

# STRONGER together



Lewes District Council



Working in partnership with **Eastbourne Homes**

<b>Document name:</b>	Policy on use of covert surveillance and/or covert human intelligence sources
<b>Document type:</b>	Policy

<b>Authority(ies) covered:</b>	Aligned
<b>Responsible (Executive Lead):</b>	Councillor James MacCleary, Leader of LDC; Cllr David Tutt, Leader of EBC
<b>Accountable (Operational Lead):</b>	Oliver Dixon Senior Responsible Officer
<b>Version (e.g. first draft, final report):</b>	Final report following IPCO inspection recommendations from June 2022
<b>Approved by:</b>	LDC Audit and Standards and EBC Audit and Governance Committees
<b>Date of publication:</b>	November 2022
<b>Revision due:</b>	November 2023
<b>Final Equality and Fairness Analysis (EaFA) report approved by:</b>	Not applicable
<b>Date final EaFA report approved:</b>	Not applicable

# Contents

1. Introduction
2. Procedure
3. Management of a CHIS
4. Review and renewal of a CHIS authorisation
5. Processing of confidential information obtained from surveillance
6. Data retention, review and destruction
7. Training and policy review
8. Conclusion
9. Appendices

## Introduction

1. The Human Rights Act 1998 gave effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Some of these rights are absolute, while others are qualified, meaning that it is permissible for the state to interfere with those rights if certain conditions are satisfied. Amongst the qualified rights is a person's right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR. It is Article 8 that is most likely to be engaged when public authorities seek to obtain private information about a person by means of covert surveillance. Article 6 of the ECHR, the right to a fair trial, is also relevant where a prosecution follows the use of covert techniques.
2. Part 2 of the Regulation of Investigatory Powers Act 2000 (RIPA) provides a statutory framework under which covert surveillance and/or use of covert human intelligence source (CHIS) can be authorised and conducted compatibly with the ECHR.
3. As part of their investigation activities to prevent and detect certain criminal offences, the Councils may need to undertake covert surveillance of individuals to gather evidence of illegal activity. They may also need to deploy a covert human intelligence source ('CHIS').
4. For the purposes of this policy, covert surveillance is taken to mean 'directed surveillance' which has a specific definition under section 26 of RIPA and is set out in full at Appendix 1.
5. The definition of a CHIS is set out in Appendix 2(a) of this policy. The distinction between a CHIS and a member of public merely volunteering information to the Council is explained at Appendix 2(b).
6. The use of social media as an intelligence gathering and/or investigations tool and, separately, the acquisition of communications data, are subject to their own respective policy statements; these are available as stand-alone documents on the Councils' website.

## Procedure

7. All physical or on-line covert surveillance (irrespective of whether its use falls within the ambit of the Regulation of Investigatory Powers Act 2000) and any use of a CHIS shall be undertaken in accordance with the procedures set out in this policy statement<sup>1</sup>.
8. The Councils shall ensure that covert surveillance and/or the use of CHIS is only undertaken where it complies fully with all applicable laws, in particular the:
  - Human Rights Act 1998 (incorporating the fundamental rights and freedoms contained in articles 2 to 14 of the European Convention on Human Rights)
  - Regulation of Investigatory Powers Act 2000 ('RIPA')
  - Protection of Freedoms Act 2012
  - General Data Protection Regulation
  - Data Protection Act 2018
9. The Councils shall, in addition, have due regard to all official guidance and codes of practice, particularly those issued by the Home Office, the Investigatory Powers Commissioner's Office and the Information Commissioner's Office. Of these, the most significant are:
  - Covert Surveillance and Property Interference – Code of Practice (Home Office, August 2018)
  - Covert Human Intelligence Sources – Revised Code of Practice (Home Office, August 2018)
10. In particular, the following guiding principles shall form the basis of all covert surveillance and CHIS activity undertaken by the Councils:
  - (i) Covert surveillance and/or the use of a CHIS shall only be undertaken where it is absolutely necessary and only for the purpose of preventing or detecting a criminal offence.
  - (ii) Covert surveillance and/or the use of a CHIS shall only be undertaken where it is proportionate to do so and in a manner that is proportionate.
  - (iii) No monitoring of social network sites for investigation purposes shall take place without considering whether such monitoring constitutes directed surveillance; nor, where it is considered to be so, without obtaining the requisite prior authorisation and approval.
  - (iv) Adequate regard shall be had to the rights and freedoms of those who are not the target of the covert surveillance.

---

<sup>1</sup> Except that, as stated in paragraph 10(vi), judicial approval is required only in relation to directed surveillance regulated by RIPA and the use of a CHIS.

