation for covert surveillance if it is necessary and proportionate.

Covert surveillance can only be justified where other investigation methods would not obtain the necessary evidence.

Who is Authorised to Conduct Surveillance?

The Council has been empowered by statute to enforce various offences within its borough. Such powers are exercised by officers on behalf of the Council.

Undertaking surveillance is incidental to the enforcement of such powers and therefore authorised under Section 111 of the Local Government Act 1972.

Officers of the Council, however, would need to ensure that any covert surveillance has been properly authorised as laid out in this policy document.

The authorisation, renewal and cancellation procedures detailed below should be followed and the standard Home Office RIPA forms that have been adapted for Hackney are to be utilised for these purposes. All forms are available via the Council's RIPA Co- ordinator.

If contractors and/or agents of the Council are authorised to undertake public functions on behalf of the Council an authorisation under RIPA may be required for the purposes of the work they do for the Council if it involves covert surveillance. Therefore, the authorisation procedures below must be followed prior to any covert surveillance being conducted by them.

1.2 Seeking Authorisation

In all instances Investigating Officers (IO) should contact the RIPA Co-ordinator to obtain the relevant form and Unique Reference Number (URN) at the start of the application process (see section 4.2). The URN must be written on the form.

The IO must always consider if there is a less intrusive way to gather information that is required to progress their investigation. If the IO considers it necessary to undertake surveillance as part of an investigation, they must complete an Application for Authority for Directed Surveillance Form.

The form must record why the IO considers surveillance necessary and proportionate to what is hoped to be achieved. When considering an application officers need to be aware of the following requirements: -

Necessity - covert surveillance shall only be undertaken where it is designed to achieve a legitimate objective. The only ground for which directed surveillance can be authorised by the Council under RIPA is to prevent or detect crime

Proportionality - the use and extent of covert surveillance shall not be excessive i.e. it shall be in proportion to what the investigation seeks to achieve. It must be specific and not designed to cover a wide range of situations. The IO shall make an assessment of the duration of the surveillance or each stage of the surveillance and the resources to be applied.

The IO must show that consideration of the size and scope of the operation against thegravity and extent of the perceived criminality ~~mischief~~ has taken place. They must also explain how and why the methods to be adopted will cause the least possible intrusion on the target and others, that the activity is an appropriate use of

the legislation and that it is the only reasonable way (having considered all others) of obtaining the desired result. The application should include details of other methods considered and why they were not implemented.

Collateral Intrusion - reasonable steps shall be taken to minimise the intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation being carried out. The officer shall also consider how any third party information obtained will be handled. The IO should record any collateral intrusion that might occur. Collateral intrusion occurs when individuals who are not part of the surveillance are unintentionally included in the course of the surveillance. For example, where photographing a target at a specific location includes members of the public being photographed.

Subsidiarity – the surveillance must cause no greater invasion of the right to privacy than is absolutely necessary to achieve its objective. All other means must be considered prior to surveillance being deemed necessary.

Confidential Information – confidential personal information (such as medical records or spiritual counselling), confidential journalistic material, confidential discussions between Members of Parliament and their constituents, or matters subject to legal privilege.

Special consideration must be given to authorisations that involve confidential personal information. Where such material has been acquired and retained the matter should be reported to the relevant Commissioner or Inspector during their next inspection and the material made available if requested

NB. Where there is a likelihood that information acquired will be Confidential Information, then the authorisation must be from the Head of Paid Service or, in their absence, a Group Director nominated by the Head of Paid Service to deputise for them.

Serious Crime Threshold – Local Authorities can only grant an authorisation under RIPA for the use of directed surveillance to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment or are related to the underage sale of alcohol or tobacco. Local authorities can no longer authorise the use of RIPA to investigate disorder that does not involve a criminal offence below this serious threshold which may include, for example, littering or dog control.

If during the investigation it becomes clear that 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 threshold, the use of directed surveillance should cease. If a directed surveillance authorisation is already in force it should be cancelled.

1.3 Role of the Authorising Officer (AO)

AOs must ensure that they are satisfied that the covert surveillance is necessary and proportionate.

An AO should consider all information provided on the Application for Authority for Directed Surveillance and if necessary ask for further information from the IO. When authorising the application the AO should write down exactly what they are authorising; i.e., who, what, where, when and how. All authorities must be signed, showing the date and time the authority was granted.

The AO should return the completed form to the IO who should keep a copy on the investigation file.

The original form will need to be presented at the judicial approval hearing prior to being forwarded to the RIPA Co-ordinator marked 'private and confidential' for filing on the central file. (see para 1.5 below)

1.4 Applying for Judicial Approval

The Protection of Freedom Act 2012 amended RIPA to require judicial approval following local authority authorisation. Following authorisation by the AO the IO should contact Thames Magistrate Court, 58 Bow Road, London E3 4DJ on telephone number 020 8271 1203 to arrange a date and time for a hearing.

The IO or another appropriate officer of the Council (e.g. RIPA Co-ordinator) will need to attend the court in person to apply for judicial approval. When attending court the IO must provide the following documents to the Magistrate/Justice of the Peace (JP): -

- the original RIPA authorisation and any supporting documents setting out the case – this will need to be shown to the JP but will be retained by the IO to file in the Council's central record on return from the hearing;
- a copy of the original RIPA authorisation and any supporting documents setting out the case for retention by the JP;
- two copies of the partially completed Judicial Application/Order Form.

