

APPENDIX 2

(13th September 2023)

LONDON BOROUGH OF TOWER

HAMLETS

POLICY ON THE USE OF COVERT

HUMAN INTELLIGENCE SOURCES

REGULATION OF INVESTIGATORY

POWERS ACT 2000

CONTENTS

1. Introduction	2
2. Definition of CHIS.....	6
3. Responsibilities	10
4. Authorisations	13
5. Combined Authorisations	18
6. Reviews and Renewals	189
7. Cancellations	21
8. Controller/Handler.....	22
9. Security of Covert Technical Equipment	25
10. Central Recording	26
11 Training	27
11. Member Oversight.....	28

1. Introduction

- 1.1 The Regulation of Investigatory Powers Act 2000 (“RIPA”) came into force on 26 July 2000 and provides a statutory framework for public authorities to use covert investigatory techniques, such as surveillance and covert human intelligence sources (CHIS), where necessary and proportionate, for the purpose of preventing or detecting crime and disorder. If such activities are conducted by council officers, then RIPA regulates the use of these powers in a manner that is compatible with the Human Rights Act 1998. RIPA sets out the circumstances in which the use of directed surveillance and CHIS may be authorised. Local authorities ability to use these investigation methods are restricted in nature and may only be used for the prevention and detection of crime or the prevention of disorder. In addition to defining the circumstances when these investigation methods may be used, RIPA also directs how applications should be made, and by whom. It also makes provision for the approval, review, renewal, cancellation and retention of records.
- 1.2 Part II of RIPA provides for the authorisation of the use and or conduct of CHISs.

1.3 The Council has broad statutory functions and takes targeted enforcement action in relation to those functions having regard to the following:

- The Tower Hamlets Plan, adopted under section 4 of the Local Government Act 2000
- The Tower Hamlets Strategic Plan
- The Tower Hamlets Local Plan
- Any external targets or requirements imposed under relevant legislation.
- The Council's Enforcement Policy

This policy must be read in conjunction with the current Home Office Guidance and relevant Codes of Conduct.

1.4 The Council understands that it is obliged to comply with the provisions of RIPA in order to use CHISs. The Council believes that by complying with the provisions of RIPA, the Council will also ensure that any use of CHIS comes within the qualification provided in Article 8(2) of the European Convention on Human Rights (ECHR) and, accordingly the Council should not breach its obligations under section 8(1) of the Human Rights Act 1998.

1.5 Whilst RIPA itself does not provide any specific sanction where an activity occurs, which should otherwise have been authorised, any evidence thereby obtained may be inadmissible in court, the activity may also be unlawful under the Human Rights Act 1998, and may result in an

investigation by the Ombudsman or the Investigatory Powers Tribunal.

1.6 The use of a CHIS involves any action on behalf of a public authority to induce, ask or assist a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of a CHIS. In general, therefore, an authorisation for use of a CHIS will be necessary to authorise the steps taken by the Council in relation to a CHIS, and the conduct of the CHIS. It is necessary to ensure that the CHIS is clear on what is and is not authorised at any given time and that all the CHIS's activities are properly risk assessed.

1.7 RIPA provides that responsibility for authorising directed surveillance, and use of a CHIS lies with a Director, Head of Service, Service Manager or equivalent. The Protection of Freedoms Act 2012 amended RIPA so that local authorities must obtain an order from a judicial authority approving an authorisation before it can take effect. This requirement has been in force since 1st November 2012. Parliament introduced this requirement to put a statutory check on local authorities and to ensure that powers are only used to detect and prevent serious crime.

1.8 The Investigatory Powers Commissioner's Office (IPCO) has recommended as best practice that public authorities develop a corporate policy. The Council has had such a policy in effect since 27 July 2004. This document is the

Council's corporate policy in relation to CHISs. The Council also has a policy in place in respect of the use of directed surveillance, which is contained in a separate document.

1.9 The council has prepared guidance notes and a procedure manual on the use of CHISs, which should be read with this policy.

1.10 The IPCO is responsible for reviewing the activities under RIPA 2000. All Councils are subject to review and inspection.

