# REGULATION OF INVESTIGATORY POWERS ACT 2000

# HARINGEY POLICY

| Policy History | | | | | |
|---|---|---|---|---|---|
| **Version** | **Summary of Change** | **Contact** | **Implementation Date** | **Review Date** | **EqIA Date** |
| 10.00 | • Inclusion of use of social media guidance<br>• Updated Authorised Officer list | Head of Audit & Risk Management | September 2014 | July 2014 | June 2014 |

| Links and Dependencies |
|---|
| RIPA – Procedure/Guidance Notes |
| Corporate Anti-fraud Policy and Fraud Response Plan |
| Whistleblowing Policy |
| Sanctions Policy |
| Anti-money Laundering Policy |
| Anti-bribery Policy |
| Employee Code of Conduct |

| Related Forms |
|---|
| RIPA Authorisation for Directed Surveillance |
| RIIPA Review of Directed Surveillance Authorisation |
| RIPA Renewal of Directed Surveillance Authorisation |
| RIPA Cancellation of Directed Surveillance Authorisation |
| RIPA Application for Communications Data |

OFFICIAL

## 1. Policy Statement

1.1 Haringey Council will apply the principles of the Regulation of Investigatory Powers Act 2000 (RIPA) to all activities where covert surveillance, covert human intelligence sources, or communications data are used. In doing so, the Council will also take into account its duties under other legislation, in particular the Human Rights Act 1998 and Data Protection Act 1998, and its common law obligations.

## 2. Overview and Purpose of RIPA

2.1 RIPA came into force in England and Wales on 25 September 2000, and aims to balance, in accordance with the European Convention of Human Rights, the rights of individuals with the need for law enforcement and security agencies to have powers to perform their roles effectively. The Human Rights Act 1998 requires that all actions which may potentially breach an individual's human rights are proportionate; necessary; non-discriminatory; and lawful. RIPA allows local authorities to collect evidence of criminal activity lawfully where the investigation requires covert surveillance, even where that may lead to them obtaining private information about individuals.

2.2 RIPA provides a statutory basis for local authorities to authorise the use of directed surveillance and covert human intelligence sources (undercover officers, agents, informants); and access communications data (postal, telecoms and internet operators' data). Three Home Office Codes of Practice: Code of practice for covert surveillance and property interference; Code of practice for the use of human intelligence sources and Code of practice for the acquisition and disclosure of communications data provide further detailed guidance.

2.3 From 1 November 2012, sections 37 and 38 of the Protection of Freedoms Act 2012 apply. Any local authority who wishes to authorise the use of directed surveillance, acquire communications data, and/or use a covert human intelligence source (CHIS) under RIPA will need to obtain an order approving the grant (or renewal) of an authorisation or notice from a Justice of the Peace (JP) before it can take effect. This is in addition to the existing internal authorisation processes under the relevant parts of RIPA.

2.4 RIPA requires a Senior Responsible Officer (SRO) to be appointed to be responsible for ensuring the Council's compliance with RIPA and its Codes; and to oversee the implementation of any post-inspection action plans recommended or approved by a Commissioner. The Assistant Director of Corporate Governance is Haringey's SRO.

2.5 Failure to comply with RIPA does not mean that an authority's actions in relation to surveillance will be unlawful; however it does mean that evidence obtained from surveillance could be inadmissible in court proceedings and jeopardise a successful outcome. Such action could also be open to challenge as a breach of the Human Rights Act and a successful claim for damages could be made against the Council.

2.6 Further information on RIPA can be obtained from the Office of Surveillance Commissioners, the body responsible for overseeing the use of covert surveillance, including the relevant RIPA Codes of Practice, together with examples of frequently asked questions for local authorities.

2.7 The Council's RIPA Procedure Notes provide guidance to investigating and authorising officers when undertaking RIPA activities. Copies of all relevant application, review, renewal and cancellation forms, together with the application for judicial review form are held on the Council's Intranet. The Head of Audit and Risk Management should be contacted in the first instance if access to Communications Data is required, or use of a CHIS is being considered.

## 3. Restrictions on the use of RIPA.

3.1 The Protection of Freedoms Act 2012 restricts the use of RIPA to conduct that would constitute a criminal offence which punishable by a maximum custodial sentence of six months or more. Low-level offences such as littering, dog fouling and school admissions should not be undertaken using RIPA.

3.2 There are some limited exceptions to the rule on criminal threshold levels, relating to specified criminal offences for the underage sale of alcohol (s146, s147 and s147A of the Licensing Act 2003) and tobacco (s7 of the Children and Young Persons Act 1933). The relevant RIPA tests of necessity and proportionality must still be applied and prior JP approval obtained before any surveillance takes place.

