LANCASTER CITY COUNCIL

Promoting City, Coast & Countryside

THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) POLICY AND PROCEDURE

Document Control

Approved by:	Audit Committee	**Date:**	28/11/2018
Document location:			
Document owner:	Information Governance		
Review period:	1 Year		
Next review date:	March 2026		

Revision History

Version	Date	Reviewed By	Amendment Details
V 1.0	28/11/2018	Audit Committee	Approval of final draft
V2.0	27/11/2019	Audit Committee	Social Media Use and guidance approved
V3.0	25/11/2020	Audit Committee	Approval of updated codes and IPCO recommendations
V3.0	23/03/2022	Audit Committee	Approved policy to remain as per last year.
V4.0	22/11/2023	Audit Committee	Update to CHIS guidance reference and forms
V5.0	03/2025	Audit Committee	Update

CONTENTS

1 Purpose

The purpose of this policy is to:

- explain the provisions of the Regulation of Investigatory Powers Act 2000 (RIPA);
- provide guidance and give advice to those Services undertaking covert surveillance; and
- ensure full compliance with RIPA and a Council-wide consistent approach to its interpretation and application.

2 Introduction

RIPA came into force on 25th September 2000 to regulate covert investigations by a number of bodies, including local authorities. It was introduced to ensure that individuals' rights are protected while also ensuring that law enforcement and security agencies have the powers they need to do their job effectively.

Lancaster City Council is therefore included within the 2000 Act framework with regard to the authorisation of both Directed Surveillance and the use of Covert Human Intelligence Sources (CHIS)

In summary RIPA requires that when a Council undertakes "directed surveillance" or uses a "covert human intelligence source" these activities must only be authorised by an officer with delegated powers when the relevant criteria are satisfied. In addition, amendments contained in the Protection of Freedoms Act 2012, which took effect on the 1st November 2012, mean that local authority authorisations, and renewals of authorisations under RIPA, can only take effect once an order approving the authorization (or renewal) has been granted by a Justice of the Peace (district judge or lay magistrate) (JP).

Authorisation for both types of surveillance may be granted only where it is believed that the authorisation is necessary, and the authorised surveillance is proportionate to that which is sought to be achieved:

An authorisation may be granted only where the Authorising Officer believes that the authorisation is necessary in the circumstances of the particular case:

"For the purpose of preventing and detecting crime and disorder"

However, amendments which took effect on the 1st November 2012 mean that a local authority may only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco. Local authorities cannot authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence punishable by a maximum term of at least 6 months' imprisonment. These amendments are referred to as "the crime threshold".

The background to RIPA is the Human Rights Act 1998, which imposes a legal duty on public authorities to act compatibly with the European Convention on Human Rights (ECHR). Article 8(1) of the ECHR gives a right to respect for private and family life, the home and correspondence. However, this is qualified by Article 8(2) which provides that there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national

security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. RIPA was enacted so as to incorporate the provisions of Article 8(2) in English law, and to establish a means by which a public authority may interfere with privacy rights in accordance with the law. The objective is to give protection to the Council and any officer involved in an investigation. The scheme of RIPA is to state that an authorisation for covert surveillance shall be lawful for all purposes, but that such an authorisation may only be granted if the authorising officer believes that what is proposed is necessary and proportionate (see paragraphs 35 and 36 below).

If the authorisation procedures introduced by RIPA are followed, they afford protection to the Council and to investigating officers in respect of challenges to the admissibility of evidence, claims under the Human Rights Act 1998, and complaints to the Local Government Ombudsman or the Investigatory Powers Tribunal.

The Act is supported by statutory Codes of Practice, the most recent versions of which were published in 2014 and are available on the Council's intranet. These are the 'Covert Surveillance and Property Interference' Code of Practice and the 'Covert Human Intelligence Sources' (CHIS) Code of Practice. RIPA requires the Council to have regard to the provisions of the Codes which are admissible as evidence in criminal and civil proceedings and must be taken into account by any court or tribunal.

3 Investigatory Powers Commissioner's Office

In May 2001 an Inspectorate was formed within the Office of Surveillance Commissioners (OSC) to keep under review the exercise and performance of the powers and duties conferred or imposed by RIPA. This Office was replaced in October 2017 and is now called the Investigatory Powers Commissioner's Office (IPCO) and is led by the Investigatory Powers Commissioner. The most recent Procedures and Guidance can be found on their website.

RIPA requires public authorities to disclose or provide to the Investigatory Powers Commissioner all such documents and information as they may require for the purpose of enabling them to carry out their functions.

