Durham County Council
RIPA Policy
2023

Contents

Definitions

The Act, or RIPA

Regulation of Investigatory Powers Act 2000

Authorising Officer

The person(s) designated under Sections 28 and 29 of the Act to grant authorisations for directed surveillance and the use and conduct of a Covert Human Intelligence Source, respectively. Within a Local Authority this may be a Corporate Director, Head of Service or Service Manager. The Council's Authorising Officers for RIPA are appointed by the Chief Executive.

Communications Service Provider

These include telecommunications, internet (including email) and postal service providers.

Conduct of a Source

Any action of that source, falling within the terms of the Act, or action incidental to it (i.e., what they do).

Controller

In relation to a CHIS, the person or designated managerial officer responsible for overseeing the use of the source and recording this information.

Covert Human Intelligence Source (CHIS)

Commonly known as Agents, Informants, Undercover Officers. Means a person who establishes a personal or other relationship with someone else for a specified covert purpose.

Covert Surveillance

Surveillance carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is taking place.

Designated Person

This is the authorising officer for the purposes of obtaining communications data who must be registered with the National 4 Anti-Fraud Network by the SRO. This person must not be the applicant.

Directed Surveillance

Surveillance which is covert but not intrusive, is conducted for the purposes of a specific investigation, is likely to result in the obtaining of private information about a person and is conducted 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 Part II of the Act to be sought.

Handler
An investigating officer, in relation to CHIS, having day to day responsibility for: - dealing with the source on behalf of the authority; - directing the day to day activities of the source; - recording the information supplied by the source; and - monitoring the security and welfare of the source.

Intrusive Surveillance
In no circumstances is the Council permitted to carry out intrusive surveillance. Covert surveillance carried out in relation to anything taking place on residential premises or in any private vehicle, which involves the presence of an individual on the premises or in the vehicle, or is carried out by means of a surveillance device. Surveillance which is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle, but is carried out without that device being present on the premises or in the vehicle, is not intrusive unless the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

IPCO
Investigatory Powers Commissioner's Office.

Private Information
This includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships. Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private 5 information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public, and where a record is being made by a public authority of that person's activities for future consideration or analysis. Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes surveillance, a directed surveillance authorisation may be considered appropriate.

RIPA Monitoring Officer

This is the Senior Lawyer for Commercial and Corporate Governance who is responsible for maintaining the central register, the oversight of RIPA applications and training.

Senior Responsible Officer (SRO)
This is the Head of Legal and Democratic Services who is responsible for the integrity of the process in place within the authority for surveillance, compliance with Part II of RIPA and the Codes of Practice, oversight of reporting errors, engagement with the IPCO during and post inspections.

Tasking
An assignment given to the source, asking him or her to obtain information, to provide access to information, or to otherwise act incidentally for the benefit of the relevant public authority.

"The Use" of a source

Any action to induce, ask or assist a person engaged in the conduct of a source or to obtain information by means of an action of the source. (What they are asked to do).

Surveillance includes:

- monitoring, observing or listening to persons, their movements, their conversations, or their activities or communications;
- recording anything monitored, observed or listened to in the course of surveillance; and
- surveillance by or with the assistance of a surveillance device (any apparatus designed or adapted for use in surveillance).

1. Introduction

1.1 The Regulation of Investigatory Powers Act 2000 ("RIPA") ("the Act") controls and regulates surveillance and other means of information gathering which public bodies employ in the discharge of their functions.

1.2 Durham County Council ("the Council") is committed to respecting all human rights and our RIPA policy demonstrates how we can carry out an investigation in a way which is compatible with Schedule 1, Article 8 of the Human Rights Act 1998, right to respect for private and family life.

1.3 The RIPA legislation regulates the following:

- Directed Surveillance;
- Intrusive Surveillance;
- The conduct and use of Covert Human Intelligence Sources (CHIS); and
- Communications Data

1.4 The Council is only permitted to undertake directed surveillance and the use of Covert Human Intelligence Sources and in no circumstances can there be an authorisation for intrusive surveillance.

1.5 As well as the Council's use of RIPA being regulated by the legislation, there are also Codes of Practice which set out the authorisation procedures and records which must be followed by the Council when undertaking investigations which fall within the scope of RIPA.

1.6 Enforcement activities of the Council which fall within the remit of RIPA are also subject to monitoring and oversight by the Investigatory Powers Commissioner's Office.

1.7 It is intended that this document will give a brief overview of the Council's use of RIPA and is aimed at members of the general public. Durham County Council staff must refer to the full corporate guidance document available on the intranet.

1.8 It should be noted that all relevant Durham County Council staff receive regular training on the use of RIPA and on the Council's policy and procedure regarding the correct use of RIPA.

2. Surveillance

2.1. As part of its investigations into serious criminal offences, the Council may carry out directed surveillance. Directed surveillance means surveillance which is conducted in a manner to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. It does not include intrusive surveillance (consisting of monitoring people in residential premises or private vehicles) which **cannot** be carried out by local authorities.