2. Definition of Covert Human Intelligence Sources (CHIS)

- 2.1 A person is a CHIS if he/she establishes or maintains a personal or other relationship with a person for the covert purpose of obtaining information or to provide access to any information to another person, or to disclose information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.
- 2.2 Not all human sources of information will fall within this definition, and so an authorisation under RIPA will not always be appropriate. A person who reports suspicions of an offence is not a CHIS. It is only if they establish or maintain a personal relationship with another person, for the purpose of covertly obtaining or disclosing information that they become a CHIS. By way of example, people who complain about anti-social behaviour, and are asked to keep a diary will not normally be a CHIS as they are not required to establish or maintain a relationship for a covert purpose. A test purchase, where a single transaction takes place and where there is no interaction between buyer and seller beyond the transaction itself is unlikely to constitute the use of a CHIS.
- 2.3 A relationship is established or maintained for a covert purpose, if and only if, it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

- 2.4 A relationship is used covertly and information obtained is disclosed covertly, if and only if, the relationship is used or the information is disclosed in a manner calculated to ensure that one of the parties to the relationship is unaware of the use and disclosure.
- 2.5 “Establishes” in a relationship means “set up”. Therefore it does not require, as “maintain” does, endurance over a particular period of time. Whether or not a relationship exists depends on all the circumstances, including the length of time of the contact between two people and the nature of the covert activity.
- 2.6 In some cases, members of the public may volunteer or provide information that is within their personal knowledge, without being asked or tasked to do so by a local authority. In such a case a relationship will not have been established or maintained for a covert purpose, and as a consequence the source will not be a CHIS for the purposes of RIPA, and no authorisation under RIPA will be required.
- 2.7 In some circumstances the local authority may task a person to obtain information covertly and this may result in authorisation under Part II of RIPA. However this will not be true in all circumstances, for example, where the tasks given to a person do not require that person to establish or maintain a relationship for the covert purpose of obtaining, providing access to, or disclosing the information sought, or

where the information is already within the personal knowledge of the individual. In those circumstances the person will not be a CHIS.

2.8 An individual who because of their work or role has access to personal information may voluntarily provide information to the council on a repeated basis and will need to be managed appropriately. The Council must keep such human sources under constant review to ensure that they are managed with an appropriate level of sensitivity and confidentiality and to establish whether at any given stage, they should be authorised as a CHIS. Determining the status of an individual is a matter of judgment by the Council.

2.9 The times when the Council will use a CHIS are limited.

2.10 If there is a need to use a CHIS who is a juvenile, it will be necessary to obtain the written consent of the juvenile's parent or responsible adult, prior to authorisation. The duration of such an authorisation is four months (with monthly reviews), as opposed to 12 months, as it is for the other types of CHIS authorisation. There are additional safeguards for juveniles identified within the Regulation of Investigatory powers (Juveniles) Order 2000 and the relevant Code of Practice.

2.11 The use of vulnerable persons should only be considered for authorisation as a CHIS in the most exceptional

circumstances. These are individuals who are or maybe by reason of mental disorder or vulnerability, other disability, age, illness is or maybe unable to take care of or protect themselves.

2.12 There may be occasions when the Local Authority may wish to use a CHIS as part of directed surveillance. It should be noted that the crime threshold which applies to directed surveillance does not apply to the use of a CHIS. As regards directed surveillance, the local authority can only authorise the use of surveillance under RIPA to prevent or detect criminal offences which are punishable by a maximum term of at least 6 months imprisonment (whether on summary conviction or on indictment) or are related to the underage sale of alcohol or tobacco. The crime threshold came into effect on 1st November 2012.

2.12 Unlike directed surveillance, which relates specifically to private information, authorisation for the use or conduct of a CHIS do not relate specifically to private information, but to the covert manipulation of a relationship to gain information. ECHR case law makes it clear that article 8 includes the right to establish and develop relationships. Accordingly, any manipulation of a relationship by the local authority is likely to engage article 8, regardless of whether or not the local authority intends to acquire private information. The local authority will therefore consider an authorisation wherever the use or conduct of a CHIS is likely to engage an individual

right under Article 8 of the ECHR, whether this is through obtaining information, particular private information, or simply through the covert manipulation of a relationship.

