Copeland borough council

Proud of our past. Energised for our future.

POLICY AND PROCEDURES DOCUMENT

ON

THE REGULATION OF INVESTIGATORY POWERS (RIPA) ACT 2000

Version: Final 1.4
Policy Date: January 2022

Document Control

Organisation	Copeland Borough Council
Title	RIPA Policy
Version	Final 1.4
Author	Head of Corporate Governance and Legal, Monitoring Officer
Filename	
Owner	Deputy Chief Executive
Subject	Guidance & procedures on RIPA
Protective Marking	None
Review Due Date	January 2023

Note: This document is uncontrolled if printed or reproduced

Revision History

Version Reviewed	Date Reviewed	Reviewed By	Description of Revision
V1.0 (2012)	August 2019	Information Governance Officer (Former CBC Officer)	In accordance with IPCO recommendations
V1.1 & V1.2	January 2022	Head of Corporate Governance and Legal Monitoring Officer	In accordance with statutory requirements
V1.3	May 2022	Head of Corporate Governance and Legal Monitoring Officer	In accordance with recommendation of the Inspector

Document Approval

Version	Approved By	Date
	Human Resources	
	Corporate Leadership Team	
	Trade Union Consultation	
	Executive	21st February 2022
	Full Council	

Document Distribution

This policy is to be available to all staff and elected members of Copeland Borough Council and placed on the Council's Intranet Site.

Contents Page

Introduction

1.1 The Regulation of Investigatory Powers Act 2000 ('RIPA') and regulations, orders and codes of practice made under RIPA create a framework for the regulation of covert investigations by a number of bodies, including local authorities. It was introduced to ensure that individuals' rights are protected while also ensuring that the UK's law enforcement and security agencies have the powers they need to do their job effectively.

1.2 An individual's rights relate to privacy and are contained in human rights legislation, both European and national. They introduce a remedy for persons claiming that their privacy has been breached. It is not an absolute right however. The right will not apply if the interference with a person's privacy is in accordance with the law, necessary and proportionate. This exception to the right has been incorporated into English law by the enactment of part II of RIPA.

1.3 The Council intends to use RIPA sparingly and only in extreme cases. It believes in overt investigatory operations and keeping interferences with a person's privacy to an absolute minimum. This is reflected in the low number of authorisations granted over recent years.

1.4 If an investigation is carried out in accordance with RIPA procedures, then any possible resultant breach of a person's privacy rights would not be actionable as a civil claim. In addition, in criminal proceedings arising from the investigation, the evidence gathered will not be challengeable under Section 78 of the Police and Criminal Evidence Act 1984, on the ground that it is a breach of privacy rights. The protection afforded by RIPA also extends to complaints made to the Investigatory Powers Tribunal and to the local government ombudsman. Strict adherence to the requirements of RIPA therefore provides a defence to any civil proceedings and claims for damages for breach of privacy.

1.5 It is therefore crucial that all investigating officers adhere to the requirements of RIPA.

1.6 The Investigatory Powers Act 2016, (IPA) is now the main legislation governing communications data. Part 3 of IPA replaced Part 1, Chapter 2 of RIPA in relation to the acquisition of communications data and puts local authorities on the same standing as the police and law enforcement agencies. Local Authorities have powers under both the IPA 2016 and RIPA.

1.7 Previously local authorities have been limited to obtaining subscriber details, (known now as 'entity' data,) such as the registered user of a telephone number or email address. Under IPA, local authorities can now also obtain details of in and out call data and cell site location. This additional data is defined as 'events' data.

1.8 A new threshold for communications data, 'events' data has been introduced under IPA as "applicable crime". Defined in section 86(2) of the IPA Act this means:

- an offence for which an adult is capable of being sentenced to one year or more in prison;
- any offence involving violence, resulting in substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal;
- any offence committed by a body corporate;
- any offence which involves the sending of a communication or a breach of privacy;
- or an offence which involves, as an integral part of it, the sending of a communication or a breach of a person's privacy.

1.9 The IPA has also removed the necessity for local authorities to seek the endorsement of a Justice of the Peace when seeking to acquire communications data. All such applications will now be considered for approval by the Independent Office of Communication Data Authorisation (OCDA).

1.10 The purpose of this guidance is to:

(a) explain the scope of the relevant parts of RIPA and the circumstances where it applies;

(b) provide guidance and give advice to those services undertaking covert surveillance and on the authorisation procedures to be followed in respect of authorisations, renewals and cancellations; and

(c) ensure full compliance with RIPA and a Council-wide consistent approach to its interpretation and application..

1.11 The Council has had regard to the Investigatory Powers Commissioners Office Code of Practice on Covert Surveillance and Property Interference (2018). This code of practice provides guidance on the authorisation of the use or conduct of covert human intelligence sources ("CHIS") by public authorities under Part II of the Regulation of Investigatory Powers Act 2000 ("the 2000 Act"). The code also provides guidance on the handling of any information obtained by use or conduct of a CHIS.

1.12 This code is issued pursuant to Section 71 of the 2000 Act, which provides that the Secretary of State shall issue one or more codes of practice in relation to the powers and duties in Part 2 of the 2000 Act. This code replaces the previous Covert Human Intelligence Sources Code of Practice (dated December 2014). This version of the code reflects changes to the oversight of investigatory powers made under the Investigatory Powers Act 2016 ("the 2016 Act"), including oversight by the Investigatory Powers Commissioner ("the Commissioner").