The order section of this form will be completed by the JP and is the official record of the JP's decision. The JP will retain one copy of this form and the other is returned to the IO to be retained on the Council's central record.

The judicial approval of the authorisation will only be given if the Magistrate/JP is satisfied that:

1. There were reasonable grounds for the Authorising Officer approving the application to believe that the covert directed surveillance or deployment of CHIS (covert human intelligence source, see Part 2 of this Procedure) was necessary and proportionate and that there remain reasonable grounds for believing so.
2. The Authorising Officer was of the correct seniority within the organisation i.e. Director, Head of Service, Service Manager or equivalent as per the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521).
3. The granting of the authorisation was for the prescribed purpose, as set out in the 2010 order, i.e. preventing or detecting crime and satisfies the newly introduced 'Serious Offence Test' for directed surveillance. In addition, where

the authorisation is for the deployment of a CHIS, the Magistrate must be satisfied that:

a. Provisions of S29(5) have been complied with. This requires the local authority to ensure that there are officers in place to carry out roles relating to the handling and management of the CHIS and the keeping of records.
b. Where a CHIS is under 16 or 18 years old, the requirements of the Regulation of Investigatory Powers (Juveniles) Order 2000 have been satisfied. This sets out the rules about parental consent, meetings, risk assessments and the duration of the authorisation.
c. Where the application is for the renewal of a CHIS authorisation, a review has been carried out by the local authority and the Magistrate has considered the results of the review.

NB. Judicial approval is required for all applications and renewals; there is no requirement for the JP to consider either cancellations or internal reviews.

1.5 Out of Hours Authorisations

In exceptional circumstances a JP may consider an authorisation out of hours. If the authorisation is urgent and cannot be handled the next working day then the IO should first obtain authorisation from the AO before phoning the court's out of hours HMCTS legal staff contact. You will need to provide basic facts and explain the urgency. If urgency is agreed arrangements will be made to see a suitable JP. As with the normal JP approval process the IO will need to provide two copies of both the authorised RIPA application form and the accompanying judicial application/order form.

Local authorities are no longer able to orally authorise the use of RIPA as all authorisations require judicial approval which must be made in writing. The authorisation cannot commence until this has been obtained.

1.6 Training

The role of an AO carries great responsibilities for the AO as well as the staff involved in the surveillance operation, the Council and members of the public. In order to protect the Council from the risk of misuse of the powers under RIPA no one will be permitted to carry out the role of an AO without having first undergone approved training. All AO's will be expected to undertake refresher training. The Corporate Head of Audit, Anti-Fraud and Risk Management should be contacted for further information.

1.7 Length of Authorisation

A written authorisation will last for up to three months unless cancelled or renewed.In all cases regular reviews should be carried out and an authorisation should be renewed or cancelled before the expiry of the original authorisation.

1.8 Surveillance Equipment – Control/Inventory

The Council will maintain a central inventory of all technical equipment capable of being used for covert surveillance. The central inventory will be maintained by the RIPA Co-ordinator as part of the Council's central records. It is the responsibility of the Service Head to ensure the issue and use of any equipment held by the service for the purpose of conducting covert directed surveillance (e.g. radios, cameras, etc) is correctly recorded and usage is subject to audit.

NB. The use of such equipment should be specified in the authorisation.

1.9 Use of CCTV Control Room

The provisions of RIPA do not cover the use of overt CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime. However, if the CCTV becomes 'directed' in any way as part of a covert operation towards an individual, authorisation must be obtained. In some circumstances police officers may ask for our cameras to be targeted at individuals or buildings, as part of their operations. In these circumstances the officer directing the CCTV should satisfy him/herself that the police have obtained proper authorisation. CCTV surveillance carried out as an immediate response to an event does not require authorisation.

If an LBH directed surveillance operation is to include the use of CCTV equipment then the Hackney IO must obtain a RIPA authorisation in the usual way. If CCTV is required for a Police directed surveillance operation they must complete Form 5429. This document is the unified protocol in which RIPA authorised use of CCTV for Directed Surveillance activity will be passed to the Public Space Surveillance Team. It must be Shared with the Public Space Surveillance Manager. In all cases only one form is required for the duration of an operation. To book the CCTV Centre for a pre-planned operation, IOs can contact 020 8356 2323 or cctv.leader@hackney.gov.uk, in advance. The Police (unlike local authorities) are able to undertake directed surveillance on the basis of a verbal authorisation in some circumstances. In the event of an urgent verbal authorisation to utilise CCTV Service cameras, this must be followed up with Form 5429.

1.10 Internet and Social Media Investigations

Information obtained from the internet must comply with all the normal rules and guidance applicable to any type of enquiry conducted within a criminal investigation, such as, the Data Protection Act (DPA), Criminal Procedures Investigations Act (CPIA) and RIPA. The use of the internet to gather information prior to and/or during an operation may amount to directed surveillance. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought as set out in this procedure. Where an investigator may need to communicate covertly online, for example, contacting individuals using social media websites, a CHIS authorisation should be considered.

Where privacy settings are available but have not been applied the data available

on social networking sites may be considered 'open source' and an authorisation is not usually required.

Repeat viewing of 'open source' sites, however, may constitute directed surveillance and this should be borne in mind e.g. if someone is being monitored through, for example, their Facebook profile for a period of time and a record of the information is kept for later analysis, this is likely to require a RIPA authorisation for directed surveillance.

1.11 Reviews

The AO should ensure that they review the authorisation at least monthly in order to satisfy themselves that authority should continue. Evidence of this review should be completed on the Review of Directed Surveillance Form.