- (v) All authorisations to carry out covert surveillance and/or to use a CHIS shall be granted by appropriately trained and designated authorising officers.
  - (vi) Directed surveillance and/or the use of a CHIS shall only be undertaken after obtaining the approval of a justice of the peace (a magistrate or district judge).
11. With this mind, the Councils have adopted a policy of not normally conducting covert surveillance and/or using a CHIS but of doing so only as a last resort, where all other investigative options have been deemed insufficient. Whilst each situation will be considered on its own merits and all relevant factors will be taken into account, covert surveillance and/or the use of a CHIS will be considered only where deemed a proportionate response of last resort.

### **Management of a CHIS**

12. Where the Councils have obtained the necessary internal authorisation and judicial approval for the use of a CHIS, they will ensure that arrangements are in place for the proper oversight and management of the source, including appointing individual officers to act as 'controller' and 'handler' for each one. The Senior Responsible Officer for RIPA will determine on a case by case basis which officers will assume these roles for each deployment of a CHIS.
13. The 'controller' will normally be responsible for the management and supervision of the 'handler' and general oversight of the use of the CHIS. In addition, the controller should maintain an audit of case work sufficient to ensure that the use or conduct of the CHIS remains within the parameters of the extant authorisation.
14. The 'handler' will have day to day responsibility for:
- dealing with the CHIS on behalf of the council
  - directing the day to day activities of the CHIS;
  - recording the information supplied by the CHIS; and
  - monitoring the CHIS's security and welfare.
15. The handler of a CHIS will usually be of a rank or position below that of the authorising officer.

### **Review and Renewal of a CHIS Authorisation**

16. The authorising officer who grants an authorisation should (i) consider subsequent renewals of that authorisation and any related security and welfare issue, and (ii) stipulate the frequency of formal reviews to be undertaken with the controller and handler.
17. Where the nature or extent of intrusion into the private or family life of any person becomes greater than that anticipated in the original authorisation, the authorising officer should immediately review the authorisation and reconsider the proportionality of the operation. This should be highlighted at the next renewal (if applicable).

18. Any proposed changes to the nature of the CHIS operation (i.e. the activities involved) should immediately be brought to the attention of the authorising officer. The authorising officer should consider whether the proposed changes are within the scope of the existing authorisation and whether they are proportionate (bearing in mind any extra interference with private or family life or collateral intrusion), before approving or rejecting them. Any such changes should be highlighted at the next renewal (if applicable).

### **Processing of Confidential Information Obtained from Surveillance**

19. Surveillance activity may result in the collection of evidence which the subject of the investigation or operation would consider confidential. Particular care must be exercised in cases where the subject might reasonably assume a high degree of confidentiality. The four categories of information that demand very careful handling are as follows:
  - (i) material containing information that is legally privileged;
  - (ii) confidential journalistic material or where material identifies a journalist's source;
  - (iii) material containing confidential personal information; and
  - (iv) communications between a Member of Parliament and another person on constituency business.
20. The scope of material containing information that would be deemed legally privileged is set out in Appendix 3 of this policy statement.
21. The acquisition of material subject to legal privilege is particularly sensitive and may give rise to issues under Article 6 (right to a fair trial) ECHR as well as engaging Article 8 (right to respect for family and private life). The Councils must therefore apply additional safeguards if it anticipates obtaining information of this type (intentionally or in error) during covert surveillance. The safeguards should provide for three different circumstances where legally privileged items will or may be obtained, namely–
  - (i) where privileged material is intentionally sought;
  - (ii) where privileged material is likely to be obtained; and
  - (iii) where the purpose or one of the purposes is to obtain items that, if they were not generated or held with the intention of furthering a criminal purpose, would be subject to privilege.
22. Where a council investigating officer anticipates the occurrence of any of the circumstances at paragraph 19 above, he/she must consult the RIPA Monitoring Officer before submitting an application for authorisation. The RIPA MO will have regard to relevant legislation and codes of practice in advising on the appropriate safeguards that would be required before the covert surveillance may lawfully proceed, assuming the necessary council authorisation and judicial approval required by RIPA were already in place.
23. Directed surveillance likely or intended to result in the acquisition of knowledge of confidential or privileged material may be authorised only by the Councils' Chief Executive or (in their absence) the person acting in that role. This authorisation level is set at a more senior level than that required for other surveillance activity, reflecting the sensitive nature of such information.