4 Statement of Intent

The Council's policy and practice in respect of RIPA is to comply fully with the law and strike a fair and proportionate balance between the need to carry out covert surveillance in the public interest and the protection of an individual's fundamental right to privacy. The Council acknowledges that this policy is very much a living document and will be reviewed and updated in line with the best guidance and advice current at the time.

5 Part 1: An explanation of the Key Provisions of RIPA

5.1 What is meant by 'surveillance'?

'Surveillance' includes:

a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication;

b) recording anything monitored, observed or listened to in the course of surveillance; and

c) surveillance by or with the assistance of a surveillance device.

5.2 When is surveillance "covert"?

According to RIPA, surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place. If activities are open and not hidden from the subjects of an investigation, the 2000 Act framework does not apply.

5.3 What is 'directed surveillance' or when is surveillance 'directed'?

Surveillance is directed if it is 'covert' but not 'intrusive' (see below) and is undertaken:

a) for the purposes of a specific investigation or a specific operation;

b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not that person is specifically identified for the purposes of the investigation or operation); and

c) 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 to be sought for the carrying out of the surveillance.

Essentially, therefore, directed surveillance is any:
(1) pre-planned surveillance activity;
(2) undertaken covertly;
(3) for the purposes of a specific investigation;
(4) in such a way that is likely to result in obtaining private information about a person.

5.4 Is it for the purposes of a specific investigation or operation?

For example, are CCTV cameras which are readily visible to anyone walking around a Council car park covered?
The answer is no if their usage is to monitor the general activities of what is happening in the car park. If that usage changes at any time the 2000 Act may apply.
For example, if the CCTV cameras are targeting a particular known individual, and are being used in monitoring his activities, that has turned into a specific operation which will require authorisation.

5.5 Is it in such a manner that it is likely to result in the obtaining of private information about a person?

5.5.1 'Private Information'

In relation to a person, includes any information relating to his 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 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.

If it is likely that observations will not result in the obtaining of private information about a person, then it is outside the 2000 Act framework. However, the use of "test purchasers" may involve the use of covert human intelligence sources see ***section 10.7***

5.5.2 'Immediate response….'

According to the Covert Surveillance Code of Practice, "covert surveillance that is likely to reveal private information about a person but is carried out by way of an immediate response to events such that it is not reasonably practicable to obtain an authorisation under the 2000 Act would not require a directed surveillance authorisation." For example, a police officer would not require an authorisation to conceal himself and observe a suspicious person that he came across in the course of a patrol.

However, if as a result of an immediate response, a specific investigation subsequently takes place, that brings it within the 2000 Act framework.

5.6 What is meant by 'intrusive surveillance' or when is surveillance 'intrusive'?

Surveillance becomes intrusive if the covert surveillance:

a) is carried out in relation to anything taking place on any 'residential premises' or in any 'private vehicle'; or a "place for legal consultation; 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; or

c) 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, and 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.

The definition of surveillance as intrusive relates to the location of the surveillance, and not to other consideration of the nature of the information that is expected to be obtained. Officers of the Council are unlikely to have access to any "place of legal consultation" but should seek advice from Legal Services on the detailed definition.

5.6.1 'Residential premises'

Is defined to include any premises that is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation. For example, the definition includes hotel rooms. It, however, does not include so much of any premises as constitutes any common area to which a person is allowed access in connection with his use or occupation of any accommodation. For example, a hotel lounge.

5.6.2 'Private vehicle'

Means any vehicle which is used primarily for private purposes, for example, for family, leisure or domestic purposes. It therefore does not include taxis i.e. private hire or hackney carriage vehicles.

5.7 Why is it important to distinguish between directed and intrusive surveillance?

It is imperative that officers understand the limits of directed surveillance or, put another way, recognise when directed surveillance becomes intrusive surveillance because **RIPA does not permit local authorities to undertake intrusive surveillance in any circumstances.**

5.8 What is a 'covert human intelligence source' (CHIS)?

According to RIPA a person is a CHIS if:

a) he **establishes or maintains a personal or other relationship** with a person for the **covert purpose** of facilitating the doing of anything falling within paragraph b) or c).

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

c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A CHIS is effectively an inside informant or undercover officer, someone who develops or maintains their relationship with the surveillance target, having the covert purpose of obtaining or accessing information for the investigator.