1.12 Renewals

There may be circumstances where the investigation requires surveillance to take place for a period longer than 3 months. In such cases, it will be necessary for the IO to obtain a renewal of authority from the AO and the JP.

The IO should submit a renewal form with a copy of the original Application for Authority for Directed Surveillance to the AO. The AO must review both documents to ensure that there is continuing justification for surveillance. A copy of the renewal form should be placed on the investigation file.

The IO must arrange a hearing with the JP for judicial approval. All authorisations must be renewed prior to the expiry date of the original authorisation but will run from the expiry date and time of the original authorisation. Applications for renewal should be made shortly before the original authorisation period is due to expire. IO's must take account of factors which may delay the renewal process (e.g. weekends or the availability of the AO and JP to grant approval).

The original renewal form will need to be presented at the judicial approval hearing prior to being forwarded to the RIPA Co-ordinator marked 'private and confidential' for filing on the central file.

1.13 Cancellations

Surveillance should be no longer than necessary to gather the required information. The AO must cancel the authorisation if satisfied that the directed surveillance is no longer required.

The IO should complete a Cancellation of Directed Surveillance Form providing information which should include a record of the date and time (if at all) that surveillance took place and when the order was made to cease the activity and the reason for the cancellation. The completed form should be passed to the AO who should ensure when countersigning the form that surveillance equipment has been removed, any property interfered with or persons subjected to surveillance since the last review or renewal is properly recorded and that a record is made of the value of the surveillance (i.e. whether the objectives as set in the authorisation were met).

The AO must make reference on the cancellation form to the handling, storage and destruction of any material obtained from the directed surveillance. The AO must ensure compliance with the Data Protection Act and the Council's own corporate retention policy.

A copy of the cancellation form should be placed on the investigation file and the original sent marked 'private and confidential' to the RIPA Co-ordinator to place on the central file.

1.14 When Authorisation is Not Required

Test Purchases

When enforcement staff undertake general observations as part of their everyday functions, this low level activity will not usually be regulated under the provisions of RIPA. For example, Trading Standards might observe and then visit a shop as part of their enforcement function to verify the supply or level of supply of goods or services that may be liable to a restriction or tax. A CHIS authorisation is unlikely to be necessary because the purchase activity does not normally constitute a relationship, but if a number of visits are undertaken to the same business to encourage familiarity then a relationship may be established and a CHIS might be appropriate.

Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, but not amount to systematic surveillance of an individual. If covert technical equipment is worn by the test purchaser, or an adult is observing the test purchase, authorisation for directed surveillance is required.

Automatic Number Plate Recognition (ANPR)

Automatic Number Plate Recognition (ANPR) is primarily used for the purposes of managing traffic, road safety and enforcement - this overt use does not require RIPA approval. However, ANPR can be used as a surveillance tool if it is targeted at suspected offending and the use is planned in advance, for example, to establish the circumstances under which a fraudulent blue badge is being used. If ANPR is used to monitor vehicles in this way then a directed surveillance authorisation should be requested.

Non-RIPA Surveillance

A RIPA authorisation can only be granted where the serious crime threshold is met (see section 1.2above). Local authorities undertake many types of investigation which do not meet this threshold, but where surveillance may be necessary to establish the facts of the case, for example:

- Staff disciplinary investigations (undertaken in accordance with the ICO Employment Practices Code);
- Anti-social behaviour disorder which does not attract a maximum custodial sentence of at least six months imprisonment;
- Safeguarding vulnerable people;

- Planning enforcement prior to the serving of a notice or to establish whether a notice has been breached.

Surveillance for these purposes may still impact people's HRA article 8 right to privacy, so the surveillance activity must consider necessity and proportionality. The approval process for non-RIPA surveillance requires that a non-RIPA application form is completed and authorised, to the same standard as would be expected for a standard RIPA case. The non-RIPA application form must be obtained from the RIPA monitoring Officer to ensure that the Council maintains a single central record of all surveillance activity.

The RIPA codes also provide guidance that authorisation under RIPA is not required for the following types of activity:

- General observations as per section 3.33 in the codes of practice that do not involve the systematic surveillance of an individual or a group of people and should an incident be witnessed the officer will overtly respond to the situation.
- Surveillance where no private information is likely to be obtained.
- Surveillance undertaken as an immediate response to events.
- The covert recording of noise where the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm), or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear. In the latter circumstance, the perpetrator would normally be regarded as having forfeited any claim to privacy. In either circumstance this is outside of RIPA.

PART 2 – COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

This is a sensitive area of activity and as a general rule the Council will not undertake surveillance that relies upon the use of a CHIS. Furthermore, there are special provisions for the use of vulnerable and juvenile sources (i.e. under the age of 18). Advice should be sought from the Corporate Head of Audit, Anti-Fraud and Risk Management and Legal Services prior to any authorisations being requested.

In some instances, the tasking given to a person will not require the CHIS to establish a personal or other relationship for a covert purpose. For example a CHIS may be tasked with finding out purely factual information about the layout of commercial premises. Alternatively, a trading standards officer may be involved in the test purchase of items that have been labelled misleadingly or are unfit for consumption. In such cases, it is for the IO and AO to determine where, and in what circumstances, such activity may require authorisation.

