

Shadow RIPA Surveillance Policy

General Statement of Policy

- **This policy document relates to use by Lancashire County Council officers of directed surveillance, and covert human intelligence sources not undertaken in relation to the prevention and detection of crime or which fall outside the RIPA regime due to offence penalties not meeting the thresholds laid down for the RIPA regime to apply.**
- **The County Council is committed to upholding human rights**
- **As a public body and responsible employer, the County Council wants to conform to the spirit of the requirements of the Regulation of Investigatory Powers Act 2000 and associated regulations and codes of practice relating to the use of covert surveillance, the use of covert human intelligence sources,**
- **County Council officers will only undertake surveillance work outwith the RIPA regime when it is both necessary and proportionate to the ends it seeks to achieve.**

CONTENTS

Introduction

- 1. Purpose**
- 2. Scope**
- 3. Responsibilities**
- 4. References**
- 5. Procedure – Directed Surveillance in relation to Lancashire County Council employees**
- 6. Procedure – Directed Surveillance in relation to Lancashire County Council residents**
- 7. Procedure – Covert Human Intelligence Source**
- 8. Monitoring and Retaining Applications**
- 9. Handling Product from Surveillance Activities**

Introduction

The Regulation of Investigatory Powers Act 2000 (RIPA) does not grant powers to carry out surveillance. It simply provides a framework that allows the Council to authorise and supervise surveillance in a manner that ensures compliance with the Human Rights Act 1998. Equally, RIPA does not prevent surveillance from being carried out or require that surveillance may only be carried out under RIPA. Where a public authority carries out surveillance in accordance with RIPA this provides protection against a claim of infringement of an individual's human right to a private and family life, his home and his correspondence.

RIPA can however only be used by a local authority for the purposes of preventing and detecting crime.

There will be times when it will be necessary and proportionate to carry out covert Directed Surveillance or use a CHIS other than by using RIPA either because the investigation is not carried out for the purposes of preventing or detecting crime, or because, in the case of directed surveillance, the penalty for the offences under investigation is below the threshold which would enable use of a RIPA authorisation. This could include surveillance for the purposes of monitoring employees who may be under investigation. It could also include matters where the authority is involved in litigation and may wish to carry out surveillance to verify whether or not information provided is true or false – for example in child protection matters where there are questions raised as to residency of individuals who may pose a threat to a child .

Indeed, there may be circumstances in which the use of Directed Surveillance or employment of a CHIS is the only effective means of efficiently obtaining significant information to take an investigation forward.

Provided the established principles of necessity, proportionality and collateral intrusion are considered, the Authority will be in a strong position to meet any challenge in respect of infringement of human rights.

Each application for covert surveillance authorisation will be assessed on a case by case basis to determine whether the application meets the criteria for the formal RIPA authorisation procedure to be followed. In all other cases the shadow RIPA regime will apply.

The Report of the Investigatory Powers Commissioner in 2017 supports the implementation of a non RIPA authorisation process that runs in parallel to any RIPA approvals in circumstances where an authorisation is unavailable under the Act.

1. Purpose of This Policy

To establish guidance within Lancashire County Council services for seeking approval for the conduct by officers of directed surveillance, and the use of covert human intelligence sources (CHIS) **which is not undertaken for the prevention or detection of crime or where the penalty for the offence under investigation falls below the threshold for Directed Surveillance to be approved under the RIPA regime.**

If the surveillance is undertaken for purposes related to the prevention and detection of crime, reference must be made to the Corporate Policy and Guidance on the Regulation of Investigatory Powers Act 2000.

This policy is Intended to cover surveillance carried out in such situations as investigations into serious allegations regarding the conduct of employees, observations on private residences to determine the veracity of information provided to the County Council in connection with the exercise of its functions, use of sources to provide information in person or on the internet or to provide officers with information in circumstances which would be covered by relevant codes of practice if the activity was undertaken for the prevention and detection of crime.

2. Scope

2.1 Surveillance which is covert but not intrusive and undertaken for the purposes of a specific investigation or operation, 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) and otherwise than by way of an immediate response to events or circumstances, the nature of which is such that it would not be reasonable practicable for an authorisation under the Act to be sought for the carrying out of the surveillance.

Private information in relation to a person includes any information relating to his private or family life. **Note that this can include information about family, professional and business relationships.**

2.2 The use of Covert Human Intelligence Sources (CHIS). A CHIS is a person who establishes or maintains a personal or other relationship with another person for the covert purpose of:

- (a) Using such a relationship to obtain information or to provide access to information to another person, or
- (b) Disclosing information obtained by the use of such a relationship or as a consequence of such a relationship.

In addition, a person who covertly provides information to a public authority is potentially a CHIS if he has obtained that information in the course of or as a consequence of the existence of a personal or other relationship, whether or not the relationship has been established or maintained for that purpose. A repeat informant, if and when it becomes apparent that he obtains his information in that way, is a CHIS to whom a duty of care is owed, if the information is acted upon. Legal advice should be taken before acting on the information provided by informants.

3. Responsibilities

- Director of Corporate Services – Senior Responsible Officer
- Head of Trading Standards Service and Trading Standards Managers – designated authorisers
- Heads of Service – awareness and day to day management
- Service Managers – awareness and day to day management

4. References

- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Protection of Freedoms Act 2012
- Codes of Practice on Covert Surveillance and CHIS
- Corporate Guidance

5. Procedure – Directed Surveillance in relation to Lancashire County Council employees

If during the course of any investigation or enquiry into an Lancashire County Council employee, the investigating officer believes it necessary to carry out directed surveillance on any person involved in the investigation he shall consider the possibility of obtaining any private information about that person and if there is such a possibility, authorisation on the relevant form should be sought by completing and forwarding the form E1 -2020 to one of the designated authorising officers.

