REGULATION OF INVESTIGATORY POWERS ACT 2000:

COVERT SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES

HARINGEY POLICY

www.haringey.gov.uk

Policy History					
Version	Summary of Change	Contact	Implementation Date	Review Date	EqIA Date
10.1	• Updated use of open source material guidance • Updated Authorised Officer list	Head of Audit & Risk Management	November 2015	October 2016	June 2014
10.2	• Updated Authorised Officer list • Updated guidance on social media	Head of Audit & Risk Management	March 2017	March 2018	June 2014
10.3	• Updated Authorised Officer list Updated reference para 8.2.	Head of Audit & Risk Management	August 2018	August 2019	June 2014
10.4	• Updated to account for changes made by the Investigatory Powers Act 2016 coming into force: communications data dealt with separately	Business Manager for Corporate Governance	November 2019	November 2020	October 2019

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

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 or covert human intelligence sources 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 2018, and its common law obligations.

1.2 The purpose of this policy is to ensure that:

- an individual's right to privacy is not unlawfully breached;
- the investigation is necessary and proportionate to the alleged offence;
- proper authorisations are obtained for the use of covert surveillance and covert human intelligence sources;
- the proper procedures are followed; and
- is the use of covert surveillance and covert human intelligence sources are considered as a last resort having exhausted all other avenues.

1.3 The procedure for communications data has now changed and is dealt with under the Investigatory Powers Act 2016 and in a separate policy.

2. Overview and purpose of investigatory powers

2.1 RIPA came into force in 2000. It aims to balance the rights of individuals with the need for law enforcement and security agencies to have powers to perform their roles effectively. Any interference with an individual's human rights must be proportionate, necessary and non discriminatory, in order to comply with the European Convention on Human Rights.

2.2 RIPA allows local authorities to collect evidence of criminal activity lawfully where the investigation requires covert surveillance or covert human intelligence sources (CHIS, e.g. informants). The Home Office RIPA Codes of Practice provide further detailed guidance.

2.3 Any local authority who wishes to authorise such investigations must: (1) obtain internal authorisation from the relevant officer, and then (2) obtain approval from a Magistrates' Court before that it can take effect.

2.4 The Covert Surveillance and CHIS Codes of Practice from August 2018 require a Senior Responsible Officer (SRO) to be appointed. The Assistant Director of Corporate Governance is Haringey's SRO. The SRO is responsible for:

- the integrity of the processes in place within the public authority;
- compliance with the relevant legislation and codes of practice;

- oversight of reporting of errors to the Investigatory Powers Commissioner, and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the Investigatory Powers Commissioner and inspectors who support the Commissioner when they conduct their inspections;
- where necessary, oversight of the implementation of post-inspection action plans;
- ensuring that all authorising officers are of an appropriate standard, addressing any recommendations and concerns in the inspection reports.

2.5 Failure to comply with RIPA may mean that the Council's actions are unlawful and/or that the evidence obtained would be inadmissible in court proceedings and jeopardise the outcome of such proceedings. Such action could also lead to a successful claim for damages 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 investigatory powers, and the RIPA Codes of Practice (as updated from time to time).

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 approval form are held on the Council's Intranet. The Business Manager for Corporate Governance should be contacted in the first instance if covert surveillance or use of a covert human intelligence source (CHIS) is being considered.

3. Restrictions on the use of RIPA

3.1 Under RIPA, in certain circumstances the Council has power to use:

i covert surveillance (Part II of RIPA); and
ii covert human intelligence sources (Part II of RIPA).

Covert surveillance

3.2 Local authority use of covert surveillance is restricted to:

- Preventing or detecting criminal offences punishable by a maximum term of at least 6 months imprisonment;
- Preventing disorder involving a criminal offence punishable by a maximum term of at least 6 months imprisonment; or
- Preventing or detecting criminal offences related to the underage sale of alcohol, tobacco or nicotine inhaling products.

Covert Human Intelligence Sources (CHIS)

3.3 Local authority use of CHIS under RIPA is restricted to:

- Preventing or detecting crime; or
- Preventing disorder.

3.4 The relevant RIPA tests of necessity and proportionality must still be applied and prior JP approval obtained before any surveillance takes place.

4. Authorisation and duration of RIPA activities

Authorisation

4.1 Each investigation involving covert surveillance or covert human intelligence sources must first be authorised internally within the council in writing. 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 taken to get judicial approval may be reduced.

Duration

4.4 Authorisations only remain valid for specific periods and may require renewal or cancellation. The relevant authorisation durations are:

- Covert surveillance: 3 months
- CHIS: 12 months
- Juvenile CHIS: 4 months

Review

4.5 Authorisations should be reviewed periodically. The CHIS Code of Practice (August 2018) states that a juvenile CHIS should be reviewed at least once per month. 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.

Cancellation

4.6 Authorisations must be cancelled if the conditions are no longer met. Authorisations do not automatically expire when the conditions are no longer met and therefore cancellations should be made at the earliest opportunity. 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.

