Isle of Wight Council

COVERT SURVEILLANCE POLICY

THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

Version 13

June 2021

CONTENTS

Page No

1. Introduction 1

1.1 Summary
1.2 Background
1.3 Review
1.4 Scope

2. General 2

2.1 Definition of Surveillance
2.2 Confidential Material

3. Directed and Intrusive Surveillance 3

3.1 Directed Surveillance
3.2 Intrusive Surveillance

4. Identifying Directed Surveillance 3

4.1 Is the surveillance covert?
4.2 Is the surveillance for the purposes of a specific investigation or a specific operation?
4.3 Is the surveillance in such a manner that is likely to result in the obtaining of private information about a person?
4.4 Is the surveillance otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to get authorisation?

5. Internet Site Monitoring 5

6. Covert Human Intelligence Sources 7

6.1 Definition
6.2 Security and Welfare

7. Communications Data 9

7.1 Definition

8. Authorisation Procedure 10

8.1 General
8.2 Who can give Provisional Authorisations?
8.3 Grounds for Authorisation – the 'necessary & proportionate' test
8.4 Collateral Intrusion
8.5 Judicial Approval of Provisional Authorisations and Renewals
8.6 Special Procedures in respect of Communications Data
8.7 Urgency
8.8 Standard Forms

9. Activities by other Public Authorities 15

10. Joint Investigations 15

11. Non-RIPA Activities 15

12. Duration, Renewals and Cancellation of Authorisations 16

12.1 Duration
12.2 Reviews
12.3 Renewals
12.4 Cancellations

13. Records 17

13.1 Maintaining the Central record of all Authorisations
13.2 Records maintained in the department
13.3 Other Record of Covert Human Intelligence Sources
13.4 Checks on the Integrity of the Process

14. Retention and Destruction 20

15. Consequences of Ignoring RIPA 20

16. Scrutiny of Investigatory bodies 21

Appendix 1 – Directed Surveillance 22

Appendix 2 – Non-RIPA Surveillance Form 25

Covert Surveillance

1. INTRODUCTION

1.1 Summary

The Regulation of Investigatory Powers Act 2000 ('RIPA') brought into force the regulation of covert investigation by various bodies, including local authorities. RIPA regulates several investigative procedures, the most recent of which is the access to communications data. This document is intended to provide officers with guidance on the use of covert surveillance including use of social networking and auction websites, Covert Human Intelligence Sources ('CHIS') and the obtaining and disclosure of communications data under RIPA.

It should be noted that these powers relating to directed surveillance can only be used by officers of the council for the purpose of **preventing or detecting crime or of preventing disorder** and further limited by the matters set out in para 8.3. If covert surveillance activity is to be undertaken that does not meet this threshold please refer to section 11 (Non-RIPA) and the Councils relevant employment policy and social media policy.

Officers must have regard to the Codes of Practice issued by the Home Office under RIPA. (the Covert Surveillance & Property Interference Revised Code of Practice (August 2018) may be found here Code of Practice link)

1.2 Background

The Human Rights Act 1998 requires the Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, their home and correspondence. The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council may interfere in the citizens' rights mentioned above, if such interference is:

(a) In accordance with the law
(b) Necessary (as defined in this document); and
(c) Proportionate (as defined in this document)

RIPA provides a statutory mechanism for authorising certain types of surveillance. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate and that both the public interest and the human rights of individuals are suitably balanced.

If the correct procedures are not followed, evidence may be excluded by the courts, a complaint of maladministration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation. It is essential, therefore, that all involved with RIPA comply with this document and any further guidance that may be issued, from time to time, by the Senior Responsible Officer.

Each officer of the Council with responsibilities for the conduct of investigations, shall, before carrying out any investigation involving RIPA, undertake appropriate training to ensure that investigations and operations that he/she carries out will be conducted lawfully.

The Strategic Manager of Legal Services is appointed as the Senior Responsible Officer ("SRO") to ensure the integrity of the process within the Council and its compliance with RIPA; to have oversight of reporting of errors to the relevant oversight commissioner; responsibility for engagement with the Investigatory Powers Commissioners Office when they conduct their inspections and where necessary, oversight of the implementation of any post-inspection action plan. The Senior Responsible Officer will also ensure that Members review the Council's use of RIPA.

The SRO may appoint a nominated officer to act to be the lead contact and to have responsibility for the central record. The nominated officer is the Lawyer appointed for crime and regulatory matters.

1.3 Review

RIPA and this document are important for the effective and efficient operation of the Council's actions with regard to surveillance. This document will be kept under review by the SRO and the outcomes of this review will be presented to the Cabinet member. Authorising Officers must bring any suggestions for continuous improvement of this document to the attention of the SRO or nominated officer at the earliest possible opportunity.

