

REGULATION OF
INVESTIGATORY
POWERS ACT 2000
HARINGEY POLICY

Policy History					
Version	Summary of Change	Contact	Implementation Date	Review Date	EqIA Date
10.1	<ul style="list-style-type: none"> Updated use of open source material guidance Updated Authorised Officer list 	Head of Audit & Risk Management	November 2015	October 2016	June 2014
10.2	<ul style="list-style-type: none"> Updated Authorised Officer list Updated guidance on social media 	Head of Audit & Risk Management	March 2017	March 2018	June 2014
10.3	<ul style="list-style-type: none"> Updated Authorised Officer list Updated reference para 8.2. 	Head of Audit & Risk Management	August 2018	August 2019	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

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 Protection of Freedoms Act 2012; 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). The Home Office [RIPA Codes of Practice](#) provide further detailed guidance.
- 2.3 The Protection of Freedoms Act 2012 (sections 37 and 38) applies to RIPA applications. 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 [Investigatory Powers Commissioner's Office](#), 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 Business Manager for Corporate Governance should be contacted in the first instance if covert surveillance, access to Communications Data, or use of a Covert Human Intelligence Source (CHIS) is being considered.

3. Restrictions on the use of RIPA

3.1 From 1 November 2012 local authority use of RIPA has been restricted to conduct that would constitute a criminal offence which is punishable by a maximum custodial sentence of six months or longer. Low-level offences such as littering, dog fouling and school admissions may 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 Justice of the Peace (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 Business Manager for Corporate Governance.

4.3 For any urgent applications, the Business Manager for Corporate Governance 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 any additional 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 be authorised by any of the authorising officers listed in Annex B. 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 Business Manager for Corporate Governance 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 and establishes a relationship or engages the individual in communication in order to obtain information. An investigator should not attempt to set up an account which adopts the identity of a person likely to be known to the subject of the investigation without authorisation and the explicit consent of the person whose identity is being used.
- 6.3 It is the responsibility of the individual to set privacy settings to protect unsolicited access of private information. Where privacy settings are available, but not applied, the data may be considered 'open source' and a RIPA authorisation is not usually required. However, repeated viewing of open source sites may constitute directed surveillance and whether authorisation is required should be considered on a case by case basis. Officers should also take account of the guidance issued by the Investigator Powers Commissioner's Office (IPCO) in this respect.

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 Business Manager for Corporate Governance 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 Legal Service'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.

8.3 The Investigatory Powers Commissioner's Office (IPCO) monitors compliance with RIPA. Haringey's SRO and Business Manager for Corporate Governance 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.

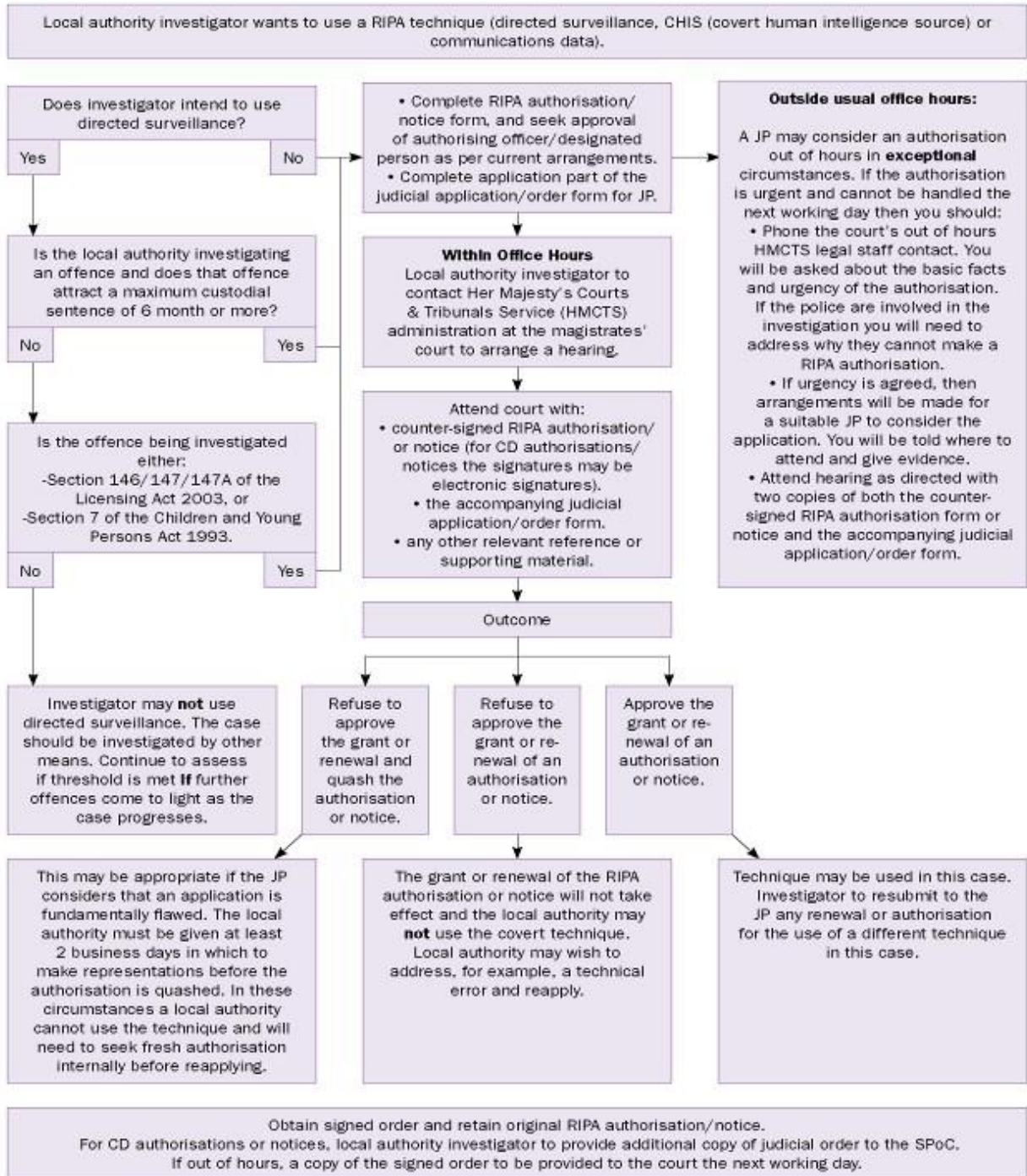
9. Monitoring and Reporting

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 Business Manager for Corporate Governance 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



Annex B

Haringey Council - Authorising Officers for RIPA

Job Title
Chief Executive (confidential information and juvenile or vulnerable adult CHIS can only be authorised by the Chief Executive)
Director of Finance
Director of Environment and Neighbourhoods
Head of Community Safety and Regulatory Services