3. Responsibilities

3.1 The Director of Legal Services is responsible for the following –

- The integrity of the process in place for the management of CHISs
- Ensuring the proper implementation of this policy and the guidance and procedures that go with it.
- Ensuring the Council complies with the requirements of Part II of RIPA.
- Ensuring that due regard is given to any code of practice issued pursuant to section 71 of RIPA.
- Engaging with commissioners and inspectors when they conduct inspections under RIPA.
- Overseeing the implementation of any recommendations and post inspection action plans made by a commissioner.

3.2 The Divisional Director Public Realm and Divisional Director Community Safety are the Council's authorising officers for the purposes of considering applications for authorisation to use a CHIS, with the exception of cases where confidential information is either targeted or likely to be obtained. If the Divisional Director, Public Realm or Divisional Director

Community Safety are unavailable and the Director of Legal Services and Governance agrees that it is appropriate in respect of a specified application for authorisation, then the Head of Fraud and Risk may act as the Council's authorising officer in respect of that application.

3.3 In cases where the CHIS is targeted to obtain confidential information or confidential information is likely to be obtained, then the Council's authorising officer is the Chief Executive, or, in the Chief Executive's absence, the person acting as Chief Executive. Confidential information includes, but is not limited to matters subject to legal privilege, confidential personal information, journalistic material constituency business of MPs and finally confidential personal information relating to physical or mental health or spiritual counselling.

3.4 The Council considers that applications for authorisation to use covert human intelligence sources should be of a high and consistent standard. For this reason, all applications should be cleared by a gatekeeper before consideration by the authorising officer. The Council's gate-keeper is the Head of Community Safety. In the absence of that officer, the Intelligence Team Leader- Audit & Risk Management may act as the gatekeeper.

3.5 All officers have responsibility to ensure that CHISs are only used where there is an authorisation from the authorising

officer, and a Justice of the Peace or a District Judge (Magistrates' Court) has approved the authorisation.

3.6 Section 29(5) of the 2000 Act deals with the responsibilities of the controller and handler relating to the record keeper for any covert human intelligence source. Officers nominated to control, handle and record-keep in respect of a covert human intelligence source must be trained to the satisfaction of both the authorising officer and the Director of Legal Services before any authorisation may be granted.

3.7 The Council is committed to only using CHISs in accordance with RIPA and the Code of Practice. The Council has adopted a guidance manual to assist officers to make applications and grant authorisations in accordance with RIPA and the Code. The Council will have regard to the most recent relevant Code of practice. The current Code came into force on 13th December 2022.

4. Authorisations

- 4.1 Prior to a CHIS being used RIPA provides that the use must be authorised by the Council's Authorising Officer as defined in section 3 of this policy.
- 4.2 The Authorising Officer must believe that an authorisation for the use and conduct of a CHIS is necessary in the circumstances of the particular case on the ground specified in section 29(3) of RIPA, namely for the prevention and detection of crime or the prevention of disorder.
- 4.3 If the use or conduct of the CHIS is deemed necessary on the relevant ground, the Authorising Officer must also believe that it is proportionate to what is sought to be achieved by carrying it out. This involves balancing the seriousness of the intrusion into the private or family life of the subject of the operation (or any person who may be affected) against the need for the activity in investigative and operational terms.
- 4.4 The Authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render the use or conduct of a CHIS proportionate. Similarly, an offence may be so minor that any deployment of a CHIS would be disproportionate. No activity should be considered proportionate if the information which

is sought could reasonably be obtained by other less intrusive means.