1.4 Scope

RIPA limits local authorities to using three covert techniques, as set out below:

- **Directed surveillance** is essentially covert surveillance in places other than residential premises or private vehicles
- A **Covert human intelligence source (CHIS)** includes undercover officers, public informants and people who make test purchases (for enforcement purposes)
- Acquisition of **Communications data (CD)** is the 'who', 'when' and 'where' of a communication, but not the 'what' (ie the content of what was said or written).

2. GENERAL

2.1 Definition of 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.

Surveillance also includes the interception of postal and telephone communications where the sender or recipient consents to the reading of or listening to or recording of the communication. This is a form of directed surveillance.

2.2 Confidential Material

Care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information, confidential journalistic material and communications between an MP and a constituent. Applications in which the surveillance is likely to result in the acquisition of confidential material will only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises. The Authorising Officer shall give the fullest consideration to any cases where the subject of the surveillance might reasonably expect a high degree of privacy, for instance in his or her home.

Where a likely consequence of surveillance would result in the acquisition of confidential material, the investigating officer must seek authority from the Chief Executive, or, in his absence, the person acting as the Chief Executive.

3. DIRECTED AND INTRUSIVE SURVEILLANCE

3.1 Directed Surveillance

Directed Surveillance is surveillance which:

(a) is covert; and

(b) is not intrusive surveillance (see definition below - the council is prohibited by law from carrying out any intrusive surveillance);

(c) is not carried out as an immediate response to events where it would not be practicable to obtain authorisation under the Act;

(d) is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation).

3.2 Intrusive Surveillance

Intrusive Surveillance occurs when surveillance:

(a) is covert;

(b) relates to residential premises and/or private vehicles; and

(c) involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

Intrusive surveillance cannot be carried out or approved by the council. Only the police or other law enforcement agencies are permitted to use such powers. Likewise, the council has no statutory powers to interfere with private property.

4. IDENTIFYING DIRECTED SURVEILLANCE

Ask yourself the following questions:

4.1 Is the surveillance covert?

Covert surveillance is any surveillance that is carried out so as to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

If your activities are not hidden from the subjects of your investigation, you are not within the RIPA framework at all. In many cases, officers will be behaving in the same way as a normal member of the public, and/or will be going about Council business openly (e.g. a market inspector walking through markets).

Similarly, surveillance will be overt if the subject has been told it will happen. For example, following a noise complaint the noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or when an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or may not identify themselves to the owner/proprietor to check that conditions are being met.

If the same outcome can be achieved by overt means then those means need to be fully explored in the first instance. Covert surveillance must only be undertaken when there is no less invasive way of achieving the outcome.

4.2 Is the surveillance for the purposes of a specific investigation or a specific operation?

The provisions of the Act do not normally cover the use of overt CCTV surveillance systems or Automated Number Plate Recognition (ANPR) in car parks. However, since members of the public are aware that such systems are in use, there may be occasions when public authorities use overt CCTV systems and/or ANPR for the purposes of a specific investigation or operation. For example, if the CCTV cameras are targeting a particular known offender then authorisation for directed surveillance may be necessary.

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

Private information includes any information relating to a person's private or family life. The concept of private information should be broadly interpreted to include an individual's private or personal relationship with others. It includes an individual's business and family relationships. Family life itself should be treated as extending beyond the formal relationships created by marriage.

4.4 Is the surveillance otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to get authorisation?

Directed surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. 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, an officer is under a continuing obligation to determine if an authorisation becomes necessary if their observation is undertaken for a sustained period. When

an immediate response to events becomes a sustained period is a matter of fact in each instance.

5. INTERNET SITE MONITORING

5.1 The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered.

5.2 Simple reconnaissance of social media and websites, ie, a preliminary examination with a view to establishing whether the site or its contents are of interest, is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation.

The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed.

In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity.

Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

Depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings. Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose

purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is **systematically collecting and recording information** about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online.

> *Example 1: A enforcement officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.*
>
> *Example 2: A local authority officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)*
>
> *Example 3: A public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.*

In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;

- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation.

> Example: Researchers within a public authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data by public authorities either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.

5.3 If the nature of the activity involves establishing or maintaining any form of relationship with the subject, their colleagues or friends with a view to obtaining information, then this activity by a Council employee or someone acting on their behalf, requires authorisation to use a covert human intelligence source (CHIS).

5.4 Use of a false identity for covert purposes is permissible if a RIPA authorisation is given. However, Council employees or someone acting on their behalf must not adopt the identity of a person known, or likely to be known, to the subject of interest, or users of the site without:

(a) RIPA authorisation,

(b) the explicit consent of the person whose identity is to be used; and

(c) giving consideration to the protection of the person whose identity is to be used.