## **Data Retention, Review and Destruction**

24. All material obtained through CHIS or covert surveillance operations, including all copies, extracts and summaries, must be handled and stored securely on Council systems to reduce the risk of loss or theft. Access to the material must be restricted to Council officers undertaking the operation or where necessary as part of the retention process or legal proceedings.
25. All material which could be relevant to a pending or future criminal or civil proceedings must be reviewed regularly to establish the aims of the authorisation are being met and retained in accordance with established disclosure requirements detailed in the Criminal Procedure and Investigations Act 1996.
26. Information obtained through CHIS or covert surveillance operations, and all copies, extracts and summaries should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer required in accordance with the Council's Data Retention, Storage and Disposal Policy.

## **Training and Policy Review**

27. All Council officers undertaking or authorising covert surveillance and/or using CHIS shall be appropriately trained to ensure that they understand their legal and moral obligations.
28. Periodic audits shall be carried out to ensure that officers are complying with this policy.
29. The Senior Responsible Officer for RIPA (currently the Head of Legal Services) shall review this policy at least once a year in the light of the latest legal developments and changes to official guidance and codes of practice.
30. The operation of this policy shall be overseen by the Audit & Standards Committee and Audit & Governance Committee by receiving reports every 12 months on this policy and its implementation, and on any RIPA activity conducted during the preceding 12-month period.

## **Conclusion**

31. All citizens will reap the benefits of this policy, through effective enforcement of criminal and regulatory legislation and the protection that it provides.
32. Adherence to this policy will minimise intrusion into citizens' lives and guard against any legal challenge to the Councils' covert surveillance and CHIS activities.
33. Any questions relating to this policy should be addressed to:

Oliver Dixon, RIPA Senior Responsible Officer

Lee Ewan, Counter Fraud and Investigations Manager and RIPA Monitoring Officer

## **Appendices**

- Appendix 1: Definition of directed surveillance
- Appendix 2(a): Definition of a CHIS
- Appendix 2(b): Distinction between a CHIS and a person volunteering information to the council
- Appendix 3: Description of information to be treated as legally privileged

## **Appendix 1 – Definition of Directed Surveillance**

Surveillance is ‘directed’ if undertaken–

- (i) in a manner that is covert but not ‘intrusive’ – see note 1 below;
- (ii) for the purposes of a specific investigation or a specific operation;
- (iii) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation);
- (iv) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance.

### Note 1

For the purposes of RIPA, ‘intrusive’ surveillance is covert surveillance that–

- (a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and
- (b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

### Note 2

Local authorities are not permitted to carry out ‘intrusive’ surveillance.

### Note 3

For local authorities, directed surveillance is amenable to authorisation under RIPA only where its purpose is the prevention or detection of a criminal offence that is punishable by a maximum term of at least six months’ imprisonment; or is related to the underage sale of alcohol and tobacco or nicotine inhaling products.

## **Appendix 2(a) – Definition of a Covert Human Intelligence Source (CHIS)**

Under the Regulation of Investigatory Powers Act 2000 Act, a person is a CHIS if:

- (1) they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (2) or (3) below;
- (2) they covertly use such a relationship to obtain information or to provide access to any information to another person; or
- (3) they covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

In relation to paragraph (1) above, 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.

In relation to paragraphs (2) and (3) above, 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 that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

## **Appendix 2(b) – Distinguishing between a CHIS and a member of the public volunteering information to the Council**

The key feature of a CHIS is the establishing and maintaining of a relationship with another person for a covert purpose.

In many cases involving information sourced from individuals, a relationship will **not** have been established or maintained for a covert purpose. A resident or someone who works in or visits the district or borough ('the source') may simply volunteer or provide information that they have observed or acquired other than through a relationship, without being induced, asked, or tasked by the Councils. In these circumstances, the source is not a CHIS for the purposes of RIPA and no authorisation under RIPA is required.

The Councils provide a confidential telephone and online facility to report suspected fraud. Even if the person using this facility is involved in the activities they are reporting, they would not be considered a CHIS as the information is not being disclosed on the basis of a relationship which was established or maintained for that covert purpose. However, should the person be asked to maintain their relationship with others involved and to continue to supply information (or it is otherwise envisaged that they will do so), an authorisation for the use or conduct of a CHIS may be appropriate.

### **Appendix 3 – Description of information to be treated as legally privileged**

- (1) Communications between a professional legal adviser and—
  - (a) his client, or
  - (b) any person representing his client,  
which are made in connection with the giving of legal advice to the client.
  
- (2) Communications—
  - (a) between a professional legal adviser and his client or any person representing his client, or
  - (b) between a professional legal adviser or his client or any such representative and any other person,  
which are made in connection with or in contemplation of legal proceedings and for the purposes of such proceedings.
  
- (3) Items enclosed with or referred to in communications of the kind mentioned in (1) or (2) above and made—
  - (a) in connection with the giving of legal advice, or
  - (b) in connection with or in contemplation of legal proceedings and for the purposes of such proceedings.