A **purpose is covert**, in relation to the establishment or maintenance of a personal or other relationship, if and only if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

It is not clear whether **'information'** is restricted to private information in line with directed surveillance. The inference is there, but it is not clear. If in doubt, the Council's policy is to obtain an authorisation.

RIPA also makes reference to the use of a CHIS which refers to inducing, asking or assisting a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of such a CHIS.

5.9 Use of Social Networking in investigations

Officers often use the internet and social networking sites for the purposes of research and carrying out checks on the subjects of an investigation. Care must be taken to ensure that officers do not stray into a surveillance situation.

It should not be assumed that all monitoring of open social media sites is automatically immune from the need for an authorisation of some sort. Use of open media, in circumstances where there is a reasonable expectation of privacy, is likely to require an authorisation, particularly if the monitoring is intensive or for a prolonged period of time i.e. more than a week. The creation of fake or anonymous websites for investigation purposes is likely to require an authorisation. Entry on to chat rooms or closed groups for investigatory purposes is also likely to require authorisation unless the officer's identity is made clear from the outset.

Use of a 3rd party's identity requires both an authorisation and express written permission from that person. Whilst overt working in this way might avert the need for a surveillance authorisation officers should be aware that a CHIS situation could inadvertently arise.

It is expected that social media sites will generate significant amounts of sensitive information.

Sensitive material that is not relevant to an investigation should be disposed of quickly and safely. Any interaction between an investigator and the public via social media could inadvertently give rise to a CHIS situation. Investigators should generally avoid interaction

whilst monitoring social media sites and take advice should any uncertainty arise. The use of the internet and social media may require an authorisation in the following circumstances:

(a). Any communications which are made with 3rd parties for the purpose of gathering evidence or intelligence about an offence in circumstances where the third party is not aware that the officer is working for the Council.

(b) Accessing private pages of social media for the purpose of gathering evidence or intelligence about an offence or other matter subject to potential litigation.

(c). Any communications between an officer and a 3rd party for the purpose of using that person to gather evidence or intelligence about a suspect.

(d). Intensive monitoring of a suspect using social media over a sustained period of time particularly when this is used in connection with other methods of investigation.

(e). The creation of a false personae or use of a third-party identity for investigation purposes.

(f). Any direct interaction in any forum – open or closed – in which an officer seeks to elicit information, when they are not explicit about their real identity.

Repeated entry to social media sites and copying material for the purpose of an investigation is likely to engage RIPA. As a rule of thumb access to Facebook and other social media sites should be made via the Council's Facebook account as opposed to a private account. If there is any doubt the officer who is conducting this activity is advised to seek legal advice.

Please see **Appendix 2** for the process which is to be followed in relation to the use of social media.

The IPCO has issued the following guidance: -

- Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as "open source" or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases, data may be deemed private communication still in transmission (instant message for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required.

- Providing there is no warrant authorising interception in accordance with section 48 (4) of the 2000 Act, if it is necessary and proportionate for a public authority to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than the mere reading of the site's content).

- It is not unlawful for a member of a public authority to set up a false identity, but it is inadvisable for a member of a public authority to do so for a covert purpose without authorisation. Using photographs of other persons without their permission to support the false identity potentially infringes other laws.

- A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the

protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done.

6 Part 2: General Authorisation Requirements

6.1 The authorisation requirements

RIPA requires that prior authorisation is obtained by all local authorities using directed surveillance and CHIS techniques.

The authorising officer must give authorisations in writing and a separate authorisation is required for each investigation. Any authorisation must also be approved by an order from a JP. The application form for such approval is available on the Council's intranet, but advice should be sought from Legal Services on making an application for judicial approval.

Whilst according to RIPA, a single authorisation may combine two or more different authorisations (for example, directed surveillance and CHIS), the provisions applicable in the case of each of the authorisations must be considered separately. Because combining authorisations may cause confusion, officers must use separate forms for different authorisations.

The purpose of the authorisation is to comply with the Human Rights Act 1998 by providing lawful authority to carry out surveillance. This is why an authorisation must be obtained where the surveillance is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation. If the surveillance is then actually carried out in accordance with the authorisation, it will be less open to challenge.

6.2 Who can authorise the use of covert surveillance?

To give effect to RIPA, the Chief Officer Governance (Monitoring Officer) has been designated to authorise the use of directed surveillance and CHIS techniques in respect of external investigations and to sanction the use of such covert surveillance in respect of internal officer/Member investigations. This designation can be directly delegated to the Deputy Monitoring Officer Any RIPA authorisation must be approved by an order from a JP. The JP will be provided with a copy of the authorisation, and with a partially completed judicial application/order form, which is available on the Council's intranet. Advice should be sought from Legal Services, who will contact the court to arrange the hearing date for the application.