5.5 Any council officer wishing to use social media to obtain private information of clients / members of the public should contact Legal Services for advice.

6. COVERT HUMAN INTELLIGENCE SOURCES

6.1 Definition

A person is a covert human intelligence source 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 to 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 source may include those referred to as agents, informants and officers working undercover.

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 so as to ensure that one of the parties to the relationship is unaware of the purpose.

A relationship is used covertly, and information obtained is disclosed covertly, if and only if it is used or disclosed so as to ensure that one of the parties to the relationship is unaware of the use or disclosure in question. The use of a source involves inducing, asking or assisting a person to engage in the conduct of a source, or to obtain information by means of the conduct of such a source.

This covers the use of professional witnesses to obtain information and evidence.

For example, it will include professional witnesses retained by Housing to pose as tenants to obtain information and evidence against alleged nuisance perpetrators.

Carrying out test purchases will not normally require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter). By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance.

The Code of Practice states that 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.

Members of the public acting in this way would not generally be regarded as a CHIS. However, if a member of the public has chosen of their own volition to supply information which they have obtained in the course of a personal or other relationship, and the council then rely upon the information, then we must ensure that appropriate safeguards are put in place to protect that member of the public as a duty of care may arise that we must satisfactorily meet.

6.2 Security and Welfare

Only the SRO is able to authorise the use of vulnerable individuals and juvenile CHIS'. The Authorising Officer shall have regard to the special safeguards and provisions that apply to vulnerable individuals and juvenile CHIS', more particularly

set out in the Covert Human Intelligence Source Code of Practice at CHIS Code of Practice link .

The Authorising Officer shall ensure that arrangements are in place for the proper oversight and management of CHIS', including appointing the following individual officers for each source:

A "**Handler**" who will have day-to-day responsibility for:

- dealing with the CHIS on behalf of the Council;
- directing the day to day activities of the CHIS;
- recording the information supplied by the CHIS; and
- monitoring the CHIS's security and welfare.

The Handler will usually be of a rank or position below that of the Authorising Officer.

A "**Controller**" who will be responsible for the management and supervision of the "handler" and general oversight of the use of the CHIS. Officers using a source shall consider the safety and welfare of that source (even after cancellation of the authorisation), and the foreseeable consequences to others of the tasks they are asked to carry out. The Authorising Officer shall carry out a risk assessment before authorising the source.

7. COMMUNICATIONS DATA

7.1 The Council may only acquire less intrusive types of CD; "Entity data" (e.g. the identity of the person to whom services are provided) or "Events Data" (e.g. the date and time sent, duration, frequency of communications). The location of the entity or events data at the time the communication is sent or received may also be obtained in appropriate cases. The Council is prohibited from obtaining "Content Data", the meaning of the communication, (e.g. what the communication says or contains).

Applications for CD are subject to independent examination, scrutiny and approval by the Investigatory Powers Commissioner (IPC) through the "Office of Communications Data Authorisations" (OCDA).

The Council will continue to maintain a collaboration agreement with the National Anti-Fraud Network (NAFN), to comply with IPA and to ensure any investigation follows best practice. The Council will consult and work with NAFN throughout the application process to ensure the legal basis for all applications are met. NAFN will act as a single point of contact between both the communications service providers and the Council concerning the request and provision of CD.

The Council will not acquire CD unless an application for authorisation is approved both internally, by designated senior officers and externally, by the Office for Communications Data Authorisations (OCDA).

An authorisation to acquire CD will remain in force for 1 month, unless a further application is made by the Council through NAFN and approved by OCDA. The authorisation may be cancelled at any time, by either OCDA or the Council.

In respect to applications for communications data made under the IPA, the "applicable crime purpose" must be met concerning all applications for both Entity Data and Events Data. The applicable crime purpose is defined differently in relation

to each of these data types. Where the CD sought is Entity Data, the applicable crime purpose is the prevention or detection of crime or the prevention of disorder. Where the CD is wholly or partly Events Data, the applicable crime purpose is defined as preventing or detecting serious crime (the serious crime threshold). Data relating to Events has the potential to be more intrusive than data relating to Entities.

An authorisation under RIPA will provide lawful authority for the investigating officer to carry out surveillance. In terms of monitoring e-mails and internet usage, it is important to recognise the interplay and overlaps with the Council's e-mail and internet policies and guidance, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and Data Protection Act legislation. RIPA forms should be used where **relevant** and they will only be relevant where the **criteria** listed on the forms are fully met.