2.1 Use of a Covert Human Intelligence Source

A CHIS may be an undercover officer or informant carrying out enquiries on behalf of the Council

Under Section 26(8) of the Act a person is a CHIS if they:-

1. establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (ii) or (iii) below;

2. covertly uses such a relationship to obtain information or to provide access to any information to another person; or

3. covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A relationship is established or maintained for covert purposes if and only if it is conducted in a way that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

All operations involving a CHIS must be approved, prior to a request for authorisation, in principle by the Team Leader or Investigation Manager. The purpose of this in principle approval is to ensure that officers handling and controlling the CHIS are doing so with proper authorisation and training. After initial approval the IO must complete an Application for Authorisation for the Use or Conduct of a CHIS. This form must be authorised by an Authorising Officer.

There is no need to seek authority where the information source is a member of the public who freely provides information that has come to them during their normal activities, for example where we ask a neighbour to keep a nuisance or harassment diary while going about their normal daily activities. However, authority must be obtained if the IO directs the CHIS activities.

2.2 Public Authority Responsibilities

Public authorities should ensure that arrangements are in place for the proper oversight and management of CHIS's, including appointing individual officers as defined in the Act for each CHIS.

The Act terms this person a Handler, they will have day to day responsibility for: -

- dealing with the CHIS on behalf of the authority concerned;
- directing the day to day activities of the CHIS;
- recording the information supplied by the CHIS; and
- monitoring the CHIS's security and welfare;

The person referred to in the Act as a Controller will be responsible for the general oversight of the use of the CHIS.

Controllers should not normally be the AO. Handlers will normally be at least one management tier below the Controller. This may or may not be the IO.

In cases where the authorisation is for the use or conduct of a source whose activities benefit more than a single public authority, responsibilities for the management and oversight of that source may be taken up by one authority or can be split between the authorities; in either case record keeping will be required.

Records relating to each CHIS must be maintained that are compliant with Statutory
Instrument 2725. A link to this can be found here.

2.3 Security and Welfare

Any public authority deploying a CHIS should take into account their safety and welfare when carrying out actions in relation to an authorisation or tasking, and any foreseeable consequences to others of that tasking. Before authorising the use or conduct of a CHIS, the AO should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking, and the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS after the cancellation of the authorisation should also be considered.

The Handler is responsible for bringing to the attention of the Controller any concerns about the personal circumstances of the CHIS, insofar as they might affect: -

- the validity of the risk assessment
- the conduct of the CHIS, and
- the safety and welfare of the CHIS.

Where deemed appropriate, concerns about such matters must be considered by the AO, and a decision taken on whether or not to allow the authorisation to continue.

2.4 Authorising the use of a CHIS

The decision on whether or not to authorise the CHIS rests with the AO followed by judicial approval by a Magistrate/Justice of the Peace (JP). Full details must be included in the authorisation form of the reason for the use of CHIS and outcomes which the CHIS activity is intended to produce. Officers must give significant thought to collateral intrusion (i.e. those who are unconnected with the subject, who may be affected by the CHIS and what private information may be obtained about them). The authorisation request should be accompanied by a risk assessment form detailing how the CHIS is going to be handled and the arrangements which are in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the source.

The use of the CHIS must be proportionate to the offence being committed. It should also be used only when other methods of less intrusive investigation have been attempted or ruled out . The application form must include details of the resources to be applied, the anticipated start date and duration of the CHIS activity, if necessary broken down over stages. CHIS authorisation forms should include enough detail for the AO to make an assessment of necessity and

proportionality (see Section 1.2). Each request should detail the nature of the source activity and the tasking which is to be given.

The original form will need to be presented at the judicial approval hearing prior to being forwarded to the RIPA Co-ordinator marked 'private and confidential' for filing on the central file. (see para 2.7 below)

NB. Where the CHIS is a juvenile or a vulnerable person, then the authorisation must be from the Head of Paid Service or, in their absence, a Group Director nominated by the Head of Paid Service to deputise for them.

2.5 Tasking a CHIS

Each CHIS will be managed through a system of tasking and review. Tasking is the assignment given to the CHIS by either the Handler or Controller. The task could be asking the CHIS to obtain information, to provide access to information or to otherwise act for the benefit of the Council. The Handler is responsible for dealing with the CHIS on a day to day basis, tasking them, recording the information provided by the CHIS and monitoring the CHIS's security and welfare. The Controller will have general oversight of these functions.

A CHIS may wear or carry a surveillance device for the purpose of recording information. The CHIS may not leave devices on the premises after they have departed, as this would constitute intrusive surveillance.
It is not the intention that authorisations be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the CHIS's task. If this changes, then a new authorisation may need to be sought.

It is difficult to predict exactly what might occur each time a meeting with a CHIS takes place, or the CHIS meets the subject of an investigation. There may be occasions when unforeseen actions or undertakings occur. When this happens, the occurrence must be recorded as soon as practicable after the event and, if the existing authorisation is insufficient it should either be updated and re-authorised (for minor amendments only) or it should be cancelled and a new authorisation obtained before any further such action is carried out.

Similarly where it is intended to task a CHIS in a new way or significantly greater way than previously identified, the persons defined as the Handler or Controller must refer the proposed tasking to the AO, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and the details of such referrals must be recorded.

2.6 Length of Authorisation

Written CHIS authorisations last for 12 months (four ~~one~~ months if the CHIS is under 18). They may be renewed prior to expiry for additional 12 month increments (four months if the CHIS is under 18). Activity should be cancelled as soon as it is no longer required. CHIS authorisations should not be left in place once cancellation becomes appropriate.

In all cases regular reviews should be carried out and a renewal or cancellation must be undertaken no more than one month from the date of the original authorisation.