The Council also must have regard to the Code of Practice on Covert Human Intelligence Sources (2018.)

In the electronic form of this document, the Codes are available via these links and are attached at Appendix A and B:

CHIS Code (publishing.service.gov.uk)

CHIS Code (publishing.service.gov.uk)

Communications_Data_Code_of_Practice.pdf (publishing.service.gov.uk)

All related forms are accessible via the following IPCO link:
RIPA forms - GOV.UK (www.gov.uk)

1.13 In summary RIPA requires that when the Council undertakes directed surveillance or uses a Covert Human Intelligence Source (CHIS) these activities must only be authorised by an officer with delegated powers when the relevant criteria are satisfied.

1.14 Surveillance operations authorisations can be made by a Director, Head of Service or Service Manager or equivalent as permitted by the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (S.I. 2010 No. 521). That Order restricts the power to grant authorisations for the

purpose of preventing or detecting crime or of preventing disorder. However only those officers who are trained can authorise surveillance and guidance, particularly that of the Surveillance Commissioner. It is recommended that only the Chief Executive and a small number of officers be allowed to authorise surveillance. Only the following persons are therefore authorised to grant authorisations:

Chief Executive, Deputy Chief Executive, Monitoring Officer, Solicitor

1.15 The Senior Responsible Officer (SRO) for RIPA purposes is the Council's Monitoring Officer.

1.16 Enhanced authorisation provisions are set out in Annex A of the Code of Practice on Covert Human Intelligence Sources 2018, when knowledge of privileged or confidential information may be acquired or when a vulnerable individual or juvenile is to be used as a source. District Councils are listed in Annex A and only the Head of Paid Service can be authorised in this regard. (The Council's Chief Executive)

1.17 From November 2012 two important changes were made to RIPA authorisations:

(a) the person authorising directed surveillance for the purpose of preventing or detecting crime or of preventing disorder can only do so if two conditions are met. The first is that the conduct being prevented or detected constitutes one or more criminal offences or corresponds to conduct which would constitute one or more criminal offences.
The second condition is that the criminal offence is punishable by a maximum term of at least 6 months imprisonment or is an offence under section 146 (sale of alcohol to children), section 147 (allowing the sale of alcohol to children) or section 147A (persistently selling alcohol to children) of the Licensing Act 2003 or is an offence under section 7 of the Children and Young Persons Act 1933 (sale of tobacco, etc., to persons under the age of 18). This is an important change as it means that authorisations cannot be granted for minor offences particularly those where fixed penalty notices could be issued. This change is made by the Regulation of Investigatory Powers (Directed surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 (S.I. 2012 No. 1500). This is considered further in paragraph 2.6; and

(b) whilst an officer listed above can grant an authorisation section 38 of the Protection of Freedoms Act 2012 introduces a new section 32A and 32B to RIPA. These new sections require authorisations for directed surveillance under section 28 of RIPA and authorisations for covert human intelligence sources under section 29 of RIPA to be approved by the 'relevant judicial authority' before the authorisation can take effect. The judicial authority is a justice of the peace.

1.18 It should be noted that the Council cannot authorise "intrusive surveillance". Such surveillance is, by section 26(3) of RIPA, covert surveillance carried out in relation to anything taking place on any residential premises or in any private vehicles and involves the present of an individual on the premises or in the vehicles or is carried out by means of a surveillance device. If the device is designed or has the main purpose of providing information about the location of the vehicle then this will not be intrusive.

1.19 No Council Officer can authorise interference or interception with any communication in the course of its transmission by the public postal service or public telecommunications system.

1.20 The SRO will maintain centralised records of all authorisations for covert surveillance or CHIS and monitor them to ensure uniformity of practice. The central records shall

contain information regarding reviews, renewals and cancellations. Original authorisations is for each service unit to retain its authorisations on a centralised file, and for a copy to be put on the individual case file.

2. Covert Surveillance

2.1 *Introduction*

RIPA provides for the authorisation of covert surveillance by public authorities, where the surveillance is likely to result in the obtaining of private information about a person. It does so by establishing a procedure for authorising covert surveillance. It prescribes the office, rank and position of those permitted to authorise covert surveillance. From 1st November 2012 the authorisation process was made subject to judicial approval and any authorisation granted by a local authority will not take effect unless it is approved by the Magistrates' Court.

2.2 *Meaning of 'surveillance'*

Surveillance includes:-

(a) monitoring, observing or listening to persons their movements, their conversations or any of their activities or communications;
(b) recording anything monitored, observed or listened to in the course of surveillance: and
(c) surveillance by or with the assistance of any surveillance device.

2.3 *Meaning of 'covert surveillance'*

Covert Surveillance is any surveillance which is carried out in a manner calculated to ensure that the subject is unaware it is, or may be taking place. The provisions of RIPA authorise the following forms of covert surveillance:

(a) directed surveillance;
(b) intrusive surveillance; and
(c) the conduct and use of covert human intelligence sources ('CHIS').

2.4 *Meaning of 'intrusive surveillance'*

Note that RIPA does not enable a local authority to make any authorisations to carry out intrusive surveillance.

Intrusive Surveillance is surveillance which is covert surveillance that:

(a) is carried out in relation to anything taking place in any residential premises or 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.