Proportionality

4.5 The following matters should be considered:

- Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others
- Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives of obtaining the necessary result
- Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

Collateral Intrusion

4.6 Before authorising the use or conduct of a source, the authorising officer should take into account the risk of interference with the private and family life of persons who are not intended subjects of the CHIS's activity (collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise interference with the private and family life of those who are not the intended subjects of the CHIS activity. Where such collateral intrusion is unavoidable, the activities may still be authorised providing this collateral

intrusion is considered proportionate to the aims of the intended intrusion. Any collateral intrusion should be kept to the minimum necessary to achieve the objective of the operation. All applications should therefore include an assessment of the risk of any collateral intrusion, and details of any measures taken to limit this, to enable the Authorising Officer to fully consider the proportionality of the proposed use or conduct of a CHIS

- 4.7 Where the use of the CHIS is likely to result in the obtaining of confidential information, the activity must be authorised by the Chief Executive or on their absence the Monitoring Officer. Confidential information includes, but is not limited to matters subject to legal privilege, confidential personal information and confidential journalistic material.
- 4.8 The Authorising Officer should be clear as to the reason why the CHIS is necessary and the nature of the conduct that the CHIS will be involved in.

Security and Welfare

- 4.9 Where the council deploys a CHIS, it should take into account the safety and welfare of that CHIS when carrying out actions in relation to the authorisation or tasking. Before authorising the use of or conduct of a CHIS, the authorising officer 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.

4.10 The ongoing security and welfare of the CHIS after the cancellation of the authorisation, should also be considered at the outset. Consideration should also be given to the management of any requirement to disclose information tending to reveal the existence or identity of a CHIS to, or in, court

Extent of authorisations

4.11 Any authorisation under Part II of RIPA for the use or conduct of a CHIS will provide lawful authorisation for any such activity that:

- Involves the use or conduct of a CHIS as is specified or described in the authorisation
- Is carried out by or in relation to the person to whose actions as a CHIS, the authorisation relates; and
- Is carried out for the purposes of, or in connection with, the investigation or operation described

It is important that the CHIS is fully aware of the extent and limits of any conduct authorised and that those involved in the use of a CHIS are fully aware of the extent and limits of the authorisation in question.

Duration of authorisation

4.12 A written authorisation will, unless reviewed, cease to have effect at the end of 12 months, beginning with the day it took effect, except in the case of juvenile CHIS when it lasts for four months.

5. Combined authorisations

5.1 A single authorisation may combine two or more different authorisations. For example an authorisation for directed surveillance and the conduct of a CHIS. This does not preclude the local authority from obtaining separate authorisations. Where the use of a CHIS and directed surveillance are sought in the scope of one authorisation, the CHIS authorisation form should be used.

6. Reviews and Renewals

Reviews

6.1 Regular reviews of authorisations should be undertaken by the Authorising Officer to assess whether it remains necessary and proportionate to use a CHIS and whether the Authorisation remains justified. The review should include the use made of the CHIS during the period authorised, the tasks given to the CHIS and the information obtained from the CHIS. The results of the review should be retained for at least three years. Reviews of authorisations should take place as frequently as considered necessary and practicable. Where the use of a CHIS provides access to confidential information or involves significant collateral intrusion authorisations should be reviewed more frequently.

6.2 An authorisation for use of a CHIS lasts for a maximum of 12 months before having to be renewed.

Renewals

6.3 Before an Authorising Officer renews an authorisation, he must be satisfied that a review has been carried out of the

use of a CHIS, as outlined above and that the results of the review have been considered.

6.4 If before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may renew it in writing for a further period of twelve months. A further judicial approval will be required.

6.5 A renewal takes effect at the time at which the authorisation would have ceased to have effect but for the renewal. An application for renewal should therefore not be made until shortly before the authorisation period is drawing to an end.

7. Cancellations

- 7.1 The authorising officer who granted or renewed the authorisation must cancel it if it is satisfied that the use or conduct of the CHIS no longer satisfies the criteria for authorisation or the grounds on which it was granted.
- 7.2 Where necessary, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled.

8. Controller/Handler

8.1 The Council is required to ensure that arrangements are in place for the proper oversight and management of a CHIS, including appointing individual officers as defined in section 29(5)(a) of RIPA. Where the use of a CHIS is authorised then section 29(5)(a) of RIPA requires the Council to have at all times a person holding a position with the Council who will have day-to-day responsibility for dealing with the source (“the handler”). This will not be the officer seeking authorisation but will be the responsibility of the person who supervises the investigation.