2.2. For the Council to be able to carry out directed surveillance for serious criminal offences (i.e., those attracting a maximum prison sentence of six months or more, or are related to the underage sale of alcohol, tobacco or nicotine inhaling products) the Council must apply for a RIPA authorisation.

2.3. A RIPA authorisation is granted by judicial approval following an application to the Magistrates Court by an Authorising Officer. An 'Authorising Officer' is the designated person(s) under Sections 28 and 29 of the Act. The Council's Authorising Officers for RIPA are appointed by the Chief Executive of the Council.

2.4. The Council also has its own procedure which it follows before making an application to the Magistrates Court. The Authorising Officer must also be satisfied that the proposed surveillance is necessary for the prevention of crime and is proportionate to what it seeks to achieve. This is to ensure the Council are balancing the human rights of residents with the need to tackle illegal activity.

2.5. All authorisations are regularly reviewed by the Council to ensure each authorisation is justified and meets the aims in which the authorisation was sought, ultimately ensuring the use of surveillance is necessary.

2.6. The Council are only authorised to collect evidence for which it has approval via the authorisation (unless in the event of an emergency).

2.7. The Council will only seek authorisation for surveillance which is deems necessary and the conduct which is being surveyed must be identified prior to seeking an authorisation.

2.8. When seeking an authorisation, the Council must be satisfied that the surveillance is proportionate to the aim the Council seeks to achieve. Therefore prior to seeking an authorisation the Council must be satisfied the surveillance meets its internal test of proportionality.

2.9. The Council's use of RIPA is also governed by annual reviews by the elected members of the Council. Members are not involved in individual authorisations but will consider the Council's use of RIPA.

2.10. Authorisations begin on the day they are approved by the Justice of the Peace and are valid for three months, unless cancelled. Expiry will be considered to be three months minus one day from the signature of approval by the Justice of the Peace.

2.11. Authorisations may be renewed for a further period of three months. A renewal grant must be approved by a Justice of the Peace. Authorisations may be renewed more than once providing the renewal meets the criteria for renewal. The number of renewals should be recorded, and details of any renewal should be recorded centrally.

2.12. The Authorising Officer should ensure they have implemented a system to review authorisations before their expiry. Timings of renewals shall be determined by the Authorising Officer; this must be stated within each authorisation as a 'control measure.' Authorisations should be reviewed prior to expiry to determine whether it is necessary to renew the authorisation, this must be conducted at least ten days prior to expiry.

2.13. Aspects of the authorisation may be reviewed by the Authorising Officer, for example the use of specific tactics may no longer be deemed appropriate or discontinuing surveillance against particular persons.

2.14. Reviews must be presented either by email or paper copy to the Senior Responsible Officer and/RIPA Monitoring Officer within 24 hours of the review and must not be backdated.

3. Covert Human Intelligence Sources

3.1 Covert Human Intelligence Sources or 'CHIS' sources are often referred to as Under Cover Officer, Informants/Agents. This person establishes or maintains a relationship with another person for the covert purpose of:

- Gathering information to provide access to information
- Disclosing information obtained

3.2 A covert relationship is established where it is conducted in manner that a person is unaware of its purpose. Where evidence is obtained through directed surveillance authorisation is not required.

3.1 The Council regularly receives complaints from members of the public and traders regarding the alleged activities of individuals. Quite often those actions will fall outside the definition of a covert source, however, if an individual develops an ongoing relationship with the Council the relationship will become subject to the CHIS policy.

3.2 Where evidence is gathered covertly, the deployment of a CHIS is likely to be governed by the RIPA act. An authorisation would be required, and the use of a CHIS would be subject to the same safeguards which apply to standard authorisations, and is backed up by the Code of Practice which regulates and controls the use of CHIS.

3.3 Should the Council fail to obtain an authorisation or use an authorisation improperly it may render them as liable to infringe the human rights of an individual and could impact the use of that evidence in obtaining a prosecution.

3.4 The Investigating Officer and controller (a Handler) will manage any relationships with informants ensuring the use of informants is necessary and remains relevant to the aim.

3.5 The council always place the health and safety of a CHIS at high regard, foreseeable consequences of deploying an informant will be considered. Therefore, the Council will conduct a risk assessment prior the commencement of any informant.

3.6 A handler is responsible for working with the informant on behalf of the Council and will monitor the ongoing welfare and safety of the informant. A handler is also responsible for the conduct of the informant.

3.7 Juvenile informants (under 16 years) can only be used where an appropriate adult is present, use of juvenile informants is subject to additional protections under the Regulation of Investigatory Powers (Juveniles) Order 2000. Juvenile informants cannot be engaged to source information from anyone with parental responsibility for them.

