Audit & Anti-Fraud Progress Report

1 April 2025 - 30 November 2025

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 to 15 December 2025. It covers the areas of work undertaken, progress with implementing audit recommendations, and information on current developments in the service.

1.2 Internal Audit provides an independent continuous review of key and high-risk activities across the Council. The effectiveness of the Internal Audit function must be monitored and reported 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 complemented by specialist IT skills from an external provider. Internal Audit relies on the cooperation of directorates and service-level management to enable us to undertake planned reviews.

2.2 The Internal Audit Team is fully staffed. An apprentice joined the team in September 2024 as part of the long-term arrangements to develop the service and plan for the future. We are focusing our resources on the areas that have been agreed with management and which will provide the necessary evidence to support the Corporate Head of Audit, Anti-Fraud & Risk Management's annual assurance statement.

2.3 The 2025/26 Audit Plan consisted of 53 audits (of which 11 were schools/children's centres). One audit has been postponed and one has been added since the plan was agreed.

3. INTERNAL AUDIT KEY PERFORMANCE INDICATORS

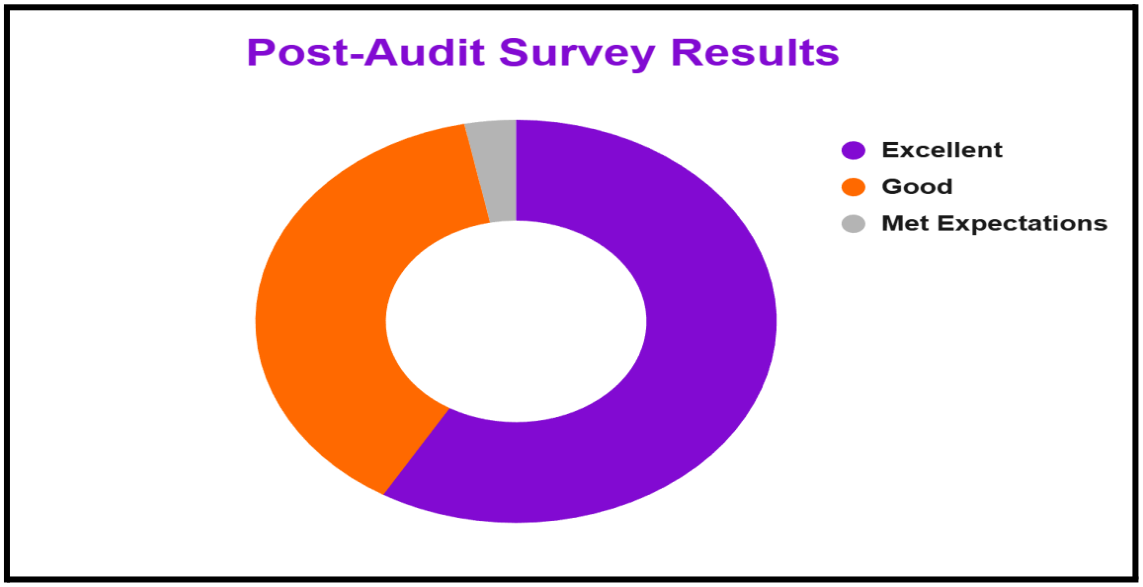
3.1 The internal audit performance for 2025/26 against key indicators is shown in Table 1 below. Post-audit survey results are summarised in paragraph 3.3.

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) 29% completed or at draft report stage. *(This compares to 41% during the same period in 2025)* 2) 9.5 days
Quality *To ensure recommendations made by the service are agreed and implemented*	1) Percentage of high and medium recommendations made that are agreed 2) Percentage of agreed high and medium-priority recommendations that are implemented	1) 100% 2) 90%	1) 100% 2) High - 68% - fully implemented and 16% partially implemented. Medium - 66% fully implemented and 13% partially implemented.
Client Satisfaction *To ensure that clients are satisfied with the service and consider it to be good quality*	● Results of Post Audit Questionnaires	1) Responses meeting or exceeding expectations	1) 100% met expectations (59% excellent, 98% good and 3% met expectations)

Table 1

3.2 As of 15 December 2025, a total of 30 internal audit reviews have been started from the 2025/26 audit plan, 11 have been completed and a further 4 are at the draft report stage. In addition, 9 reviews carried forward from the 2024/25 annual plan were reported.