It should also be noted that in accordance with the relevant Regulations, the designation of the Chief Officer Governance (Monitoring Officer) to sanction the use of RIPA regulated covert surveillance extends upwards to the Chief Executive.

Ideally, the Authorising Officer should not be responsible for authorising their own activities i.e. those operations/investigations in which they are directly involved. However, the Codes of Practice recognize that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently.

6.3 Justification for covert surveillance

In order to use covert surveillance (both directed surveillance and a CHIS) lawfully the person granting the authorisation (i.e. the authorising officer) will have to demonstrate that the surveillance is both 'necessary' and 'proportionate' to meet the objective of the prevention or detection of crime or of prevention of disorder. The JP must also be satisfied that the use of the technique is necessary and proportionate.

6.3.1 The 'necessity' test

RIPA first requires that the authorising officer must be satisfied that the authorisation is necessary, in the circumstances of the particular case, for the prevention and detection of crime, or prevention of disorder. This is the only statutory ground on which local authorities are now able to carry out directed surveillance and use a CHIS. For the purposes of the authorisation of directed surveillance, the crime threshold referred to in paragraph 4 above must be met. Covert surveillance cannot be "necessary" unless, in that particular case, there is no reasonably available overt method of discovering the desired information.

6.3.2 The 'proportionality' test

Then, if the activities are necessary, the authorising officer must be satisfied that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is **excessive** in the circumstances of the case or if the information which is sought could reasonably be obtained **by other less intrusive means**. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

6.4 CHIS – additional requirements

In addition, there are further criteria in relation to CHIS authorisations. Namely, that specific arrangements exist to ensure that, amongst other things, the source is independently managed and supervised, that records are kept of the use made of the source, that the source's identity is protected from those who do not need to know it, and that arrangements also exist to satisfy such other requirements as may be imposed by an Order made by the Secretary of State.

RIPA provides that an authorising officer must not grant an authorisation for the use or conduct of a source unless he believes that arrangements exist that satisfy these requirements. In this regard, the particular attention of authorising officers is drawn to paragraphs 7.15 – 7.21 of the CHIS Code of Practice concerning the security and welfare of a CHIS and the need to carry out a **risk assessment**.

The Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI No. 2725) details the particulars that must be included in the records relating to each CHIS. The authorising officer should comment on all these aspects in his "comments" box, as he may have to justify the fact that he has taken account of these requirements and made an appropriate provision to comply.

6.4.1 The Covert Human Intelligence Sources (Criminal Conduct) Act 2021

This new piece of legislation amends RIPA to allow some agencies to authorise someone that they are deploying as a CHIS to commit crimes in the course of, or otherwise in connection with the conduct of Covert Human Intelligence Source. This act is mentioned here to confirm that Local Authorities are **NOT** one of the relevant authorities or agencies that can authorise this kind of conduct.

6.5 Collateral Intrusion

Before authorising surveillance, the authorising officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (particularly when considering the proportionality of the surveillance). This is referred to as collateral inclusion, and the following should be considered:

I. measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those not directly connected with the investigation or operation;

II. an application for an authorisation should include an assessment of the risk of any collateral intrusion and the authorising officer should take this into account, when considering the proportionality of the surveillance;

III. those carrying out the surveillance should inform the authorising officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation; and

IV. when the original authorisation may not be sufficient, consideration should be given to whether the authorisation needs to be amended and re-authorised or a new authorisation is required.

6.6 Local community sensitivities

Any person applying for or granting an authorisation will also need to be aware of what the Codes of Practice refer to as “any particular sensitivities in the local community” where the surveillance is taking place or of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance.

7 Part 3: Directed Surveillance Authorisation Requirements

7.1 Applications for directed surveillance authorisation

Applications for authorisation to carry out directed surveillance must be made in **writing** using the **standard Application Form** and judicial approval form available on the Council’s intranet.

7.2 Duration of directed surveillance authorisations

A written authorisation granted by an authorising officer, and approved by a JP, will cease to have effect (unless renewed) at the end of a period of **three months** beginning with the day on which it took effect.

7.3 Reviews of directed surveillance authorisations

Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to **‘confidential information’** (see below) or involves collateral intrusion.

Authorisations must be reviewed by the authorising officer therefore **at least monthly** using the **standard Review Form** available on the Council’s intranet to ensure that they remain in force only for so long as it is necessary.