Residential premises include a rental flat occupied for residential purposes, a police cell and a hotel bedroom.

Examples of places which may **not** be regarded as residential premises are a communal stairway in a block of flats or the front garden of premises readily visible to the public.

There are a number of exceptions applicable to the use of certain monitoring equipment some of which are not considered to constitute the use of intrusive surveillance. It is important to note that not all surveillance of a suspect's home or vehicle is likely to amount to intrusive surveillance. For example, if an Investigating Officer observes a suspect leaving his home from the street using binoculars, this is unlikely to be intrusive, unless the quality of the image obtained is of the same quality as might be expected to be obtained from a device actually present on the premises. But the intrusiveness of the surveillance proposed must be considered before any surveillance operation takes place.

For the avoidance of doubt, surveillance that enables an Investigating Officer to view or monitor anything going on inside a dwelling is almost certainly going to be regarded as intrusive and conduct of that nature cannot be authorised by a local authority.

2.5 *Meaning of 'directed surveillance'*

Local authorities are permitted under RIPA to authorise directed covert surveillance on the grounds that such surveillance is necessary for the prevention or detection of crime . Surveillance is directed if it is covert but not intrusive and is undertaken:

(a) for the purpose of a specific investigation or a specific operation;
(b) in such a manner as is likely to result in the obtaining of private information (see 2.7 below) about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
(c) otherwise and 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 RIPA to be sought for the carrying out of the surveillance.

2.6 *Limitation on the Use of Directed Covert Surveillance*

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 (SI 2012/1500) (2012 Order) came into force on 1 November 2012. It restricts Authorising Officers in a local authority in England or Wales, from authorising the carrying out of directed surveillance unless it is for the purpose of preventing or detecting a criminal offence and meets the following conditions:

(a) That the criminal offence to be prevented or detected is punishable by a maximum term of at least six months' imprisonment or
(b) Constitutes an offence under sections 146, 147 or 147A of Licensing Act 2003 (sale of alcohol to children) or section 7 of the Children and Young Persons Act 1933 (sale of tobacco to children under 18 years old).

It is therefore essential that Investigating officers consider the penalty attached to the criminal offence which they are investigating, before considering whether it may be possible to obtain an authorisation for directed surveillance.

2.7 *Meaning of 'private information'*

Information is considered to be private information if it includes any information relating to the subject's private or family life or the private or family life of any other person. It would include any aspect of a person's private or personal relationship with others, including family and professional or business relationships. Private information may include personal data for example names, telephone numbers and address details.

Private information may be acquired through covert surveillance even where a person is in a public place and may have a reduced expectation of privacy. For example, where two people hold a conversation on the street they may have a reasonable expectation of privacy over the contents of that conversation. A directed surveillance authorisation may therefore be required if a public authority records or listens to the conversation as part of a specific investigation or operation.

Note also that the information relating to the private life of an individual may be obtained when a number of records are analysed together, or where a number of pieces of information are obtained, covertly, for the purpose of making a record about a person or for data processing to generate further information. The totality of the information may constitute private information even if the individual records do not.

For example, enforcement officers may photograph the exterior of business premises for record purposes without the need for a RIPA authorisation. If, however the officers wished to establish a pattern of occupancy of those premises by any person and took photographs on a number of occasions, that conduct would be likely to result in the obtaining of private information and a RIPA authorisation would be needed.

2.8 *Tracking devices*

The use of a surveillance device designed or adapted for the purpose of providing information regarding the location of a vehicle does not necessarily constitute directed surveillance as it may not provide private information about any individual, but simply information about the location of the device at any one time. However, using that information coupled with other surveillance activity which may obtain private information, may amount to directed surveillance and an authorisation may be required.

2.9 *Exceptions where a RIPA Authorisation is not required*

Some surveillance activity does not constitute directed surveillance for the purposes of RIPA and no authorisation can be provided for such activity. These activities include:

(a) covert surveillance by way of an immediate response to events;
(b) covert surveillance as part of general observation activities -for example, if enforcement officers attend a market where it is suspected that counterfeit goods are being sold, but they are not carrying out surveillance of any particular individual and their intention is to identify and tackle offenders, then this forms part of the general duties of the public authority and the obtaining of private information is unlikely. In such a case a directed surveillance authorisation need not be sought;
(c) covert surveillance not relating to the prevention or detection of crime or the prevention of disorder; and
(d) overt surveillance by CCTV and automatic number plate recognition (APNR) systems.

2.10 *CCTV and ANPR Systems*

Where overt surveillance equipment is used for example in town centres, members of the public will be aware of the use and no RIPA authorisation is required. The use of an ANPR system to monitor traffic flows or to detect traffic offences would not require a RIPA authorisation.

If, however, CCTV cameras or an ANPR system are used in a covert, pre-planned manner as part of a specific investigation or operation for the surveillance of a particular individual, then an authorisation for directed surveillance may be required. Such surveillance is likely to result in the obtaining of private information about a person, that is, a record of his movements and activities.

Section 33 of the Protection of Freedoms Act 2012 requires all local authorities to pay due regard to the Surveillance Camera Code of Practice (SCCoP) where they operate surveillance cameras overtly in public places. All surveillance camera systems will be processing personal data so must comply with both the Data Protection Act 2018 and the requirements under General Data Protection Regulation (GDPR). The Council's Surveillance Equipment Policy sets out how the Council will manage and operate surveillance equipment under the Council's control.