3.3 Post-Audit Survey results from 1 April 2025 to 15 December 2025 continue to show that overall expectations of auditees are met, with 97% responding that expectations were exceeded, see chart below.



4. SUMMARY OF INTERNAL AUDIT WORK

4.1 Progress with 2025/26 planned audits is summarised in Table 2 below and detailed in Appendix 2.

2025/26 Audit Plan Stage of Audit Activity	**Number of assignments**	**Percentage of the revised plan**
Scoping/TOR agreed	17	32
Fieldwork in progress	15	28
Draft report issued	4	8
Completed	11	21
Total work completed and in progress	**47**	**89%**
Original Plan	53	
Additional requests	1	
Cancelled or Postponed	1	
Total Revised Plan	**53**	

Table 2

4.2 The table shows that 89% of the revised plan assignments are either work in progress, have been completed, or have been scoped/terms of reference agreed.

4.3 Table 3 outlines agreed changes to the original audit plan. These adjustments are identified as the financial year progresses, with evolving priorities, capacities and risks. However, sometimes deferral requests are concerning, as they may indicate weaknesses in the local control environment. For instance, reasons such as the absence of systems due to the cyberattack, key staff shortages, significant organisational change including the impact of the transformation agenda, or repeated deferrals could signal issues. If a deferral request highlights such

problems, the relevant review area in the table may be marked as likely to provide limited or no assurance. It's important to acknowledge that this assessment involves a higher degree of subjectivity than one resulting from an Internal Audit review.

Cancelled reviews	**Reason for Cancellation**	**Assurance concern identified?**
Postponed reviews	**Reason for Deferral**	
Organisational Development	Management Request - Engaging with Workforce to develop the People & OD Strategy	N/A
Additional reviews	**Reason for Addition**	
Queensbridge Primary School	Management Request	N/A

Table 3

4.4 Each completed audit is assigned an overall assurance grading, categorised as 'Significant', 'Reasonable', 'Limited', or 'No' assurance. The assurances resulting from audit work completed this financial year under the current and previous Internal Audit plans are shown below. The 23 final audit reports to date in 2025/26 include 12 audits from the 2024/25 audit plan. Information about the different assurance levels is provided in Appendix 3.

Assurance Level	**2025/26 YTD**	**2024/25**	**2023/24**	**2022/23**	**2021/22**
No	1	2	0	0	1
Limited	3	5	2	0	0
Reasonable	10	21	17	7	8
Significant	8	18	16	17	5
Not Applicable	1	2	0	0	0
Total	**23**	**48**	**35**	**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 15 December 2025 are shown in Table 5.

Categorisation of Risk	**Definition**	**Number 2025/26 Plan**	**Number 2024/25 Plan not previously reported**
High	Major issues that we consider need to be brought to the attention of senior management.	2	10
Medium	Important issues that should be addressed by management in their areas of responsibility.	26	31
Total		**28**	**41**

Table 5

5. SCHOOLS

5.1 The results of school audits are reported to Hackney Education (HE) within the Children's and Education Directorate. In addition, progress with the implementation of agreed recommendations from 2023/24 to the current date is 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. It also includes a review of schools earmarked for closure.

6. IMPLEMENTATION OF RECOMMENDATIONS

6.1 Progress with the implementation of agreed internal audit recommendations is tracked to ensure that the control environment is strengthened. The results of this work for the 'High' priority recommendations from audits undertaken from 2023/24 onward that were due to be implemented by 30 November 2025 are presented in Table 6.