7.4 Renewals of directed surveillance authorisations

If at any time before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may renew it in writing for **a further period of three months** using the **standard Renewal Form** available on the Council’s intranet. The same conditions attach to a renewal of

surveillance as to the original authorisation. An order from a JP is required for a renewal in the same way as for an authorisation.

A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An application for renewal should not be made until **10 working days** before the authorisation period is drawing to an end. However, where renewals are timetabled to fall outside of court hours, for example during a holiday period, care must be taken to ensure that the renewal is completed ahead of the deadline.

Any person who would be entitled to grant a new authorisation can renew an authorisation, but an order from a JP is also required. Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

7.5 Cancellation of directed surveillance authorisations

The authorising officer who granted or last renewed the authorisation **must** cancel it using the **standard Cancellation Form** available on the Council's intranet if he is satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Authorisations should not be allowed to simply expire.

Where the authorising officer is no longer available, this duty will fall on the person who has taken over the role of authorising officer or the person who is acting as authorising officer **(see the Regulation of Investigatory Powers (Cancellation of Authorisations) Order 2000; SI No: 2794).**

If the authorising officer is on sick or annual leave or is otherwise unable to cancel the authorisation for good reason, any other officer designated to grant authorisations may cancel the authorisation.

7.6 Ceasing of surveillance activity

As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date and time when such an instruction was given should be recorded in the notification of cancellation where relevant (see standard cancellation form).

7.7 Urgent Cases

A JP may consider an authorisation out of working hours in exceptional cases. This must be arranged through the court, and two completed judicial application/order forms must be provided so that one can be retained by the JP.

7.8 Confidential Information

RIPA does not provide any special protection for 'confidential information'.
The Codes of Practice, however, do provide additional safeguards for such information. Confidential information consists of matters subject to legal privilege; confidential personal information (information relating to the physical or mental health or spiritual counselling of a person who can be identified from it) or confidential constituent information (relating to communications between a Member of Parliament and a constituent in respect of constituency matters) or confidential journalistic material (material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence). Further details about these categories of confidential information are set out in the Codes themselves, and advice can be obtained from Legal Services.

Special care should be taken if there is a likelihood of acquiring any confidential information. Such authorisations should only be granted in exceptional and compelling circumstances with full regard to the proportionality issues such surveillance raises.

In accordance with the provisions of the Code, in cases where through the use of the surveillance it is likely that confidential information will be acquired, the use of surveillance must be authorised by the Chief Executive.

If, exceptionally, any Council investigation is likely to result in the acquisition of confidential material, officers are required to obtain the prior approval of Legal Services before applying for an authorisation.

If confidential material is acquired during the course of an investigation, the following general principles apply:

- confidential material should not be retained or copied unless it is necessary for a lawful purpose;
- confidential material should be disseminated only where an officer (having sought advice from the Legal Services Manager) is satisfied that it is necessary for a lawful purpose;
- the retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information; and confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

8 Part 4: CHIS Authorisation Requirements

Generally speaking, the authorisation requirements for directed surveillance also apply to a CHIS authorisation. There are, however, some variations, and the crime threshold as set out in paragraph 4 does not apply to a CHIS authorisation.

8.1 Duration of CHIS authorisations

A written CHIS authorisation granted by an authorising officer and approved by a JP, will cease to have effect (unless renewed) at the end of a period of **twelve months** beginning with the day on which it took effect.

8.2 Renewal of CHIS Authorisations

An authorising officer may renew a CHIS authorisation in writing **for a further period of twelve months**. This is subject to approval from a JP.

The same conditions attach to a renewal of surveillance as to the original authorisation. However, before renewing an authorisation for the use or conduct of a CHIS, officers are required to carry out a review of the use made of that source, the tasks given to that source and the information so obtained.

8.3 CHIS Forms

Standard **CHIS Application; Review; Renewal, and Cancellation Forms**, and the **Judicial Approval form** are available on the Council's intranet. Officers are required to use these forms in the appropriate circumstances.

8.4 Vulnerable Adults

In accordance with the CHIS Code of Practice, a **'vulnerable person**' should only be authorised to act as a CHIS in the most exceptional circumstances and must be authorised by the **Chief Executive**. Legal advice should always be sought. A 'vulnerable individual' is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation.