2.7 Applying for Judicial Approval

Following authorisation by the AO the IO should contact Thames Magistrate Court, 58
Bow Road, London, E3 4DJ on telephone number 020 8271 1203 to arrange a date and time for a hearing.

The IO (or another appropriate officer of the Council, e.g. the RIPA Co-ordinator) will need to attend the court in person to apply for judicial approval. When attending court the IO must provide the following documents to the Magistrate/Justice of the Peace (JP): -

- The original RIPA CHIS authorisation and any supporting documents setting out the case – this will need to be shown to the JP but will be retained by the IO to file in the Council's central record on return from the hearing;
- A copy of the original RIPA CHIS authorisation and any supporting documents setting out the case for retention by the JP;
- Two copies of the partially completed Judicial Application/Order Form. The order section of this form will be completed by the JP and is the official record of the JP's decision. The JP will retain one copy of this form and the other is returned to the IO to be retained on the Council's central record.
- There is no need for the JP to know the true identity of the CHIS. Extreme caution needs to be taken with any documentation that reveals the true identity of the CHIS.

NB. Judicial approval is required for all applications and renewals; there is no requirement for the JP to consider either cancellations or internal reviews.

2.8 Reviews

The AO should ensure that they review the authorisation on a regular basis in order to satisfy themselves that authority should continue. Each operation should be reviewed after the key stages have been completed. The responsibility for the review rests with the AO. Details of the review should be recorded on an appropriate form and retained with the original authorisation held by the RIPA Co-ordinator, a copy should also be held on the investigation file. Cases should be reviewed at no more than one-month intervals. Evidence of this review should be completed on the Review of the Use of a CHIS Form.

2.8 Renewals

There may be circumstances where the investigation requires a CHIS for a period longer than 12 months. In such cases, it will be necessary for the IO to obtain a renewal of authority from the AO.

The IO should submit a renewal form with a copy of the original Application for Authorisation of the Use or Conduct of a CHIS to the AO. The AO must review both

documents to ensure that there is continuing justification for surveillance.

The IO must arrange a hearing with the JP for judicial approval. All authorisations must be renewed prior to the expiry date of the original authorisation but will run from the expiry date and time of the original authorisation. Applications for renewal should be made shortly before the original authorisation period is due to expire. IO's must take account of factors which may delay the renewal process (e.g. weekends or the availability of the AO and JP to grant approval).

The original renewal form will need to be presented at the judicial approval hearing prior to being forwarded to the RIPA Co-ordinator marked 'private and confidential' for filing on the central file. A copy of the renewal form should also be placed on the investigation file.

3. Cancellations

The use of a CHIS should be no longer than necessary to gather the required information. The IO must complete a Cancellation of the Use or Conduct of a CHIS Form to pass to the AO to enable the AO to cancel the authorisation if satisfied that the use of the CHIS is no longer required. A copy of the cancellation form should be placed on the investigation file and the original sent marked 'private and confidential' to the RIPA Co-ordinator to place on the central file.

PART 3 – COMMUNICATIONS DATA (INVESTIGATORY POWERS ACT 2016)

3.1 What is Communications Data

Communications data is the 'who', 'when', and 'where' of a communication but NOT the
'what' (i.e. the content of what was said or written in any communications).

Communications data covered by the Act includes such items as the following: -

- details written on the outside of a postal communication
- details relating to the sender/recipient of an email communication
- telephone/mobile phone subscriber checks
- Handset, cell site and GPRS data

A different threshold of what constitutes serious crime applies to Investigatory Powers Act applications for communications data, i.e. any of the following:

- An offence that attracts a sentence of 12 months imprisonment or more;
- An offence that involves a large number of people acting for a common purpose;
- Any offence by a body corporate;
- Any offence involving sending a communication or breach of privacy; or
- Any offence involving significant financial gain.