Directorate	Implemented/ No longer relevant	Partially Implemented	Not implemented /No response	Not Yet Due	Total*
Adults, Health & Integration	2	0	0	0	2
Chief Executive's	2	1	1	0	4
Children & Education	0	0	0	1	0
Housing, Climate & Economy	1	2	1	1	4
Finance & Corporate Resources	3	0	0	0	3
ICT	4	0	0	0	4
Corporate	1	0	1	0	2
Total number	13	3	7	4	19
Percentage (%)*	68%	16%	16%	n/a	100%

* Does not include "Not Yet Due"

Table 6

6.2 The Council's target for 2025/26 is 90% of 'High' and 'Medium' priority recommendations should be implemented by the agreed timescale. Internal Audit followed up on 23 'High' priority recommendations, the implementation rate currently stands at 68% fully implemented and 16% partially implemented.

6.3 Of the 148 'Medium' priority recommendations followed up 67% were assessed as implemented and 10% partially implemented. Details are shown in Table 7. It should be noted that the outstanding recommendations listed against HCE include a significant number that concern TMO audit reviews.

Directorate	Implemented /No longer relevant	Partially Implemented	Not implemented /No Response	Not yet due	Total*
Adults, Health & Integration	7	2	1	3	10
Chief Executive's	13	4	0	2	17

Directorate	Implemented /No longer relevant	Partially Implemented	Not implemented /No Response	Not yet due	Total*
Children & Education	13	1	11	5	25
Housing, Climate & Economy**	17	5	17	4	39
Finance & Corporate Resources	33	3	1	0	37
ICT	9	4	3	15	16
Corporate	8	0	0	0	8
Total number	100	19	33	29	152
Percentage (%)	66%	13%	21%	n/a	100%

* Does not include "Not Yet Due"
**Includes 20 recommendations concerning TMOs that are either partially implemented or no response

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 the 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	8	4	0	1	12
Medium	57	9	2	16	68
Total Number	65	13	2	17	80
Percentage (%)	81%	16%	3%	n/a	100%

* Does not include "Not Yet Due"

Table 8

7. DEVELOPMENTS WITHIN INTERNAL AUDIT

7.1 The Audit & Anti-Fraud Service faced staffing and capacity issues during the year due to sickness and recruitment challenges. This has impacted the delivery of certain areas within the 2025/26 annual plan. To address these challenges, proactive measures were implemented, including the recruitment of a fixed-term contract auditor.

7.2 Progress on the planned 2025/26 ICT audits is satisfactory, following disruption in previous years. Five reports from the 2024/25 period have been issued as final or draft in 2025/26, and the current 2025/26 workplan is currently on course.

7.3 As of April 2025, all Internal Audit activities must comply with the Global Internal Audit Standards (GIAS). A recent self-assessment of our conformance with these new standards has led to the development of an Internal Audit GIAS action plan. This plan aims to ensure the successful implementation of necessary actions and full adherence to the GIAS. In addition, to ensure full conformance with new standards, Internal Auditors have updated their knowledge and skills by participating in various training courses and webinars.

Internal Audit activity must be carried out in compliance with the Standards, there is a

requirement that an independent External Quality Assessment (EQA) should take place at least every 5 years. The most recent review was completed in November 2023 and concluded that the service 'generally conforms' with the previous standards regime. This was the second highest of four possible outcomes.

8. ANTI-FRAUD SERVICE

8.1 Investigation activity continues to be impacted by backlogs that have built up in the criminal justice system and which were amplified by the pandemic. In addition, tenancy fraud work has been limited by team capacity issues during this reporting year. The situation has already improved significantly and future outcomes are expected to revert to the previous levels.

8.2 Statistical information relating to the work of the Anti-Fraud Teams is shown in 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 Audit resources continue to be allocated to support the Corporate Head of Audit, Anti-Fraud & Risk Management's annual assurance statement.