2.11 *Use of Noise Monitoring Equipment*

Where possible the use of noise monitoring equipment should be notified to the owner and occupier of the offending premises. Where this is not possible, covert monitoring may be considered a reasonable and proportionate approach. If it is decided to seek an authorisation, then the Authorising Officer should consider whether the surveillance equipment is capable of measuring volume only, or whether it can identify individuals, being mindful that the more sensitive the equipment, the greater the risk that the surveillance will be Intrusive Surveillance.

If the noise monitoring equipment is calibrated only to detect excessive noise levels it may be considered that no private information is likely to be obtained and it may be that in such circumstances, an authorisation is not necessary.

2.12 *An Example of the Use of Directed Surveillance*

This type of surveillance may be used to gather evidence for an offence such as a fraudulent claim for housing benefit. An Investigating Officer may need to carry out surveillance of a suspect's home to obtain information about their contacts and work patterns. This would be directed surveillance as it would result in obtaining private information. A RIPA authorisation should be obtained. The Investigating Officer would need to demonstrate that such surveillance was necessary and proportionate. The Authorising Officer must be satisfied that the action proposed would not amount to intrusive surveillance and place conditions on the conduct to avoid this happening prior to authorising the application or decline to authorise as necessary.

Note that if the surveillance involves the use of a surveillance device, that provides detail of the same quality as may be expected to be obtained by a device located on the premises, this may amount to intrusive surveillance. No RIPA authorisation may be given for intrusive surveillance.

2.13 ***Grounds for Making an Authorisation under RIPA***

The grounds on which a local authority may make an authorisation permitting the use of directed surveillance under RIPA **are limited to the prevention or detection of crime or the prevention of disorder.** If directed surveillance is carried out for any other purpose, then an authorisation under RIPA cannot be granted.

2.14 ***Core Functions***

A local authority may only make authorisations under RIPA when performing its core functions. Those are the specific public functions undertaken by the local authority as opposed to its ordinary functions which are undertaken by all public authorities.

For example, an authorisation under RIPA cannot be used when the principal purpose of an investigation is for taking disciplinary action against an employee, as the disciplining of an employee is not a core function. It may, however, be appropriate to seek an authorisation under RIPA if there are associated criminal investigations.

2.15 ***Further Guidance on Covert Surveillance***

Further guidance on the use of covert surveillance may be found in the Home Office Code of Practice for Covert Surveillance and Property Interference at the link shown in paragraph 1.12 above.

3. The Conduct of Covert Human Intelligence Sources

3.1 ***Grounds for granting authorisation***

A local authority may grant an authorisation under RIPA for the use of a Covert Human Intelligence Source (CHIS). The conduct that may be authorised is any conduct that:

(a) is comprised in any such activity including the conduct of CHIS or use of CHIS, as are specified in the authorisation;

(b) consists in conduct by or in relation to a person who is so specified or described as a person as to whose actions as a CHIS the authorisation relates;

(c) is carried out for the purposes of or in connection with the investigation or operation so specified or described;

(d) is necessary and proportionate to the intelligence dividend that it seeks to achieve;

(e) is necessary for the purpose of the prevention or detection of crime or the prevention of disorder.

3.2. ***Meaning of 'CHIS'***

A person is considered to be a CHIS if:

(a) s/he establishes or maintains a personal or other relationship with a person for the covert purpose of doing anything falling within paragraphs (b) or (c) below;

(b) s/he covertly uses such a relationship to obtain information or provide access to any information to another person;

(c) s/he covertly discloses information obtained by the use of the said relationship, or as a consequence of the existence of such a relationship.

3.3 ***Meaning of 'relationship'***

Authorisations for the use of a CHIS do not relate solely to the obtaining of private information. An authorisation is necessary where there is covert manipulation of a relationship to gain any information. Article 8 of ECHR includes the right to establish and develop a relationship so such a right may be infringed where a public authority manipulates that relationship to obtain information.

To establish a relationship simply means to "set up" a relationship and does not require endurance of a relationship over a period of time. The use of a CHIS is most likely to arise when individuals are used to make test purchases. Whether a relationship exists between the buyer and seller depends upon the circumstances, but a repetition of purchases is not always necessary to give rise to a relationship.

3.4 ***Examples where the use of a CHIS may arise***

(a) Test purchases – this kind of investigation is commonly undertaken by

County Council Trading Standards Officers when carrying out test purchases in off licences. Enforcement Officers of this Council may be drawn into such operations as the Council is licensing authority under the Licensing Act 2003. Council officers should not take part in the investigation relating to test purchases. If offences do arise using evidence from test purchase the correct course of action should then be for Trading Standards to commence a review of the off licence's premises licence. If the Enforcement Officer, as part of that joint investigation, observes Licensing Act offences being committed these are likely to fall as part of his general duties and not constitute covert surveillance.

Test purchases can arise however in respect of taxi fares where a CHIS may be used to hire a taxi to determine if the correct fare is being charged. Such an offence however is unlikely to be one which carries a sentence of imprisonment not less than six months unless there is a pattern of deliberate dishonesty or theft involved.