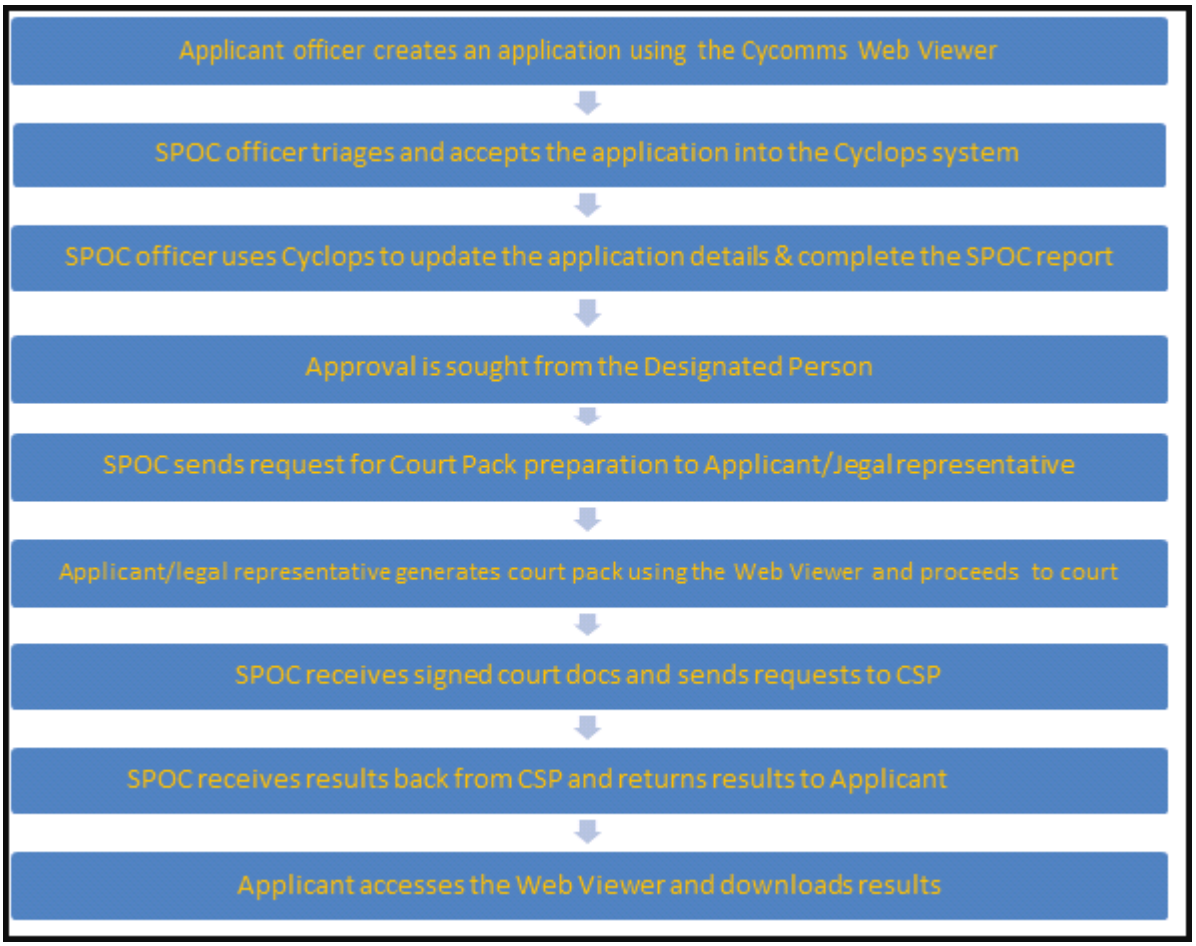
Communications data requests also need to set out why provision of the information will be proportionate to the matter being investigated, and make clear why the application is necessary in the context of the specific case.

3.2 Communications Data Applications

All communications data applications are now made under the IPA 2016, not RIPA. Local Authority applications for communications data must be channelled through the National Anti-Fraud Network (NAFN), an organisation that Hackney subscribes to. The chart below sets out the NAFN application process, the roles are as follows:

- **Applicant** - the LBH investigator requesting communications data via NAFN;
- **Approved Rank** - a nominated LBH manager who will be notified of (but does not authorise) any communications data request that is sent to NAFN. Note that any service requesting communications data must first notify a senior person to act in the AR role.
- **Single Point of Contact** (SPOC) - the NAFN officer that receives the application NAFN officer
- **Designated Person** - a role that sits with the regulator (the Office for Communications Data Authorisations), the person that provides authorisation for information to be provided
- **Communications Service Provider** (CSP) - the data provider
- **Senior Responsible Officer** (SRO) - the LBH officer with responsibility for the IPA process, including engagement with the regulators.

NAFN IPA Process



If an investigator considers it necessary to obtain communications data as part of an investigation, they must complete an application form requesting communications data to be obtained and disclosed using the NAFN CycComms system. All applicants will need to register with NAFN using the Hackney corporate membership at nafn.gov.uk prior to making an application on the online system, and complete the Comms Data training module available on the NAFN site.

The application form must record why the investigator considers this data necessary and proportionate to what is to be achieved, (see section 1.2) and should include any source material. The investigator must ensure that all paperwork and decision documents are stored securely.

All requests for communications data must be recorded on the Hackney spreadsheet, this is administered by the RIPA co-ordinator and details of any data requests should be notified to the RIPA co-ordinator by email.

Communications data applications requesting traffic data must reach the serious crime threshold. If an application for communications data is no longer required then the application MUST be cancelled.

PART 4 – RECORD KEEPING & MONITORING

Record Keeping

4.1 Senior Responsible Officer (SRO)

The Corporate Head of Audit, Anti-Fraud and Risk Management is the SRO and is responsible for the integrity of the process in place with the local authority to authorise directed surveillance, ensure compliance with the Act, engage with the Commissioners and Inspectors when they conduct their inspections and where necessary, overseeing the implementation of any post-inspection action plans recommended and or approved by the Commissioner.

4.2 RIPA Co-Ordinator

The RIPA Co-Ordinator duties include: -

- Retaining copies of the forms for a period of at least 5 years;
- Maintaining the Central Register (a requirement of the Codes of Practice) of all of the authorisations, renewals and cancellations;
- Issuing the unique reference number that is necessary for all surveillance applications;
- Keeping a database for identifying and monitoring expiry dates and renewal dates.
- In conjunction with the SRO, other authorising officers and investigation officers, ensure that electronic and paper records relating to a RIPA investigation are used, retained or destroyed in line with the Councils Information Management policies, departmental retention schedules and the Data Protection Act 2018.
- Provide administrative support and guidance, promote consistent practice and monitor compliance with this policy;
- Facilitate RIPA training and regularly review the contents of this Policy.

Hackney must maintain a central record of all RIPA authorisations, reviews, renewals and cancellations, which shall be made available to the Investigatory Powers Commissioner's Office (IPCO) as part of any inspection.