8.5 Juvenile Sources

Special safeguards also apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. Legal advice should always be sought. On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him. In other cases, authorisations should not be granted unless the special provisions contained within **The Regulation of Investigatory Powers (Juveniles) Order 2000 (SI No. 2793)** are satisfied. Authorisations for juvenile sources must be authorised by the **Chief Executive** the duration of such an authorisation is **one month only** instead of the usual twelve months.

9 Part 5: Other Authorisation Requirements

The Codes of Practice provide that a centrally retrievable record of all authorisations should be held by each public authority and regularly updated whenever an authorisation is granted, reviewed, renewed or cancelled. The record should be made available to the relevant Commissioner or an Inspector from the Investigatory Powers Commissioner's Office (IPCO), upon request. These records will be retained for a period of at least three years from the ending of the authorisation and will comprise of the information prescribed in the Codes.

The Council will also maintain a record of specified documentation relating to authorisations as further required by the Codes.

To give effect to these requirements The Authorising Officer is required to e-mail all completed RIPA forms to the Monitoring Officer within two working days of the grant; review; renewal; or cancellation of the authorisation so that the Council's central recording and monitoring systems can be kept up to date.

The Authorising Officer should however ensure that original RIPA forms are kept on the investigation case file and stored securely.

In addition, the Monitoring Officer will report periodically to Audit Committee with the register of authorisations to enable them to be satisfied that RIPA authorisation requirements are being complied with.

9.1 Retention and destruction of the product of surveillance

Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable period, commensurate to any subsequent review.

The Codes of Practice draw particular attention to the requirements of the code of practice issued under the **Criminal Procedure and Investigations Act 1996**. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

Where material is obtained by surveillance, which is **wholly unrelated** to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be **destroyed immediately**. Consideration of whether or not unrelated material should be destroyed is the responsibility of the authorising officer.

There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. Each Service must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Authorising officers must ensure compliance with the appropriate data protection requirements relating to the handling and storage of material.

9.2 Acting on behalf of another

In cases where one agency is acting on behalf of another, it is usually for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by the Police with the use of the Council's CCTV systems, an authorisation must be obtained by the Police.

10 Part 6: Practical Application of RPIA

10.1 Who is affected by RIPA?

As the Council has already recognised in respect of the application of the **Human Rights Act 1998**, RIPA will impact on the enforcement activities of all the Council's regulatory Services, but, in the case of authorisations for directed surveillance, the crime threshold referred to in paragraph 4 must be met. This means that directed surveillance will no longer be able to be used in some investigations where it was previously authorised, e.g. dog fouling. However, this does not mean that it will not be possible to investigate these matters with a view to stopping offending behaviour. Routine patrols, observation at trouble "hotspots", immediate response to events and overt use of CCTV are all techniques which do not require RIPA authorisation.

A public authority may only engage RIPA when in performance of its "core functions" in contrast to the "ordinary functions" which are undertaken by all authorities (e.g. employment and contractual matters). Accordingly, the disciplining of an employee is not a core function, although related criminal investigations may be.

10.2 'General observation vs. 'systematic surveillance'

According to the Covert Surveillance Code of Practice "General observation duties of many law enforcement officers, and other public authorities do not require authorisation under the 2000 Act". For example, police officers will be on patrol to prevent and detect crime, maintain public safety and prevent disorder or trading standards or HM Customs and Excise officers might covertly observe and then visit a shop as part of their enforcement function to verify the supply or level of supply of goods or services that may be liable to a restriction or tax. Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual.

The clear view expressed therefore is that usually low-level activity such as general observation will not be regulated under the provisions of RIPA provided it does not involve the systematic surveillance of an individual. That said, the determination of what constitutes 'general observation' on the one hand and 'systematic surveillance' on the other is a question

of fact, the determination of which is not always straightforward and depends on the particular circumstances of an individual case.

In practice, the issue will turn on whether the covert surveillance is likely to result in obtaining any information in relation to a person's private or family life, whether or not that person is the target of the investigation or operation. If in doubt you are strongly recommended to obtain an authorisation.

10.3 'Covert' vs. 'overt' surveillance

In accordance with the Council's usual practice, wherever possible and appropriate Services should give advance warning of their intention to carry out surveillance. This is because the provisions of RIPA regulate the use of covert surveillance only. In some cases, a written warning may itself serve to prevent the wrongdoing complained of.