(b) Public Volunteers - not every human intelligence source will be a CHIS. Where a person volunteers information to the local authority without being induced, asked or tasked by the local authority, no authorisation under RIPA is required**.** For example, if a person provides a piece of information about something he has witnessed in his neighbourhood, he would not be regarded as a CHIS as the information he is passing is not as a result of a relationship which has been established or maintained for a covert purpose.

However care needs to be taken with such volunteers. There is a risk that an informant may in reality be a CHIS even if he is not tasked to obtain the information covertly. It is possible that a person could become engaged in the conduct of a CHIS without a public authority inducing, asking or assisting the person to engage in that conduct. Where an informant gives repeat information about a suspect or about a family and it becomes apparent that the informant may be obtaining that information in the course of a family or neighbourhood

relationship then this is likely to mean that the informant is in reality a CHIS to whom a duty of care is owed if the information is then used. Where information is volunteered, more than once, legal advice should be sought before using the information provided by the informant. Paragraphs 2.20 to 2.22 of the Code relating to CHIS provides further information.

For a further example, if a member of the public is asked by an Investigating Officer to maintain a record of vehicles arriving at and leaving a specific location, no relationship has been established or maintained in order to gather that information. A CHIS authorisation is therefore not required. Note there may, in such circumstances, be the need to obtain a RIPA authorisation for directed surveillance.
In contrast, if an Investigating Officer wishes to use a neighbour to question an individual about the activities carried on at a site which for example, was subject to enforcement action under the Planning Acts, this may amount to the use of a covert human intelligence source.

(c) Professional or Statutory Duty - any regulatory or professional disclosure made by an individual should not result in that individual falling within the definition of a CHIS, as the information disclosed is derived from a business relationship which will not have been established for the covert purpose of disclosing such information. In addition, such disclosure is undertaken as a statutory requirement and is unlikely to infringe an individual's privacy.

3.5 Further Guidance on the Use of a CHIS

Further guidance on the use of a CHIS may be found in the IPCO Covert Human Intelligence Sources Code of Practice which can be found at the link shown in paragraph 1.12 above.

4. The Procedure for Obtaining Authorisations (Directed Surveillance and CHIS)

4.1 *Introduction*

Each form of covert surveillance which is subject to the provisions of RIPA must be authorised in accordance with the provisions of RIPA.

4.2 *Authorising officers*

Regulations prescribe that within a local authority, Authorising Officers must hold the rank of Director, Head of Service, Service Manager or equivalent. The Council's Scheme of Delegation delegates the Director of Services, all Heads of Service and all Service Managers as Authorising Officers.

No person designated as an Authorising Officer should act as an Authorising Officer unless s/he has undertaken appropriate training within 3 years prior to the date of making an authorisation.

4.3 *Making an application for an authorisation*

4.3.1 The whole of this section applies to directed surveillance and the use of a CHIS. When completing an application for directed surveillance or use of a CHIS, and when

completing review, renewal and cancellation forms, regard should be had to this Policy and Procedure.

4.3.2 The Investigating Officer must complete all of the information required by the appropriate prescribed form. There are different forms for authorising directed surveillance and for authorising the use of CHIS.

Electronically, the forms may be found on the Home Office web site at:

Surveillance and counter-terrorism - GOV.UK (www.gov.uk)

4.3.3 The activities to be authorised must be necessary for the purpose of preventing or detecting crime or of preventing disorder. If they are necessary they must be proportionate to what is sought to be achieved by carrying them out. Both the investigating officer and the authorised officer must balance the seriousness of the intrusion into a person's privacy against the need of undertaking the activity in investigative and operational terms.

The Code of Practice on covert Surveillance and Property Interference provide useful information and examples on the necessary and proportionality test.

> *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 intrusive actions proportionate. Similarly an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by less intrusive means.*
>
> *The following elements of proportionality should therefore 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."*

4.3.4 Authorisations or renewals of authorisations must be given by the Authorising Officer in writing except in urgent cases when it can be done orally. The Authorising Officer should forward a scanned copy of the hand signed authorisation by email immediately to the Senior Responsible Officer (or, in their absence, the Solicitor). The Senior Responsible Officer (or Solicitor as appropriate) will inform the Authorising Officer of the unique reference number (URN) that has been allocated to that authorisation. The URN must be included on all future review, renewal or cancellation forms in relation to that authorisation.

4.3.5 Before giving authorisation for surveillance or the use of a CHIS the Authorising Officer must be satisfied that:

(a) it is necessary for the purpose of preventing or detecting crime or of preventing disorder. The written authorisation should specify the objectives of the activity in factual terms, for example, to gather evidence. The type of crime must also be specified and what facts led the Authorising Officer to believe that the activity will achieve its objectives;

(b) it is proportionate to the seriousness of the crime or the matter being investigated and the history and character of the subject concerned.

(c) the Investigating Officer has completed all relevant sections of the appropriate authorisation form. S/He must also be satisfied that all of the matters detailed in the paragraph headed "Making an Application", above, have been properly considered and set out in sufficient detail on the form.

(d) that the surveillance proposed may infringe the human rights of its subject or of others. S/He must also be satisfied that the covert surveillance for which the authorisation is sought is proportionate i.e. that the information could not be obtained by any other means and that it is necessary to further the objectives of the investigation. S/He should consider whether the benefits of obtaining the information are significant rather than marginal. S/He must also consider the risk of collateral intrusion into the privacy of other persons.