Internal Audit Annual Plan *Progress to 15 December 2025 (including 2024/25 audits completed in the current year)*					
Code	**Description**	**High Priority**	**Medium Priority**	**Audit Assurance**	**Status**
2024/25 Audits					
2425LBH01	AGS Coordination 2024/25	0	0	**Reasonable**	AGS Report
2324LBH02	Organisational Culture				WiP
2425HR01	LBH Recruitment & Retention / Workforce	3	2	**Limited**	Final Report Issued
2425AHI01	Care Provider Capacity - Fragility of the Care Provider market	0	4	**Reasonable**	Final Report Issued
2425AHI05	Collection of Care Charges	1	2	**Reasonable**	Final Report Issued
2425FCR07	Grant Monitoring	0	4	**Reasonable**	Final Report Issued
2425FCR09	Pensions - Investments	0	0	**Significant**	Final Report Issued
2425ICT02	Telephony & Network Connections	2	8	**Limited**	Final Report Issued
2425ICT04	Synergy	0	6	**Reasonable**	Final Report Issued
2425ICT05	Disaster Recovery and Backup Arrangements				Draft Report Issued
2425ICT06	Change Management			**Limited**	Final Report Issued
2425CE05	Children with Disabilities	0	0	**Significant**	Final Report Issued
2425CHE01	Housing Legal Disrepair				Draft Report
2425CHE04	Leaseholder Major Works Debt Recovery	4	2	**No Assurance**	Final Report Issued
2425SCH01	Clapton Park CC	0	3	**Significant**	Final Report Issued
2025/26 Audits					
Corporate / Cross-Cutting					
2526LBH01	AGS Coordination 2025/26				Feb 2026 start.
2526LBH02	Climate Change/Zero Tolerance				WiP
2526LBH03	Council Owned Companies				Q4 Scoping
2526LBH04	Grant Certifications				Q4 Tbc
Chief Executive's					
2526CEX01	Establishment Control				WiP

2526CEX02	Organisational Development				Management Request to defer.
2526CEX03	Grievances				Q4 Scoping
2526CEX04	Strategic Delivery Team - Disbursement of Funds				Draft ToR Issued
2526CEX05	Voluntary & Community Sector - Advisory				Q4 Tbc
Adults, Health & Integration					
Adults/Public Health					
2526AHI01	Mortuary	0	2	**Significant**	Final Report Issued
2526AHI02	Suicide Prevention				Final ToR Issued
2526AHI03	Safeguarding Provisions within Contracted Services				WiP
2526AHI04	Shared Lives				WiP
2526AHI05	MHRA National Patient Safety Alerts				Final ToR Issued
2526AHI06	Public Health - Partnership relationship between LBH & City of London				Draft Report Issued
Finance & Corporate Resources					
Financial Management					
2526FCR01	Accounts Payables				WiP
2526FCR02	Accounts Receivables				WiP
2526FCR03	Treasury Management				WiP
Revenues & Benefits					
2526FCR04	Council Tax				WiP
ICT					
2526ICT01	Records Retention				WiP
2526ICT02	3rd Party ICT Security				Final ToR Issued
2526ICT03	Business Continuity				Final ToR Issued
2526ICT04	Academy	0	4	**Reasonable**	Final Report Issued
2526ICT05	Licence Management				Final ToR Issued
2526ICT06	Device Management				Final ToR Issued
2526ICT07	Follow-up of Recommendations				Q4 Scoping