Renewal

4.7 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 the same period as the original authorisation and will take effect from the date of expiry of the original authorisation. Any renewal application must take place prior to the expiry of the original authorisation. If this timeframe cannot be met, no further surveillance can be carried out until a further application has been authorised.

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 Head of Paid Service (i.e. at Haringey, 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 covert 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 Investigatory 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 such that it would not be reasonably practicable to obtain an authorisation under RIPA 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 services' 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

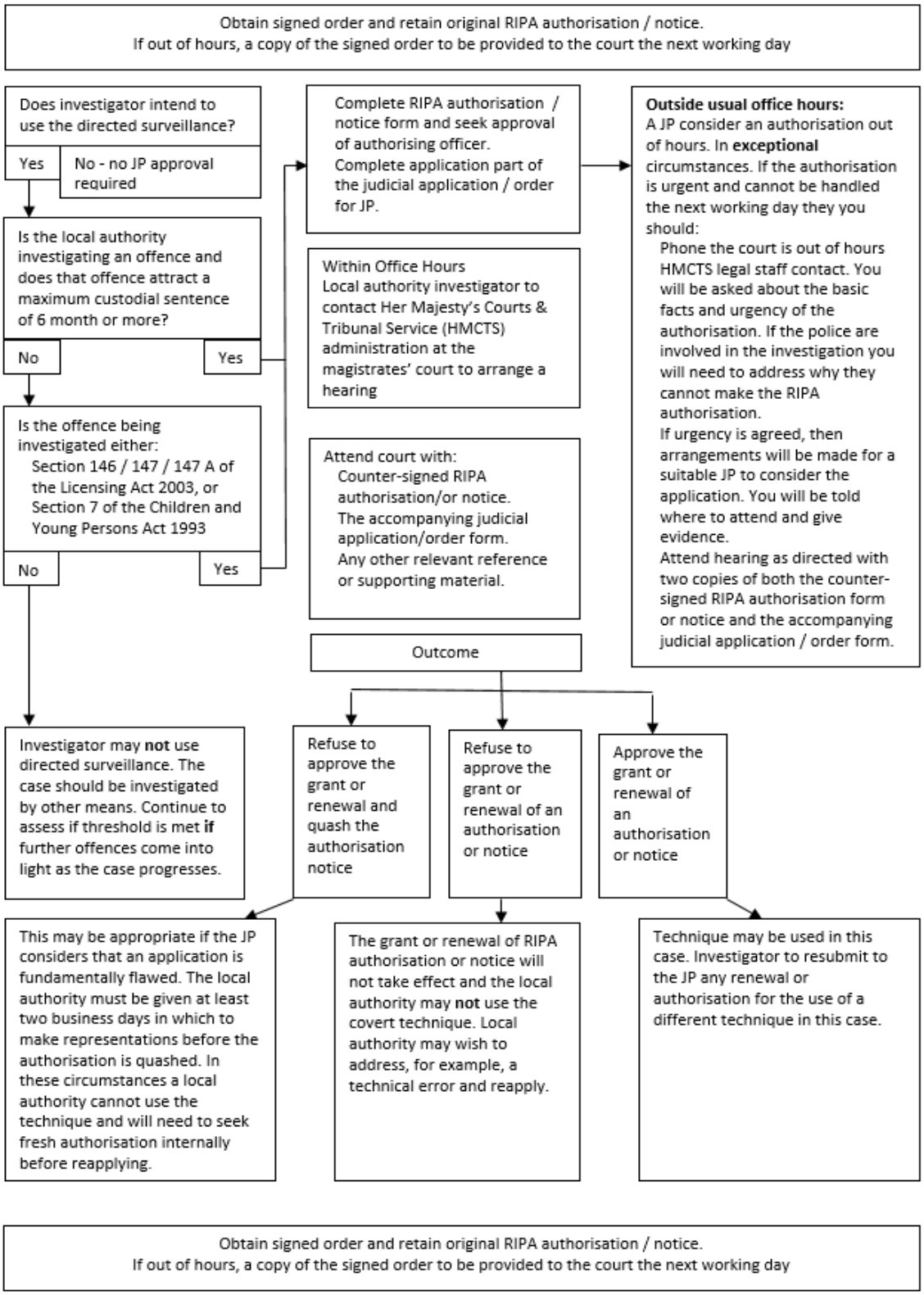
9.1 The Assistant Director of Corporate Governance is responsible for the maintenance and operation of this policy, as the Council's nominated SRO under RIPA. The Assistant Director of Corporate Governance will liaise with the Business Manager for Corporate Governance to review the policy on a regular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

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



Annex B

Haringey Council - Authorising Officers for RIPA

Job Title
Chief Executive (applications relating to confidential information and juvenile or vulnerable adult CHIS can only be authorised by the Chief Executive)
Director of Finance
Director of Environment and Neighbourhoods
Assistant Director for Stronger Communities