(e) In addition when an authorisation is sought for use of CHIS, the Authorising Officer must be satisfied that:

(1) there is a person within the investigating team who will have day to day responsibility for dealing with the source on behalf of the authority and that he will ensure the sources security and welfare;

(2) there will at all times be another person within the investigating team who will have general oversight of the use made of the source;

(3) there will be a person within the investigating team who will have responsibility for maintaining a record of the use made of the source;

(4) the records relating to the source contain all matters as may be specified in regulations;

(5) records maintained that disclose the identity of the source will not be available to persons except to the extent that there is a need for them to be made available; and

(6) that the form specifies the person to whose actions as a CHIS the authorisation relates, describes the purposes of the investigation or operation and any limit on the conduct authorised.

If the Authorising Officer is not completely satisfied that the application has been properly completed, s/he should liaise with the Investigating Officer to obtain further information.

4.3.6 In considering whether to grant an authorisation the Authorising Officer must demonstrate how s/he has reached the conclusion that the activity is proportionate to what it seeks to achieve. There are four elements of proportionality to consider:

(a) balancing the size and scope of the operation against the gravity and extent of the perceived crime or offence;

(b) explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others;

(c) that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result; and

(d) evidencing, as far as reasonably practicable, what other methods have been considered and why they were not implemented.

4.3.7 In granting an authorisation the Authorising Officer should clearly set out what activity and surveillance equipment is authorised so that the investigating Officer is certain what has been sanctioned.

4.4 ***Specific matters relating to CHIS***

In respect of Covert Human Intelligence Sources in addition to the above it is necessary under S29(5) RIPA that there are in force such arrangements as are necessary for ensuring:

(a) that there will at all times be a person holding an office, rank or position with the relevant investigatory authority who will have day to day responsibility for dealing with the CHIS on behalf of that authority and for the CHIS's security and welfare;

(b) that there will at all times be another person holding an office, rank or position with the relevant investigating authority who will have general oversight of the use made of the CHIS;

(c) that there will at all times be a person holding an office, rank or position with the relevant investigating authority who will have responsibility for maintaining a record of the use made of the CHIS;

(d) that the records relating to the CHIS that are maintained by the relevant investigating authority will always contain particulars of all such matters (if any) as may be specified for the purposes of this paragraph in regulations made by the Secretary of State; and

(e) that the records maintained by the relevant investigating authority that disclose the identity of the CHIS will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.

In other words there must be an officer given direct day to day management of the CHIS to look after his/her needs and another officer in overall control of the use of the CHIS. A record must be made by a specified person of the use of the CHIS. Regulations have been made giving details of the type of particulars needed to be recorded. (See 12 below for details). The identity of CHIS's is not to be disclosed unless there is a need to do so. NB - There is no need for 3 different officers. The person responsible for maintaining a record should be an authorising officer.

(f) Records relating to the CHIS must contain the following by reason of the Regulation of Investigatory Powers (Source Records) Regulations 2000:-

(i) the identity of the CHIS;
(ii) the identity, where known, used by the CHIS (i.e. his or her 'alias');
(iii) any relevant investigating authority other than the authority maintaining the records;
(iv) the means by which the CHIS is referred to within each relevant investigating authority (i.e. his or her 'code name');
(v) any other significant information connected with the security and welfare of the CHIS;
(vi) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a CHIS that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the CHIS(s) have where appropriate been properly explained to and understood by the CHIS(s);
(vii) the date when, and the circumstances in which, the CHIS was recruited; (or if already employed by WBC and allocated this task);
(viii) the identities of the authorising officer and the applicant;
(ix) the periods during which those persons have discharged those responsibilities;
(x) the tasks given to the CHIS and the demands made of him or her in relation to their activities as a CHIS;
(xi) all contacts or communications between the CHIS and a person acting on behalf of any relevant investigating authority;
(xii) the information obtained by each relevant investigating authority by the conduct and use of the CHIS;
(xiii) any dissemination by that authority of information obtained in that way; and
(xiv) in the case of a CHIS who is not an under-cover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the CHIS activities for the benefit of that or any other investigating authority.

Therefore, the officer in charge of maintaining a record of the use of each CHIS should record all these details. The way these records are kept is designed to try to keep the CHIS safe from discovery by the subjects and safe from any harm which could result from their disclosure

and also to keep in the open any money or other benefits paid to a CHIS who is not an employee officer of an authorising body.

Additional requirements for Authorising the use of Juveniles as CHIS:

The use of juveniles as CHIS is regulated by the Regulation of Investigatory Powers Act (Juveniles) Order 2000. These regulations provide that when seeking an authorisation the Investigating Officer must:

(a) make a risk assessment to demonstrate that the physical and physiological risks have been identified and evaluated and explained to CHIS, and

(b) that an appropriate adult will be present at meetings of any CHIS under 18.

There is a prohibition on a CHIS under the age of 16 being used if a person under surveillance is a parent or has financial responsibility for that CHIS.

4.5 *Obtaining Judicial Approval of Authorisations*

4.5.1 Authorising Officers must when making authorisations be aware that each authorisation (or renewal of an authorisation) will be subject to judicial approval. The Protection of Freedoms Act 2012, amends RIPA, to require that where a Authorising Officer has granted an authorisation for the use of directed surveillance or for the use of covert human intelligence sources, judicial approval will be required.