In all instances of directed surveillance, IOs should contact the RIPA Co-ordinator to obtain a Unique Reference Number (URN) at the start of the application process. This number must be written on the form in the box provided. A sequential numbering system is in place to enable ease of identification. The RIPA Co-ordinator will supply a unique reference number (URN) at the outset of the application for authorisation that all departments will be required to use for directed surveillance. An authorisation will be identified in the following manner: -

Dept / Div / Investigation case no / URN - e.g.
FCR/AAF/xxxxx/01

CHE/ILLOCC/001/01
NB – Additional identification numbers as highlighted below should be inserted on forms by the IO to identify the type of form. See examples below.

Reviews - Insert 'RV' before the authorisation number (e.g. FCR/AAF/001/RV0225)
Renewals - Insert 'RN' before the authorisation number (e.g. CHE/ILLOC/001/RN01)
Cancellations - Insert 'C' before the authorisation number (e.g. CHE/TS/001/C07)

The RIPA Co-ordinator will ensure that the confidential central record is updated. Forms relating to the authorisation for the use of a CHIS will be held on a separate file along with the risk assessment form. A central file will be maintained for the CHIS, Handlers and Controllers and this will also be held by the RIPA Co-ordinator. In addition individual Control Sheets will be maintained for directed surveillance, CHIS and communications data. This sheet will include information on the authorisations, reviews, renewals and cancellations as well as an indication of any confidential information obtained and whether the urgency provisions were used.

All applications (including those refused by an AO), authorisations, renewals and cancellations must be retained for a period of at least three years.

4.3 Investigation Officers

IO's are responsible for ensuring that all the relevant original forms are forwarded to the RIPA Co-ordinator, and for maintaining copies on the investigation file. Hard copies of RIPA forms may be held on specific investigation files. These documents should not be scanned into individual non-investigatory case records (e.g. tenancy files) as this could compromise security and data protection.

4.4 Elected Members role

Elected Members should review the authority's use of the 2000 Act and the policy on a regular basis. They should also consider internal reports on the use of RIPA and IPA on at least a quarterly basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose. They should not, however, be involved in making decisions on specific authorisations.

4.5 Monitoring & Quality

The RIPA Co-ordinator and the Corporate Head of Audit, Anti-Fraud and Risk Management will review a sample of the authorisation forms on a regular basis and where necessary provide feedback/suggestions to the IO/AO's to ensure all authorisations meet the required standard.

PART 5 - OFFICERS DESIGNATED TO GRANT AUTHORITY

There are three levels of designated authority: -

Responsible Officer	What is being authorised
Chief Executive (Head of Paid Service) In the absence of the Chief Executive this responsibility will fall to the person acting as the Head of Paid Service in relation to RIPA.	Children/Vulnerable Adults being used as a CHIS or where confidential information (including legally privileged and medical material) is likely to be obtained as a result of directed surveillance.
Level 2 authorisers (see below)	CHIS and all other authorisations
All Other Authorising Officers	All other authorisations

Covert surveillance may only be authorised in accordance with this policy. In the absence of a nominated AO the authorisation must be given at the equivalent or a more senior level. The AO need not necessarily work in the same area of business activity.

The Corporate Head of Audit, Anti-Fraud and Risk Management maintains a list of officers approved to undertake the role of an AO which is attached at Appendix 1.

NB. AOs should not authorise surveillance for an investigation in which they are directly involved.

PART 6 - COMPLAINTS

Any person who reasonably believes they have been adversely affected by surveillance activity by or on behalf of the Council may complain to the Corporate Director of Legal and Democratic Services who will investigate the complaint. Such a person may also complain to the Investigatory Powers Tribunal at:

Investigatory Powers Tribunal
PO Box 33220
London,
SW1H 9ZQ
Tel: 020 7035
3711

There is no complaint route for a judicial decision unless it was made in bad faith. Any complaints should be addressed to the Magistrates' Advisory Committee.

LIST OF KEY RIPA and IPA CONTACTs

1 October 2023

Section/Position	Responsibility(s)	Level of Authority*
Dawn Carter-McDonald Interim Chief Executive dawn.cartermcdonald@hackney.gov.uk	RIPA authorising officer	1
Jackie Moylan Interim Group Director, Finance jackie.moylan@hackney.gov.uk	RIPA authorising officer	2
Michael Sheffield Corporate Head of Audit, Anti-Fraud and Risk Management - michael.sheffield@hackney.gov.uk	RIPA authorising officer Senior Responsible Officer Approved Rank (Comms data)	2
Vinny Walsh Audit Investigation Team Manager vinny.walsh@hackney.gov.uk	RIPA authorising officer Approved Rank (Comms data)	3
Gerry McCarthy Head of Community Safety, Enforcement and Business Regulation gerry.mccarthy@hackney.gov.uk	RIPA authorising officer	3
Karen Cooper Principal Auditor (Special Investigations) karen.cooper@hackney.gov.uk	RIPA Co-ordinator	N/A

*Key to Level of Authority

1	Head of Paid Service - Children/Vulnerable Adults being used as a CHIS or where confidential information is likely to be obtained
2	Group Director/Senior Responsible Officer - CHIS
3	All Other Authorising Officers - All other authorisations

Document and version control

Document and version control	
Title of document	London Borough of Hackney Surveillance and Communications Data Policy and Procedures
Owner	Michael Sheffield
Job title of owner	Corporate Head of Audit, Anti-Fraud & Risk Management
Directorate	Finance and Corporate Resources
Approved by	tbc (Audit Committee)
Publication date	tbc
For use by	All investigations staff and management
Why issued	Corporate Policy
Review date	XXXX 2024

Version control details				
Version No.	**Author / editor**	**Version date**	**Approval date**	**Overview of changes**
V1.0	Michael Sheffield	October 2019	October 2019	
V1.1	Michael Sheffield	XXXXX 2023	XXXXX 2023	Additional guidance re. Test purchases, ANPR and non-RIPA surveillance; Inclusion of the requirement for any person seeking judicial approval to be authorised to represent the Council under the LGA 1972; Inclusion of IPA application process map and explanation of LBH roles; Additional detail re. LBH RIPA roles and responsibilities; Updated contact details.