However, in order to properly put a person on notice that he is or may be the subject of surveillance, the notification letter must be couched in sufficiently precise terms so that he knows what **form** the surveillance will take (i.e. record of noise; photographs etc.). In fact, in line with directed surveillance requirements, notification letters should state **how long** the surveillance is likely to last (which should not be longer than three months); the necessity for the surveillance should be **reviewed at least monthly**; if it is necessary to continue the surveillance beyond the initial specified period a **renewal letter** should be sent to the 'noisy' neighbour, for example, and he should be informed when the surveillance has ceased.

It is also important to instruct the investigating officer not to exceed the limits of the 'surveillance' he has been asked to carry out.

Whilst it is accepted that the definition of 'covert' set out in RIPA could be interpreted very broadly, it is suggested that whether the surveillance activity is covert or not depends on the investigator's intention and conduct. If there is some element of **secrecy** or **concealment** the activity is likely to be covert.

Wherever possible or appropriate, officers should be **open; obvious and overt**.

10.4 CCTV

Overt CCTV systems used for general purposes are not usually regulated by RIPA (but CCTV in general is regulated by the Data Protection Act 2018, the GDPR 2016/679 and the CCTV Code of Practice issued by the Information Commissioner). If, however, CCTV systems are used to **track individuals** or **specific locations** and the surveillance is **pre-planned** (i.e. not an immediate response to events or circumstances which by their very nature, could not have been foreseen) **a directed surveillance** authorisation must be obtained.

10.5 Recognising a CHIS

The provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information to the police or other authorities, as part of their normal civic duties, or to contact numbers set up to receive information (such as Crime stoppers, Customs Confidential, the Anti-Terrorist Hotline, or the Security Service Public Telephone Number). Members of the public acting in this way would not generally be regarded as sources.

However, when an informant gives repeat information about a suspect or about a family, and it becomes apparent that the informant may be obtaining the information in the course of a family or neighbourhood relationship, this probably means that the informant is a CHIS, to

whom a duty of care is owed if the information is then used, even though he or she has not been tasked by the authority to obtain information on its behalf.

The use of professional witnesses to obtain information and evidence is clearly covered.

10.6 "…. establishing or maintaining a personal or other relationship……"

Whilst the meaning of "...establishing or maintaining a personal or other relationship…" is not clear and is open to interpretation, it is suggested that there has to be some measure of **intimacy** beyond the ordinary conversation. Only if an officer, for example, establishes some measure of **trust and confidence** with the person who is the subject of the surveillance will he be establishing or maintaining a personal or other relationship.

Usually a simple enquiry or a request for general information (i.e. a request for information which would be supplied to any member of the public who enquired) not obtained under false pretences is not likely to be regulated by RIPA.

10.7 Simple test purchase transactions

Whether or not test purchase transactions are regulated by RIPA depends on the circumstances and in particular the conduct of the person carrying out the surveillance. Usually simple covert test purchase transactions carried out under existing statutory powers where the officer involved does not establish a personal or other relationship will not require a CHIS authorisation.

Officers should, however, be wary of the law on **'entrapment'**. Whereas officers can in appropriate circumstances, present a seller or supplier, for example, an opportunity which he could act upon, officers cannot 'incite' the commission of an offence i.e. encourage, persuade or pressurise someone to commit an offence.

10.8 Use of DAT recorders

If it is appropriate to do so, Environmental Health officers, and to a much lesser extent Council Housing officers, use a recorder to monitor noise levels (usually at residential premises) following noise nuisance complaints. Whilst the recorder is installed by officers, the complainant decides when to switch the recorder on and off.

The covert recording of suspected noise nuisance where the intention is only to record excessive noise levels from adjoining premises, and the recording device is calibrated to record only excessive noise levels, may not require an authorisation, as the perpetrator would normally be regarded as having forfeited any claim to privacy.

That said, a Digital Audio Tape (DAT) recorder is a sophisticated piece of monitoring equipment and if used covertly may constitute directed surveillance. In general, a letter is sent to the person who is to be the subject of the surveillance, and this should mean that subsequent surveillance is overt, and an authorisation will not as a matter of course be required. However, if there is any doubt as to whether surveillance is covert, e.g. if any longer than a few weeks has passed since the alleged perpetrator was informed that monitoring might be carried out, and if it is likely that private information will be obtained, then an authorisation should be sought.