8.2 The person identified as the handler will have day to day responsibility for:

- Dealing with the CHIS on behalf of the authority concerned
- Directing the day to day activity of the CHIS
- Recording the information supplied by the CHIS
- Monitoring the CHIS’s security and welfare

The CHIS handler is responsible for bringing to the attention of the CHIS controller any concerns about the personal circumstances of the CHIS in so far as they might affect the validity of the risk assessment, the conduct of the CHIS, and the safety and welfare of the CHIS. In appropriate circumstances the authorising officer should consider whether or not to allow the authorisation to continue.

- 8.3 Further, section 29(5)(b) of RIPA requires the Council to have at all times another person holding a position with the Council who will have general oversight of the use made of the source (“the controller”). The controller is the officer responsible for the general oversight of the use of the source. The controller will be the Service Manager for the Service in which the officer seeking the authorisation is based so that the Service Manager will be the controller and will be the person managing the handler.
- 8.4 The Council will not permit an authorising officer to be responsible for authorising their own activities, e.g. those in which they, themselves, are to act as the source or in tasking the source. Therefore if the authorising officer would be the Service Manager for the handler then a Service Manager of the same level from another Service will be the controller.
- 8.5 Additionally, section 29(5)(c) of RIPA requires the Council to have at all times a person holding a position with the Council who will have responsibility for maintaining a record of the use made of the CHIS. This will be the Service Head (i.e. the Service Manager’s manager) responsible for the service area using the covert human intelligence source. If the service area falls within the authorising officer’s

responsibility, then the Corporate Director of Communities must maintain the record.

8.6 Guidance suggests that a local authority may prefer to seek the assistance of the police to manage its CHIS. In such a case a written protocol between the parties should be produced in order to ensure that an identified CHIS is properly managed. Without such an agreement the local authority must be capable of fulfilling its statutory responsibilities. Where the CHIS is not a Council Officer then the intention is to seek assistance of the police. Where the CHIS is a Council Officer then prior to the authorisation being sought, the investigating officer must give consideration to seeking the assistance of the Police and if it is decided not to, then justification for that decision must be included within the risk assessment for the use of the CHIS.

9. Security of Covert Technical Equipment

9.1. The Council requires each Service that uses covert technical equipment when undertaking surveillance to ensure that such equipment is securely locked away when not used. Further, such equipment will only be issued to an officer who has authorisation to use it. There will be a logging in and out book and the officer will be required to sign for the equipment. In signing for the equipment, the officer will be reminded that misuse of the equipment is a disciplinary offence.

10. Central Recording

10.1. The Council is required to keep records in relation to authorisations centrally. Those records will be maintained by Legal Services. These records should be updated whenever an authorisation is granted, renewed or cancelled and should be available to the relevant Commissioner or an Inspector upon request. Records should be retained for at least 3 years from the end of the authorisation to which they relate.

10.2. The relevant authorising officer must provide copies of all authorisations and all reviews, renewals and cancellations to the Director of Legal Services and Governance or a person nominated by either of them. The authorisation officer must provide those documents forthwith following signing by the authorising officer.

10.3. All officers are expected to use the most up to date versions of forms recommended by the Home Office.

11. Training

11.1 Authorising officers can only authorise once they have undertaken training on the operation of RIPA and the Code of Practice. The Council's gatekeepers may only clear applications for consideration by the authorising officer after undertaking the same training as the authorising officers.

11.2 Officers may only undertake the roles of controller, handler, or record-keeper if they have undertaken training in the discharge of those roles. If there are no officers who have been trained to the satisfaction of the authorising officer and the Divisional Director - Legal, then the Council will not use covert human intelligence sources.

11.3 All officers who may seek to use covert human intelligence sources during an investigation must also have undertaken training on the operation of RIPA and the Code of Practice.

11.4 The Council will arrange appropriate training courses at regular intervals. It is expected that members of the Corporate Leadership Team will require authorising officers, gatekeepers and those who may apply to conduct directed surveillance to undertake the training.

12. Member Oversight

12.1 The Council's Standards Committee review this Policy and will have oversight of the Council's use of covert human intelligence sources. If issues arise, the Audit s Committee will make recommendations to Cabinet for action.