External Quality Assessment Draft findings related to Internal Audit

PSIAS Reference	Findings	Management Actions and Comments	Timescale	Update
PSIAS 2450 **Overall Audit Opinion**	Consider the nature and quantity of deferrals when providing the overall assurance opinion.	Further discussion on this point is required before the draft EQA report is finalised. The annual audit opinion does consider the amount of audit work delivered, alongside other assurance sources including third party reviews and the arrangements that are confirmed through the Annual Governance Statement. It is also noted that reviews of key financial systems have continued as usual. The annual audit opinion in recent years has clearly set out a higher level of interruption to internal audit work than usual because of the unprecedented disruption to all service areas since March 2020. The opinion also recognised that our understanding of the control environment in previous years has been an additional factor taken into consideration when reaching a conclusion on the current control environment.	TBC	TBC
PSIAS 2010 **Planning**	The process to request and agree deferral requests for scheduled internal audit reviews has not been formalised. Departmental heads should be required to formally document the reasons for audit deferral requests and these should be presented to the Audit Committee for approval.	While deferral requests were always required to be set out in writing and include the reason for seeking a postponement there was not a formalised approach. Following receipt of the draft EQA report the Internal Audit manual has been revised to set out the steps to be followed, including a requirement that the relevant Head of Service is notified of the request. In addition, following a review of our Committee reporting arrangements that was independent of the EQA, we are finalising arrangements to revise future	31/10/2023	Completed

		quarterly Progress Reports to highlight those audit areas where the deferral request of itself raises concerns about the internal control environment.		
PSIAS 2010 Planning	Map the risks set out in the Corporate Strategic Risk Register to audits carried out in previous years and planned audits, and present the map to Audit Committee.	While the IA annual plan is always based on an assessment of the Council's risk environment, the mapping was not presented to the Audit Committee. This will be included in the annual plan report in future years, starting in April 2024.	30/04/2024	Action Agreed
PSIAS 2060 Reporting to Senior Management and the Board	Revisit KPIs presented within the annual internal audit report to Audit Committee and ensure that they accurately reflect the performance of the service. If any discrepancies are identified, re-report outcomes against these KPIs to Audit Committee.	The recommendation relates to the first KPI which requires 90% plan completion at year end, reporting has historically set out both completed work and that which is in progress against this KPI. The draft EQA report notes that the KPI was met and the issue is one of clarity for readers of the internal audit report. The plan completion KPI will be thoroughly reviewed ahead of the next scheduled approval date (April 2024) and reporting will accurately reflect performance against the indicator.	30/04/2024	Action agreed
PSIAS 1312 External Assessments	Ensure that the next EQA is scheduled to comply with PSIAS requirements (before or in 2028).	The need to meet the PSIAS timetable is understood and agreed. The exceptional circumstance of the pandemic (which delayed all EQA assessments) and the compounding effect of the cyberattack at Hackney are the only reasons that the current assessment has been delayed.	31/10/2024	Action agreed and considered complete at this time
PSIAS 2330 Documenting Information	Update the service's retention schedule to reflect council and legislative requirements.	The team procedures included reference to old government guidance about document retention which had not been updated. The same retention timescales were separately documented in the LBH Records Management Policy and Retention Schedule, and the	31/10/2023	Completed

		timescales set out there are consistent with the old guidance and they remain appropriate. The audit procedures have been updated to reference the LBH guidance instead.		
PSIAS 2110 Governance	Ensure that the review of ethics and culture is carried out within 2023/24 in line with the audit plan.	The audit is documented in the 2023/24 audit plan that was approved by the Audit Committee in April 2023, it remains part of the plan and the scope of the audit is being prepared. Although we are unsure as to why planned work has been put forward as a recommendation point we remain committed to delivering the audit review.	30/04/2024	In progress
No PSIAS reference	Consideration may be given to amending the structure of working papers to ensure that each risk is linked to multiple controls.	The EQA reviewed a sample of LBH working papers and identified that these were PSIAS compliant and resulted in as good an outcome as the proposed alternative. This recommendation was put forward for consideration and will not be adopted.	N/A	Recommendation has not been accepted
No PSIAS reference	Consider including a statement on conflicts of interest within the Terms of Reference template.	Strong controls are already in place to manage potential conflicts of interest that could arise for the IA service. The corporate process is followed to address general conflict situations and a local declaration process is also in operation to manage any other conflicts which might specifically arise in the course of auditing. The risk is well managed by IA no issues have previously arisen. This recommendation was put forward for consideration and will not be adopted because additional information in the ToR risks detracting from the key purposes of that document.	N/A	Recommendation has not been accepted
No PSIAS reference	Ask the IT Audit service provider to complete an annual Declaration of Interest or to confirm that such declarations	These declarations have been requested and supplied so that all personnel involved in LBH IA reviews have completed a consistent process.	31/10/23	Completed

	are held.			