Document Number: 22302534

Document Name: Appendix 1 Draft RIPA Policy 2019

Surveillance and Communications Data

Policy and Procedures

Hackney

Audit & Anti-Fraud Division
October 2019

INDEX

INTRODUCTION

The purpose 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; and
- provide guidance on the authorisation procedures to be followed.

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 follow this policy when involved in any of the above activities. Links to the following Home Office Codes of Practice are available on the intranet:-

- Surveillance COP
- Communications Data COP
- Covert Human Intelligence
- Source COP

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

Audit & Anti-Fraud regularly coordinate training for officers who may need to use or approve surveillance powers.

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. The URN must be written on the form.

If an IO considers it necessary to undertake surveillance as part of an investigation, s/he 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: -

- preventing or detecting crime

NB. It must be necessary in that particular case

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 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 detail 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 82711203 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 a directed surveillance operation is to include the use of CCTV equipment then the IO must complete Form 5429 which is available on the intranet. This document is the unified protocol in which RIPA authorised use of CCTV for Directed Surveillance activity will be passed to Hackney CCTV & Emergency Planning Service. It must be delivered to the CCTV Service Deputy Manager/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, please contact 020 8356 2333, in advance. In the event of an urgent authorisation utilising CCTV Service cameras verbal arrangements may be agreed which must be followed up with the form.

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

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. 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.

NB. If covert technical equipment is worn by the test purchaser, or an adult is observing the test purchase, authorisation for directed surveillance is required.

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 (one month if the CHIS is under 18). They may be renewed prior to the end of the 12 month period. 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. Applications must be made through the team leaders of the Legal Team.

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.

INVESTIGATORY POWERS ACT 2016

PART 3 – COMMUNICATIONS DATA

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 channeled through the National Anti-Fraud Network (NAFN), an organisation that Hackney subscribes to. A link to NAFN's process can be found on the intranet

If an IO considers it necessary to obtain communications data as part of an investigation, they must complete an application for requiring communications data to be obtained and disclosed. All applicants will need to register with NAFN at nafn.gov.uk prior to making an application on the on line system.

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

All requests for communications data must be recorded on the Hackney's spreadsheet, this is administered by the RIPA co-ordinator and requests for access should be emailed.

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

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 Elected Members role

Elected Members should review the authority's use of the 2000 Act and the policy at least once a year. 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.

4.3 Record Keeping

Hackney must maintain a central record of all RIPA authorisations, reviews, renewals and cancellations, which shall be made available to the OSC and the IOCCO.

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. 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.

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.

4.4 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.

4.5 Identifying Authorities

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 – directed surveillance only. An authorisation will be identified in the following manner: -

Dept / Div / Investigation case no / URN (see examples below) FIN/AAF/xxxxx/01
HH/ILLOCC/xxx
xx/xx
NNR/TS/xxx
xx/xx

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	Renewals	Cancellations
Insert 'RV' before the authorisation number (e.g. HSB/ASB/0011/RV0225)	Insert 'RN' before the authorisation number (e.g. HH/ILLOC/xxxxx/RN01)	Insert 'C' before the authorisation number (e.g. NNR/TS/xxxxx/C07)

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 (see below) (authorisers (see Below)	CHIS and all other authorisations
All Other Authorising Officers	All other authorisations

Covert surveillance may only be authorised by officers of 3rd Tier Level or above. 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 be responsible for authorising 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.

Senior Responsible Officer:

Michael Sheffield, Corporate Head of Audit, Anti-Fraud and Risk Management,
Finance & Corporate Resources Directorate

LIST OF KEY RIPA OFFICERS

1 August 2019

Section/Position	Authorising Officers	Level of Authority*
Chief Executive	Tim Shields	1
Group Director Finance & Corporate Resources	Ian Williams	2
Corporate Head of Audit, Anti-Fraud and Risk Management	Michael Sheffield	2
Audit Investigation Team Manager	Vinny Walsh	3
Head of Community Safety, Enforcement and Business Regulation	Gerry McCarthy	3
RIPA Co-ordinator	Karen Cooper	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/Director - CHIS
3	All Other Authorising Officers - All other authorisations