4.5.2 The Authority will be required to make an application, without giving notice, to the Magistrates' Court. The Magistrates will give approval if at the date of the grant of authorisation or renewal of an existing authorisation if and only if, they are satisfied that:

(a) there were reasonable grounds for believing that obtaining the covert surveillance or use of a human covert intelligence source was reasonable and proportionate and that these grounds still remain;

(b) the "relevant conditions" were satisfied in relation to the authorisation. Relevant conditions include that:

(i) the relevant person was designated as an Authorising Officer;

(ii) it was reasonable and proportionate to believe that using covert surveillance or a covert human intelligence source was necessary and that the relevant conditions have been complied with;

(iii) the grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under section 25(3) of RIPA; and

(iv) any other conditions provided for by an order made by the Secretary of State were satisfied.

4.5.3 If the Magistrates' Court refuses to approve the grant of the authorisation, then it may make an order to quash that authorisation.

4.5.4 No activity permitted by the authorisation granted by the Authorising Officer may be undertaken until the approval of the Magistrates' Court to that authorisation has been obtained. To ensure compliance with this requirement, any Authorising Officer who

proposes to approve an application for the use of directed surveillance or for the use of a covert human intelligence source must immediately inform the Solicitor by telephone or e-mail of the details of the authorisation. The Solicitor will then make the necessary arrangements for an application for an order to approve the authorisation to be made to the Magistrates' Court. The Authorising Officer and the Investigating Officer may be required to attend the Magistrates' Court to support the application.

4.6 *Cases where Authorisations must be obtained from Specifically Designated Officers*

4.6.1 Confidential Information

Note that where an authorisation for a CHIS is sought and it is likely through the conduct of the CHIS that confidential information would be obtained, then a higher level of authorisation is required. i.e. authorisation by the Chief Executive or by a Director of Services.

"Confidential Information" consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.

4.6.2 Legally Privileged Information

This is any communication or information passing between a subject and their legal advisors. It is considered to be particularly sensitive. It is unlikely that such information obtained from CHIS would be admissible in evidence in criminal proceedings. Action which may lead to legally privileged information being obtained by a CHIS is subject to additional safeguards. Investigating officers seeking to obtain such information must refer to the Home Office Covert Human Intelligence Sources Code of Practice.

4.6.3 Confidential Personal Information

This is information held in confidence concerning an individual who can be identified from it (whether living or dead) relating to their physical or mental health or to spiritual counselling or assistance to which a person has had recourse.

4.6.4 Confidential Journalistic Material

This is material acquired or created for the purpose of journalism or communications resulting in information being so acquired and held subject to an undertaking to hold it in confidence.

4.6.5 Use of Juveniles as CHIS

Note that an authorisation as to the use of a juvenile as a CHIS may only be made by the Chief Executive or in his absence the Director of Services.

4.7 *Duration, review, cancellation and renewal of authorisations*

4.7.1 Regular reviews of authorisations must be undertaken to assess the need for the surveillance to continue. The Authorising Officer must determine how often a review should take place. Reviews should be undertaken by an authorising officer as frequently as s/he considers necessary and practicable. Bearing in mind the intrusive nature of surveillance the presumption must be in favour of early reviews. In any event a review must take place no later than one month after the date of the authorisation/renewal or

last review. The reviews should review the continued necessity and proportionality of the authorised covert activity and a record or the review be kept. Periodic reviews are important – they keep the momentum on the investigation and should ensure that intrusions into privacy are kept to a shorter period as possible.

4.7.2 The Authorising Officer must cancel an authorisation as soon as he or she believes that the activity is no longer necessary or proportionate. Authorisations do NOT lapse automatically – they must be formally cancelled.
Once an investigation has been completed or the circumstances of the case dictate that it must be closed, the Investigating Officer must complete a cancellation of authorisation form and submit it to the Authorising Officer who granted or last renewed the authorisation. Upon cancellation all the original documentation in relation to the authorisation must be forwarded by secure means to the Senior Responsible Officer. The Authorising Officer may cancel the authorisation if he considers that the requirements of the authorisation are no longer satisfied. The Authorising Officer who granted a CHIS authorisation must cancel it if s/he is satisfied that the use of the CHIS no longer meets the criteria for authorisation.

4.7.3 A written authorisation for directed surveillance granted by an authorising officer and judicially approved will cease to have effect (unless renewed or cancelled) at the end of a period of three months beginning with the time at which it took effect. Urgent oral authorisations granted by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after 72 hours, beginning with the time when the authorisation was granted. If at any time before an authorisation for directed surveillance would cease to have effect the authorising officer considers it is necessary for the authorisation to continue for the purpose of which it was given he may renew it in writing for a further period of three months. Renewals may also be granted orally in urgent cases and last for a period of 72 hours. Both procedures are subject to the requirement for judicial approval. The Code of Practice recommends that renewal occurs shortly before the authorisation period is drawing to an end. Due to the need for judicial authorisation the renewal process should be undertaken during the last 2 weeks of the current authorisation period. Paragraph 5.12 – 5.16 of the Code relating to covert Surveillance and Property Interference provides more information on renewals.