Those carrying out the covert surveillance should inform the authorising officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way. This is known as collateral intrusion and steps should be taken to minimise the risks of the surveillance affecting other individuals who are not targets of the investigation, including considering the appropriateness of recording and retention of evidence regarding those individuals.

Before giving the authorisation, the authorising officer will at first satisfy him/herself that the authorisation is necessary on particular grounds and that the surveillance is proportionate to what it seeks to achieve. This could include, for example, serious disciplinary investigations.

Assessing proportionality includes the following:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived conduct;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others
- Considering whether the surveillance activity is an appropriate response 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

If other overt methods of obtaining the information can be tried, then these methods should be attempted – covert surveillance should be the last resort.

Where there is a possibility that confidential material may come into the possession of the Service special safeguards should be observed.

In such circumstances the matter should be referred to the Chief Executive immediately and legal advice sought. (If the Chief Executive is not available, the matter should be referred to a Chief Officer, it is not appropriate for the matter to be delegated).

Confidential material is defined in the Home Office code of practice but relates to matters subject to legal privilege; confidential personal information; or confidential journalistic material. Such material should not be retained or copied unless necessary for a specific purpose, should not be disseminated except for a specific purpose and if retained or disseminated this should be done with a clear warning of its confidential nature. Reasonable steps should be taken to ensure that there is no possibility of its content being known to any person whose possession of it might prejudice any criminal or civil proceedings related to the information.

Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

6. Procedure – Directed Surveillance on Lancashire County Council Residents

The Council receives complaints and information on occasions in relation to LCC residents who are alleged to be involved in activities which may infringe child protection guidelines or other County Council guidelines.

Covert surveillance can only be authorised in relation to Lancashire County Council residents by the designated Head of Trading Standards and Trading Standards Managers. The applicant should outline in the application why the activity is considered to be necessary and proportionate, as in paragraph 5 above.

7. Procedure – Covert Human Intelligence Sources

The Council receives complaints/information routinely from the public regarding the alleged activities of individuals. The actions of these complainants do not generally fall within the definition of a covert source since they are a one off provision of information. However, a person may become a covert source if an ongoing relationship with the Council develops and activities described in above are carried out. The use of CHIS could also cover circumstances where an employee of LCC establishes a relationship in order to gain information about a particular situation.

Where the nature of the complaint relates to a matter where an officer requests the complainant to obtain further information covertly via a relationship with another individual, this activity is likely to fall within CHIS. A shadow authorisation will therefore be required before seeking such information. By following the authorisation procedures, the Council will also be in a position to seek to safeguard the identity of the source in any subsequent legal proceedings.

Further guidance should be sought from the Director of Corporate Services on this issue to ensure that the identities of any such individuals are safeguarded in the event of any legal proceedings, tribunals or disciplinary hearings.

NB: Juvenile surveillance CHIS – normally no one under 18 years or any vulnerable individual should be considered as a CHIS.

8. Monitoring and Retaining Applications

The Local Authority must maintain a central record of all Authorisations. This is the responsibility of Information Governance. These records will be confidential and should be retained for a period of at least five years from the ending of the authorisation. Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.

Authorisations last for a period of three months and may be renewed more than once, if necessary, by completion of the relevant document. The renewal should be kept/recorded as part of the "authorisation record".

Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the relevant form (**E2 - 2020**). Generally, unless circumstances dictate otherwise, reviews will be carried out at monthly to six weekly intervals.

Once surveillance activities have ceased, the officer who made the application must submit an application for cancellation to the Authorising officer. The cancellation application should be submitted immediately the activities are no longer required. The authorising officer who granted an authorisation must cancel it if satisfied that the action authorised by it is no longer necessary.

In summary, the **practical procedure** for obtaining an Authorisation is as follows:

1. A completed application should be submitted to the authorising officer using form **E1-2020**. The authorising officer will consider the necessity and proportionality of the application and the likelihood of any collateral intrusion.
2. A review should take place at monthly to six weekly intervals. (**Form E2 – 2020**)
3. At the end of the surveillance operation, the investigating officer will submit a cancellation form (**E3-2020**) to the authorising officer. A copy of the cancellation form will be given to the investigating officer. All forms will be provided to Information Governance for retention in the central record.
4. The investigating officer may seek a renewal of the authorisation if necessary (**Form E4 – 2020**).
5. Copy documents will be retained on the investigation file.

9. Handling Product from Surveillance Activities

Product from Covert Surveillance activities may consist of:

- Photographs
- Video film
- Voice recordings
- Surveillance log
- Officer's notes

The above may be required as evidence in current or future proceedings. Officers must have regard to Data Protection provisions in relation to this material. Product obtained via an authorisation may be used by the authority in other investigations.

Officers should record the results of any surveillance. When product is disposed of, a note should be made on the file.

The use of any product obtained by authorised surveillance activities outside of the Public Authority or the Courts should only be authorised in the most exceptional circumstances. This requirement seeks to prevent product from being used for grounds other than that for which it was obtained. **Joint operations should make reference to the potential use of evidence by each agency.**

Officers may receive requests from other agencies for product, which may include photographs of suspects, descriptions, and vehicle details. Where this information has been obtained under an authorisation, further guidance should be sought from the Authorising Officer, since disclosure may not be permitted under the provisions of the Code of Practice.

Version Control

Named Owner:	Laura Sales: Director – Corporate Services
Version Number:	4.00
Date Of Creation:	November 2016
Last Review:	August 2021
Next Scheduled Review:	July 2022
Overview of Amendments to this Version:	Grammatical and formatting changes only