3.8 The use of juvenile informants is can only be issued by the Chief Executive of Durham County Council.

3.9 Judicial approval of all use of informants must be sought and their use must be necessary and proportionate.

3.10 CHIS authorisations are effective for twelve months following judicial approval, juvenile authorisations are only effective for one month. The Authorising Officer will continually monitor all authorisations to safeguard all informants.

3.11 Records of authorisations will be retained in line with the non-statutory code of practice but also with respect to the Council's obligations under The Data Protection Act 2018. Records will be held to protect the Council from civil claims made under the Human Rights Act 1998, therefore it will be policy to retain these records for six years. All authorisation records are subject to strict control which is set out in 'The Durham County Council RIPA Guidance' document.

3.12 An authorisation may be renewed following review by the Authorising Officer, if the Officer can be satisfied the original criteria can continue to be met, a renewal may be authorised. All renewals must be approved by a Justice of the Peace before it can take place.

3.13 During the period of authorisation regular reviews will be conducted to ensure the validity of the activity and to assess the ongoing welfare of the informant. Any changes will require the Council to undertake further risk assessments.

3.14 Reviews should take place at a maximum of three-month intervals, the Authorising Officer should implement a system to identify review dates.

3.15 Authorisations must be cancelled where the use or conduct of the 'CHIS' fails to meet the original criteria or, where procedures for managing the source are no longer in place.

3.16 Where evidence has been obtained, the authorisation must be cancelled rather than allowed to expire, the reason for cancellation must be documented.

3.17 Cancellations must follow the strict policy which is documented within the Council's internal 'The Durham County Council's RIPA Guidance' document. This policy meets statutory criteria and up to date code of conduct guidance. Cancellations must be in writing by paper copy or email to the Senior Responsible Officer and/or RIPA Monitoring Officer within 24 hours of cancellation. Cancellations cannot be backdated.

4. Communications Data

4.1. Before the Council take part in the surveillance of communications data, the Council must follow procedure outlined under the Investigatory Powers Act 2016 and follow the established code of practice.

4.2. Communications data is placed into two categories, entity and event.

4.3. Entity data relates to information about a person or thing, and links to a telecommunications service. An example of such data is the connections made through mobile devices, such as connection to services, subscription services and information about the devices used. This is not an exhaustive list

4.4. A Communications Data authorisation protects password data, the Council can only receive access to such information by compiling with section 6 of the RIPA legislation which states the Council must have appropriate lawful authority.

4.5. Events data encompasses time-bound events which take place access a telecommunications system. An example of such data is, information which identifies a person, call logs, internet connect records. This is not an exhaustive list.

4.6. Applications to obtain communications data are obtained through the National Anti-Fraud Network (NAFN) and follow the procedure rules under the Investigatory Powers Act 2016. All authorisations are subject to oversight by a NAFN Single Point of Contact. Additionally independent authorisation by the Office for Communications Data Authorisations (OCDA) must be sought.

4.7. The Council's policy must ensure the Senior Responsible Officer (SRO) is aware of all applications for communications data being made and before such applications are reported to the OCDA.

5. Social Media

5.1. Where officers are using social media in an investigation they must follow (along with the legislation and relevant code of practices), the full RIPA guidance (available to all staff) and follow all of the Council's policies and procedures regarding social media.

5.3. Following on from the obligations the Council has under the Human Rights Act, people have a reasonable expectation of privacy, that also applies to information they post/make available via social media. The Council therefore applies strict policies to ensure that balance is struck.

5.4. For ease we have created a guide to demonstrate where an authorisation would need to be struck and what steps the Council would need to follow for surveillance and information to be captured. These have been broken down into 5 'levels' of engagement.

- General internet searches: no authorisation needed.
- 'Drive-by' visits to social media profiles: Access authorisation needed;
- Monitoring visits for 'non-serious criminal offence' purposes: Directed Surveillance authorisation needed;
- Monitoring visits relating to more serious offences: RIPA (Directed Surveillance) authorisation needed
- Befriending people for covert purposes: RIPA CHIS authorisation needed.

5.5. Preliminary searches of social media to assess a person's presence on social media is unlikely to require an authorisation.

5.6. Council officers must not use their own social media accounts to investigate social media profiles. Each service of the Council who use social media for RIPA will have their own social media accounts for this purpose. This can include the use of 'open' or 'fake' accounts and approval from an authorising officer must be sought before any officer can use a fake account.

5.7. The Council's use of social media for surveillance purposes will follow the guidance in section 26 of the Regulation of Investigatory Powers Act 2000.

6. RIPA Officers

Senior Responsible Officer

Head of Legal and Democratic Services

RIPA Monitoring Officer

Senior Lawyer Corporate and Commercial Governance

Authorising Officers for the Purposes of Directed Surveillance and CHIS

Chief Executive

Chief Internal Auditor and Corporate Fraud Manager

Public Protection Manager

Neighbourhood Protection Manager

Authorising Officers for the Purposes of Communications Data

Chief Internal Auditor and Corporate Fraud Manager

Fraud Manager, Resources

Public Protection Manager