4.7.4 With regard to an authorisation for the use of CHIS a written authorisation will, unless renewed, cease to have effect at the end of a period of 12 months beginning with the day on which it took effect, except in the case of a juvenile CHIS which lasts for one month. Urgent oral authorisations will, unless renewed, cease to have effect after 72 hours beginning with the time when the authorisation was granted. A renewal can be granted for a further same period and the same procedure as outlined in 4.9.3 applies. When considering an application for renewal of an authorisation for a CHIS the Authorising Officer must consider:

(a) the use made of the source in the period since the grant or latest renewal of the authorisation; and

(b) the task given to the source during that period and the information obtained from the conduct or use of the source. The Authorising Officer must be certain that all of the information which was presented to justify the original authorisation is still subsisting and relevant. This applies to authorisations both for directors of surveillance and for use of CHIS.

4.7.5 To assist with the proper review, renewal and cancellation of an authorisation the Investigating Officer should keep the following record and diarise the dates for renewal and cancellation:

(a) a copy of the authorisation together with supporting documents;

(b) a copy of any renewal of any authorisation together with supporting documents;

(c) any authorisation which was granted or renewed orally (an urgent case) and the reason why the case was considered to be urgent ;

(d) any risk assessment raised in relation to a CHIS ;

(e) the circumstances in which tasks were given to the CHIS;

(f) the value of the CHIS to the investigation;

(g) a record of the results of any reviews of the authorisation;

(h) the reasons for not renewing an authorisation;

(I) the reasons for cancelling an authorisation; and

(j) the date and time when any instructions were given by the authorising officer since using a CHIS.

The Investigating Officer should diarise the dates for review of each authorisation.

4.8 *Maintaining Records of Authorisations, Renewals and Cancellations*

4.8.1 The Authorising Officer must send the originals of all records of authorisations, renewals and cancellations to the Senior Responsible Officer who will keep a central record. The Unique Reference Number (URN) required on the paperwork must bear a prefix indicating which service the paperwork has originated from (e.g.EH for Environmental Health or A for audit).

4.8.2 All of the information relating to the authorisation will form part of the records of the investigation and must be kept on the appropriate file for 5 years or longer if appeals are made.

4.8.3 Information that may be of value in connection with concurrent investigations may be kept, but information not relevant to those enquiries must be destroyed.

4.8.4 The Senior Responsible Officer will provide a Unique Reference Number for each RIPA application, upon request by an Investigating Officer. S/He will maintain a central record of all RIPA authorisations, renewals and cancellations. In addition, he will review the authorisations/renewals made on a regular basis to ensure that such authorisations/renewals are made properly, are appropriate and that all forms have been fully completed. S/He will be able to provide advice on RIPA issues to Investigating and Authorising Officers.

5 General

5.1 *The Senior Responsible Officer (SRO)*

The appointed Senior Responsible Officer for RIPA within the Council's Monitoring Officer and has responsibility for the integrity of the process to authorise directed surveillance, to ensure compliance with the Act and the Codes of Practice, to engage with the Commissioners and Inspectors when they conduct inspections, to oversee the implementation of any post-inspection action plan recommended or approved by a Commissioner and to ensure all Authorising Officers are of an appropriate standard in the light of any concerns raised by an inspection.

5.2 *Investigatory Powers Commissioners Office (IPCO)*

Office of Surveillance Commissioners was replaced by Investigatory Powers Commissioner's Office.

Information must be provided on request and inspections are carried out regularly by the IPCO office.

5.3 The Investigatory Powers Tribunal

The Tribunal is a judicial body which operates independently of government to provide a right of redress for anyone who believes they have been a victim of unlawful action by a public authority using covert investigative techniques. The Investigatory Powers Act 2016 strengthened the provisions governing the Tribunal by providing a new right of appeal from decisions and determinations of the Tribunal in circumstances where there is a point of law that raises an important point of principle or practice, or where there is some other compelling reason for allowing an appeal.

As the remit of the Tribunal is to deal with covert techniques and matters of national security, complainants are not required to provide evidence to support their complaint or Human Rights Act Claim. Instead they are asked to specify what activity they know or believe has taken place. The Tribunal is under a duty both to investigate and to determine valid complaints and public authorities are under a duty to provide the Tribunal with all documents and information the Tribunal may require to assist in that investigation. Nothing can be held back from the Tribunal for reasons of secrecy or national security. To counter this, and to protect sensitive information, the Tribunal may not disclose to the complainant anything which might compromise national security or the prevention and detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of the functions of any of the intelligence services. However, wherever possible, and subject to this limitation, the Tribunal will provide findings of fact or a summary of the determination.

The Tribunal has at its disposal a range of possible remedies, as wide as those available to an ordinary court which is hearing and deciding an ordinary action for the infringement of private law rights. However, unlike Rule 10 of the Tribunal Procedure (First-Tier Tribunal) General Regulatory Chamber Rules 2009 (SI No.1976 [LINK to this SI]), there is no express power to award costs in Section 67(7) of RIPA, nor in the Rules. The Tribunal has only awarded costs on one occasion: see Chatwani & Others v the National Crime Agency in Chapter 5.

Apart from compensation, other orders that may be made by the Tribunal include -

- An order quashing or cancelling any warrant or authorisation; and

- An order requiring the destruction of any records of information which (i) have been obtained in exercise of any power conferred by a warrant or authorisation; or (ii) are held by any public authority in relation to any person.

5.4 *Officer training*

Officers will be provided with appropriate training including refreshers and updates regarding any changes in legislation, etc. Records of training will be kept by Human Resources.