3.3 The purpose of this policy is to ensure that:

- the proper procedures are in place in order to carry out covert surveillance;
- an individual's right to privacy is not breached;
- the investigation is necessary and proportionate to the alleged offence;
- proper authorisation is obtained for covert surveillance;
- the proper procedures have been followed; and
- covert surveillance is considered as a last resort having exhausted all other avenues.

## 4. Authorisation and Duration of RIPA Activities

4.1 Each covert surveillance operation involving directed surveillance, covert human intelligence sources and the acquisition of communications data must be authorised internally within the council in writing first. All applications must use the forms provided on the Council's intranet and, following internal approval, all applications must also be externally authorised by a JP. Annex A provides a summary flow chart of the RIPA process. **No investigation can commence until both internal and external authorisations have been given.**

4.2 The application form will only be considered by a JP if it is authorised by a relevant authorising officer. Authorising officers are those listed at Annex B to this policy. Authorising officers can only authorise the use of RIPA if they have completed the SRO approved training. Guidance on completing the application and authorisation process is included in the Council's RIPA Procedure Notes and further advice can be obtained from the Head of Audit and Risk Management.

4.3 For any urgent applications, the Head of Audit and Risk Management and Legal Services should be contacted at the earliest opportunity in order to make urgent arrangements to see a JP. The application form and internal authorisation will still be needed but the time in which to get judicial approval may be reduced.

4.4 Authorisations only remain valid for specific periods and may require renewal or cancellation. Written authorisations can only last for a maximum period of 3 months and will expire after 3 months. Authorisations must be cancelled if the conditions are no longer met. Authorisations do not expire when the conditions are no longer met and therefore cancellations should be made at the earliest opportunity.

4.5 Authorisations should be kept under regular review, especially if the risk of obtaining private information or of collateral intrusion is high, and in accordance with the circumstances of the case. Internal reviews should be recorded on the relevant forms, but do not need approval by a JP.

4.6 Authorisations can be renewed, but these will be subject to the same internal and external authorisation processes to determine whether the grounds for authorisation still exist. A renewal can be granted for a further 3 months from the date of expiry of the original application. Any renewal application must take place prior to the expiry of the original application. If this timeframe cannot be met, no further surveillance should be carried out until a further application has been authorised.

4.7 If the conditions for surveillance being carried out are no longer satisfied, and the authorisation period has not ended, a cancellation form must be completed and all those involved in the surveillance should receive notification of the cancellation, which must be confirmed in writing at the earliest opportunity. Cancellations do not need approval from a JP.

## 5. Covert Human Intelligence Sources (CHIS)

5.1 If a CHIS is to be used, there are detailed requirements regarding management of their activities which are set out in the Home Office code of Practice. The use of a CHIS who is an adult and not a vulnerable person can authorised by any of the authorising officers. In a case where the proposed CHIS is a juvenile or a vulnerable person, only the Chief Executive can grant an authorisation.

5.2 Before making any decisions about using a CHIS, the Assistant Director of Corporate Governance and Head of Audit and Risk Management must be consulted. There are statutory risk assessment requirements specified in section 29 of the Act which are designed for the safety of the individual acting as a CHIS and the protection of the Human Rights of those who may be directly or indirectly involved in the operation. Guidance on the use of a CHIS is contained in the Council’s RIPA Procedure Notes, including the records which must be kept when using a CHIS.

## 6. Social Networking Sites and Internet Sites

6.1 Social networking and internet sites are easily accessible, but if they are going to be used during the course of an investigation, the investigator must consider whether RIPA authorisation should be obtained.

6.2 In most cases, the Council will not seek to covertly breach a site's access controls, but if this is deemed necessary and proportionate, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by the officer (i.e. the activity is more than simply reading the site's content). This could occur if an officer covertly asks to become a 'friend' or 'network contact' of someone on a social networking site.

**7. Requests to undertake Covert Surveillance using CCTV**

7.1 The Council's CCTV Control Room staff may be requested to undertake covert surveillance on behalf of other enforcement authorities, including the police. The Council supports working with external enforcement agencies and organisations to prevent and detect crime; but any requests must be supported by an appropriate RIPA authorisation from the relevant enforcement authority and be provided to the CCTV Manager before the covert surveillance is commenced.

7.2 Surveillance that is unforeseen and undertaken as an immediate response to a situation falls outside the definition of directed surveillance and therefore authorisation is not required.