Children & Education					
Children & Families					
2526CE01	Short Breaks for Children with Disability				WiP
2526CE02	Supporting Families Programme Grant				Q4 Tbc
Education & Schools					
2526CE03	Permanent Exclusions				WiP
2526CE04	Unregistered Settings	0	5	**Reasonable**	Final Report Issued
2526CE05	Free School Meals				Q4 Final ToR Issued
2526CE06	School Thematic Audit - Corporate Services Support				WiP
2526CE07	Schools Overview Report 2024/25	0	3	n/a	Final Report Issued
Schools					
Primary Schools & Children's Centres					
2526SCH01	Ann Taylor Children's Centre				WiP
2526SCH02	Berger Primary School				Q4 Final ToR Issued
2526SCH03	Blossom Federation - Daubeney, Seabright, & Lauriston Primary Schools	0	1	**Significant**	Final Report Issued
2526SCH04	Leap Federation - Gayhurst, Kingsmead, & Mandeville Primary Schools				Q4 Final ToR Issued
2526SCH05	Oldhill Community Primary School	0	0	**Significant**	Final Report Issued
2526SCH06	Princess May Primary School				Q4 Final ToR Issued
2526SCH07	Sir Thomas Abney Primary School	0	0	**Significant**	Final Report Issued
2526SCH08	St. Dominic's Primary School	1	1	**Reasonable**	Final Report Issued
2526SCH09	St. Mary's CoE Primary School	0	1	**Significant**	Final Report Issued

2526SCH12	Queensbridge Primary School				Draft Report Issued
Secondary Schools					
2526SCH10	Our Lady's Catholic High School				Draft Report Issued
2526SCH11	Yesodey Hatorah Senior Girls School	0	9	**Reasonable**	Final Report Issued
Special Schools					
Housing, Climate & Economy					
Housing					
2526CHE01	Complaints Handling - Follow Up				Q4
2526CHE02	Lordship TMO				Q4 Final ToR Issued
2526CHE03	Wyke TMO				Q4 Final ToR Issued
2526CHE04	TMO Oversight				WiP
2526CHE05	Housing Repairs				Draft ToR Issued
2526CHE06	Temporary Accommodation Income Collection				Draft ToR Issued
Environment & Climate Change					
2526CHE07	Building Control Service	1	0	**Reasonable**	Final Report Issued
Regeneration					
2526CHE08	Private Rented Sector - Incentive Payments				WiP
2526CHE09	Hackney Living Rents				Draft Report Issued

* ToR - Terms of Reference
* WiP - Work in Progress

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 that, 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 that 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 that 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 that 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 from 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 October 2025 to 30 November 2025

1. Investigations Referred

The Anti-Fraud service has received 325 referrals during the year to date, which is broadly consistent with the level of activity in 2024/25.

Group	Department	Number of Cases Referred in Period	Number of Cases Closed in Period	Cases Currently Under Investigation	Referrals 2025/26 YTD	Referrals 2024/25
Housing, Climate & Economy (HCE)	**Housing, Climate & Economy**	3	4	16	16	10
	Tenancy Fraud	29	35	293	117	161
	Parking	17	19	51	108	181
Children's & Education	**Children's**	1	1	0	6	2
	No Recourse to Public Funds (NRPF)	22	11	32	70	122
	Hackney Education	0	0	7	0	7
Adults, Health & Integration	**Adults, Health & Integration**	2	2	9	6	6
Finance & Corporate Resources (F&CR)	**Finance & Resources**	1	1	4	1	3
	Covid business grants	0	0	1	0	0
Chief Executive's Directorate	**Chief Executive's Directorate**	1	0	5	1	3
Total		76	73	418	325	495

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.

Source	Number of Cases Referred in period	Number of Cases Closed in period	Cases Currently Under Investigation	Referrals 2025/26 YTD	Referrals 2024/25
Internal	1	1	0	4	11
Other Local Authority / Housing Association	16	14	2	65	68
HMRC	3	3	0	6	1
Police	9	9	0	36	26
Immigration	0	0	0	1	7
DWP	0	0	0	8	18
Other	18	17	1	28	46
Total	47	44	3	148	177

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 2025 (with the Council Tax matches being received on an annual basis). Matches are investigated by various LBH teams over the 2 year cycle, AAF investigates many 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 NFI2024/25	Number Matches Cleared NFI2022/23
Payroll	61	36	21	33
Housing Benefit	702	0	372	833
Housing Tenants	1,338	18	364	797
Right to Buy	23	0	4	143
Housing Waiting List	1,529	50	68	n/a
Concessionary travel / parking	929	2	478	812
Creditors	8,393	0	8230	6,784
Pensions	268	1	263	140
Council Tax (SPD)	11,639	111	9,330	
Council Tax Reduction Scheme	1,249	62	67	n/a
Procurement/Other	36	2	15	25
Total	26,167	282	19,212	10,388

Table 3

Hackney has been able to fully participate in the 2024/25 NFI matching after the two previous exercises were disrupted because some data was not available following the cyber attack in October 2020.