10.9 RIPA forms

It is imperative that RIPA forms are completed in full whenever RIPA regulated surveillance activity is planned. The information given must be specific and detailed; must relate to the particular facts of an individual case (i.e. avoid standard wording if at all possible) and must demonstrate that a proper risk assessment has been carried out. Both those who apply for an authorisation and the Authorising Officer should refer to this policy and to the relevant Code of Practice in completing the relevant form,

10.10 Role of Authoring Officers

The Authorising Officer is required to ask themselves: “Have I got sufficient information to make an informed decision as to whether or not to authorise surveillance activity on the particular facts of this case?” and must recognise that RIPA imposes new and important obligations on those Services affected by RIPA

Authorising officers must be satisfied that there are adequate checks in place to ensure that the surveillance carried out is in line with what has been authorised. Such monitoring should be properly documented as well as the decision-making process in general.

Officers are strongly recommended to read this policy in conjunction with the Covert Surveillance and CHIS Codes of Practice which provide supplementary guidance.

If the surveillance is not properly authorised, the protection offered by RIPA will be lost.

10.11 How to access RIPA documents?

RIPA itself; explanatory notes to RIPA, the Covert Surveillance and CHIS Codes of Practice; RIPA statutory instruments and other RIPA documents are available on the Home Office web-site: https://www.gov.uk/government/collections/ripa-codes
Relevant RIPA documents as well as this policy and the Council’s standard forms have also been posted on the Council’s intranet.

11 Training and awareness

It is the policy of the Council to provide adequate training for all its employees so that they are aware of the RIPA provisions and know when certain activities are required to be authorised. Authorising Officers will be trained in the proper use of their powers as with investigating officers The Council seeks to ensure that all staff likely to be engaged in surveillance work and the use of CHIS understand the regulatory framework and know which officers are authorised Investigating Officers and the Authorising Officer

Training and refresher training shall be provided on a regular basis.

Appendix 1:

Directed surveillance forms

Application for the authorisation of directed surveillance:
RIPA-application-directed-surveillance.doc (sharepoint.com)

Review of directed surveillance authorisation:
RIPA-review-directed-surveillance.doc (sharepoint.com)

Renewal of directed surveillance authorisation:
RIPA-renewal-directed-surveillance.doc (sharepoint.com)

Cancellation of a directed surveillance authorisation:
RIPA-cancellation-directed-surveillance.doc (sharepoint.com)

CHIS (Covert Human Intelligence Source) forms

Application for authorisation of use or conduct of a CHIS:
chis-application.doc (sharepoint.com)

Review of a CHIS authorisation:
chis-review.doc (sharepoint.com)

Renewal of a CHIS authorisation:
chis-renewal.doc (sharepoint.com)

Cancellation of a CHIS authorisation:
chis-cancellation.doc (sharepoint.com)

Judicial Approval Form
JP-approval-order-form.doc (sharepoint.com)

Appendix 2:

PROCESS TO BE FOLLOWED WHEN CONSIDERING USING SOCIAL NETWORKING SITES IN INVESTIGATIONS OR TO GATHER EVIDENCE.

Where an officer considers it necessary to view a social networking site to investigate an allegation or to gather information the following process is to be followed:

1. Officers must not use their own personal or private account when accessing social networking sites for investigations/evidence gathering, only Council accounts should be used.

2. Officers may access the main page of an individual's profile to take an initial view as to whether there is any substance to the allegation of the matter being investigated and is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation.

3. Officers are required to keep a log recording when social networking sites are viewed for investigations/evidence gathering. Each viewing of a company or individual's social networking site must be recorded on the log. This is to enable the Council to monitor the use of these sites for investigations/evidence gathering and use this information to review policies and guidance. See attached excel template below.

4. If it is considered that there is a need to monitor a company's or individual's social networking site, for example by systematically collecting and recording information about a particular person or group, then the officer must refer the matter to their Head of Service for consideration as to whether a RIPA authorisation from the Magistrates Court may be required. If officers are in any doubt as to whether an authorisation is required, they should seek advice from the Information Governance Manager or Authorising Officer (Director for Corporate Services), before continuing to access a social networking site.

5. If the offence being investigated falls under RIPA, a formal RIPA application must be completed, authorised by the Council's Authorising Officer and then approved by a Magistrate.

6. If the offence being investigated falls outside RIPA, a 'Non-RIPA' form must be completed and forwarded to the Authorising Officer.

7. Officers also need to be aware that any evidence captured as part of a criminal investigation will need to comply with the relevant legislation (The Police and Criminal Evidence Act 1984, Criminal Procedure Rules 2018 and the Criminal Procedure and Investigations Act 1996) and advice should be sought from the Council's Legal Services Manager.

8. A copy of all forms should be forwarded to the Council's Information Governance Manager so that a central record of RIPA requests and Authorisations can be kept.

Social Media Access Log v1.0.xlsx