**8. Records and Inspections**

8.1 RIPA requires the Council to maintain records, including details of all applications, reviews, renewals and cancellations. The Head of Audit and Risk Management maintains the Central Record on behalf of the SRO, and retains hard and electronic copies of all forms and JP approval records.

8.2 The documents in the Central Record are retained in accordance with Audit and Risk Management's records management policy which complies with relevant Data Protection legislation. The original documents should be retained by the service area responsible for the surveillance activity.

8.2 The Office of the Surveillance Commissioner has set up an Inspectorate to monitor compliance with RIPA. Haringey's SRO and Head of Audit and Risk Management will act as the first point of contact for the Inspectors, but all service areas that use RIPA should expect to be involved in any inspection visits.

**9. Monitoring and Reporting**

9.1 The Assistant Director of Corporate Governance is responsible for the maintenance and operation of this policy, as the Council's nominated SRO under RIPA. The Assistant Director of Corporate Governance will liaise with the Head of Audit and Risk Management to review the policy on a regular basis.

9.2 Regular reports will be made to Members in accordance with the requirements of the RIPA Codes of Practice.

# ANNEX A

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE

Local authority investigator wants to use a RIPA technique (directed surveillance, CHIS (covert human intelligence source) or communications data).

Does investigator intend to use directed surveillance?

Yes

No

Is the local authority investigating an offence and does that offence attract a maximum custodial sentence of 6 month or more?

No

Yes

Is the offence being investigated either:
-Section 146/147/147A of the Licensing Act 2003, or
-Section 7 of the Children and Young Persons Act 1993.

No

Yes

• Complete RIPA authorisation/notice form, and seek approval of authorising officer/designated person as per current arrangements.
• Complete application part of the judicial application/order form for JP.

**Within Office Hours**
Local authority investigator to contact Her Majesty's Courts & Tribunals Service (HMCTS) administration at the magistrates' court to arrange a hearing.

Attend court with:
• counter-signed RIPA authorisation/or notice (for CD authorisations/notices the signatures may be electronic signatures).
• the accompanying judicial application/order form.
• any other relevant reference or supporting material.

**Outside usual office hours:**

A JP may consider an authorisation out of hours in **exceptional** circumstances. If the authorisation is urgent and cannot be handled the next working day then you should:
• Phone the court's out of hours HMCTS legal staff contact. You will be asked about the basic facts and urgency of the authorisation. If the police are involved in the investigation you will need to address why they cannot make a RIPA authorisation.
• If urgency is agreed, then arrangements will be made for a suitable JP to consider the application. You will be told where to attend and give evidence.
• Attend hearing as directed with two copies of both the counter-signed RIPA authorisation form or notice and the accompanying judicial application/order form.

Outcome

Investigator may **not** use directed surveillance. The case should be investigated by other means. Continue to assess if threshold is met **if** further offences come to light as the case progresses.

Refuse to approve the grant or renewal and quash the authorisation or notice.

Refuse to approve the grant or renewal of an authorisation or notice.

Approve the grant or renewal of an authorisation or notice.

This may be appropriate if the JP considers that an application is fundamentally flawed. The local authority must be given at least 2 business days in which to make representations before the authorisation is quashed. In these circumstances a local authority cannot use the technique and will need to seek fresh authorisation internally before reapplying.

The grant or renewal of the RIPA authorisation or notice will not take effect and the local authority may **not** use the covert technique. Local authority may wish to address, for example, a technical error and reapply.

Technique may be used in this case. Investigator to resubmit to the JP any renewal or authorisation for the use of a different technique in this case.

Obtain signed order and retain original RIPA authorisation/notice.
For CD authorisations or notices, local authority investigator to provide additional copy of judicial order to the SPoC.
If out of hours, a copy of the signed order to be provided to the court the next working day.

17

Annex B

**Haringey Council - Authorising Officers for RIPA**

| Job Title | Officer's Name | Contact number |
|---|---|---|
| Chief Executive (confidential information and juvenile or vulnerable adult CHIS only) | Nick Walkley | 0208 489 2648 |
| Assistant Director for Finance | Kevin Bartle | 0208 489 5972 |
| Director of Regeneration, Planning and Development | Lyn Garner | 0208 489 4523 |
| Assistant Director for Environmental Services and Community Safety | Stephen McDonnell | 0208 489 2485 |
| Interim Head of Community Service | Hazel Simmonds | 0208 489 5458 |
| Director of Children's Service | Lisa Redfern | 0208 489 3206 |
| Director of Adult Social Services | Beverley Tarka | 0208 489 5919 |
| Director of Public Health | Jeanelle de Gruchy | 0208 489 2828 |