Responsibility for investigating Housing Benefit matches passed to the DWP in 2014.

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	2025/26 YTD	2024/25
Disciplinary action	1	3	4
Resigned as a result of the investigation	0	10	7
Referred to Police or other external body	0	0	3
Prosecution	0	10	18
Referred to Legal Services	1	12	10
Investigation Report/ Management Letter issued	0	12	13
Council service or discount cancelled	1	30	52
Covid business grants cancelled	1	1	1
Blue Badges recovered	12	66	120
Other fraudulent parking permit recovered	0	6	13
Parking misuse warnings issued	4	47	126
Penalty Charge Notice (PCN) issued	27	50	85
Vehicle removed for parking fraud	8	30	66
Recovery of tenancy	10	31	20
Housing application cancelled or downgraded	0	7	7
Right to Buy application withdrawn or cancelled	1	1	0

Table 4

The disciplinary outcome relates to conduct outside of work.

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 October to November 2025 a total of 10 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 £420,000.

In the same period 0 housing applications have been cancelled following a TFT review. These investigations help to ensure that Hackney's social housing is only allocated to those in genuine need. The Audit Commission had variously reported the potential benefit to the public purse of each cancelled application as between £4,000 and £18,000. One Right to Buy claim was disallowed following investigation, so that a housing unit was not lost from the Council stock and a discount of £16,000 was not given.

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). During this reporting period, 1 support packages were cancelled or refused following AAF investigations. This equates to a saving in the region of £387 per week, if these had been paid for the full financial year it would have cost Hackney approximately £20,179.

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 12 Blue Badges or other parking permits, which equates to £1,200, and enforcement charges of £3,355 also arose.

In addition, costs, penalties and victim surcharges related to the parking prosecution cases totalled £591.

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.

6. Matters Referred from the Whistleblowing Hotline

All Hackney staff (including 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. Two referrals were 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/Group Director FCR/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	2025/26 YTD	2024/25
Production	1	2	3
Restraint	0	0	0
Compensation	0	0	1
Confiscation	0	0	0
Total	1	2	4

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

The 2025/26 proactive counter fraud plan contains the following items:

- Temporary accommodation placements outside Borough
- NRPF long-term client review
- Various fraud awareness training
- Facilitation and delivery of the 2024/25 NFI

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

Surveillance and Communications Data

Policy and Procedures

Audit & Anti-Fraud Division
February 2026

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 -

3) Surveillance COP
4) Communications Data COP
5) 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. The RIPA Co-ordinator should be contacted in the event of staff non-RIPA surveillance activity to ensure that this is documented. 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 the gravity and extent of the perceived criminality 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): -

2) 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;
3) a copy of the original RIPA authorisation and any supporting documents setting out the case for retention by the JP;
4) 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:

5 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.
6 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).
7 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:

7.2 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.

7.3 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.

7.4 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: -

3) the validity of the risk assessment

4) the conduct of the CHIS, and

5) 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 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: -

3) details written on the outside of a postal communication
4) details relating to the sender/recipient of an email communication
5) telephone/mobile phone subscriber checks
6) 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:

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

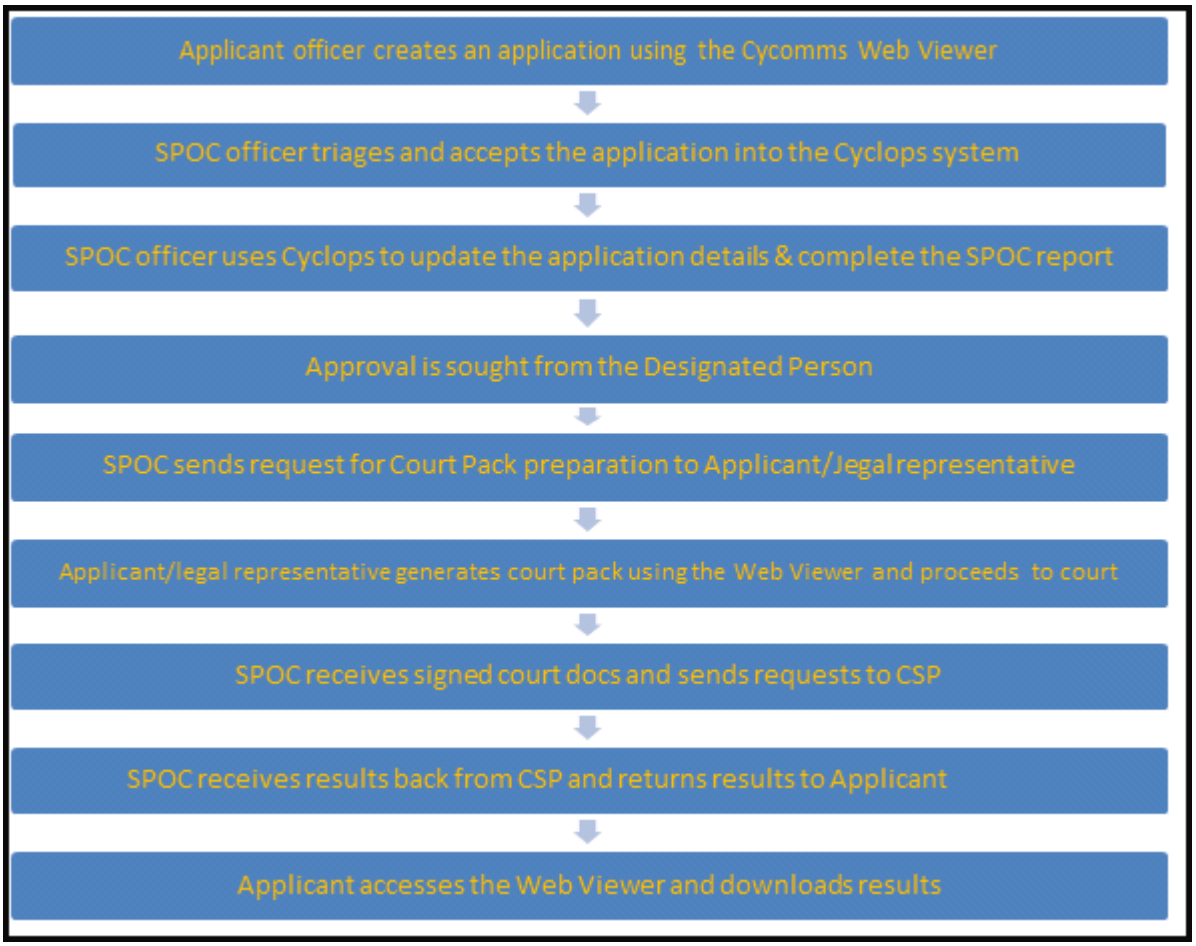
Communications data requests also need to set out why provision of the information will be proportionate to the matter being investigated, and make clear why the application is necessary in the context of the specific case.

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
Level 1 authoriser 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 February 2028

Section/Position	Responsibility(s)	Level of Authority*
Dawn Carter-McDonald Interim Chief Executive dawn.cartermcdonald@hackney.gov.uk	RIPA authorising officer	1
Naeem Ahmed Interim Group Director Finance & Corporate Resources naeem.ahmed@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	13 January 2026 (Audit Committee)
Publication date	1 February 2026
For use by	All investigations staff and management
Why issued	Corporate Policy
Review date	February 2028

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	October 2023	25 October 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.
V1.2	Michael Sheffield	February 2026	13 January 2026	Updated contact details