8. AUTHORISATION PROCEDURE

8.1 General

Authorisation is required for the use of directed surveillance, for the conduct and use of CHIS' and for the conduct in relation to a postal service or telecommunication system and the disclosure to any person of such data, hereto referred to as the "RIPA powers".

Any officer who undertakes investigations (applicant) on behalf of the Council shall seek provisional authorisation in writing from an Authorising Officer in relation to any directed surveillance or for the conduct and use of any CHIS. Each provisional authorisation then needs to receive judicial approval before being acted upon.

Any officer wishing to engage in conduct in relation to a postal service and telecommunication system for obtaining communications data and the disclosure to any person of such data must also seek authorisation, the procedure and procedure of which differs slightly and is outlined in paragraph 8.6.

Authorising Officers will ensure that staff who report to them follow this policy document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document.

The authorising officer should also ensure that they clearly set out what activity and equipment has been authorised in order that those conducting the surveillance are clear on what has been sanctioned (as per the R v Sutherland ruling).

It is the council policy that a draft application be sent to Legal Services prior to provisional authorisation for quality check, unless it is not practicable to do so.

8.2 Who can give Provisional Authorisations?

By law, the 'Authorising Officer' for local authority purposes is the Chief executive, any Head of Service, service manager or equivalent (or Group Manager in relation to the Fire Service). Except in relation to communication data, an Authorising Officer may grant a provisional authorisation which does not take effect until it receives judicial approval (See paragraph 8.5). In relation to communication data, the local authority does not require judicial approval but is required to use the NAFN service to complete the application to OCDA.

Please note that certain provisional authorisations, namely those relating to confidential information, vulnerable individuals and juvenile CHIS', can only be granted by the Chief Executive, or, in his genuine absence, the officer appointed as Deputy Chief Executive.

A list is maintained by the SRO of the Council's Authorising Officer posts. The SRO has the delegated authority to add, delete or substitute posts.

It will be the responsibility of Authorising Officers who have been duly certified to ensure their relevant members of staff are also suitably trained as 'applicants' so as to avoid common mistakes appearing on forms for RIPA authorisations.

Training will be given, or approved by the SRO, before Authorising Officers are certified to sign any RIPA forms.

The Authorising Officers attend the magistrates' court for the purpose of presenting RIPA cases. These officers are best placed to answer any questions or clarify any points the magistrates may have on the application.

8.3 Grounds for Authorisation – the 'necessary & proportionate' test

An Authorising Officer has a number of obligations within the provisions of the Act, which must be met before using any of the RIPA powers. An Authorising Officer shall not grant a provisional authorisation for the use of the RIPA powers unless he believes:

(a) that a provisional authorisation is necessary and

(b) the provisionally authorised investigation is proportionate to what is sought to be achieved by carrying it out.

For local authority investigations, provisional authorisation is deemed "necessary" in the circumstances of the particular case if it is for the purpose of the prevention or detection of crime(s) punishable by 6 months imprisonment or more, or relates to the sale of alcohol or tobacco to underage persons, and if that objective could not be achieved without the information sought. For activities that do not meet this threshold please refer to the Non-RIPA section below.

Conduct is not deemed "proportionate" if pursuing the legitimate aim listed above will not justify the interference and the means used are excessive in the circumstances. Any conduct must meet the objective in question, must not be arbitrary or unfair, nor must the impact on any individuals or group be too severe.

The least invasive method of achieving the aim should be adopted. The risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation must be assessed and taken into account (see Collateral Intrusion below).

Consideration must be given to the seriousness of the offence under consideration and whether it could be punishable on summary conviction or on indictment, by a maximum term of at least six months imprisonment.

Careful consideration needs to be made by authorising officers of all of these points using the list below:

(a) Is the size and scope of the operation balanced by the gravity and extent of the perceived crime or offence?

(b) Is it clear how and why the methods to be adopted will cause the least possible intrusion on the subject and others?

(c) Is the activity an appropriate use of the legislation and the only reasonable way, having considered all alternatives, of obtaining the necessary result?

(d) Has evidence been provided of other methods considered and why they were not implemented?

Such consideration needs to be demonstrated on the authorisation form in the relevant parts. Authorising Officers must exercise their minds every time they are asked to sign a form. They must never sign or rubber stamp the form without thinking about both their own and the Council's responsibilities.

Any boxes not needed on the form/s must be clearly marked as being 'not applicable' or a line put through the same. Great care must also be taken to ensure accurate information is used and inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and retained for future audits.

Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved.

8.4 Collateral Intrusion

Before provisionally authorising investigative procedures, the Authorising Officer shall 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 (collateral intrusion). The investigating officer shall take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

An application for a provisional authorisation shall include an assessment of the risk of any collateral intrusion.

Where an operation unexpectedly interferes with the privacy of individuals who were not the subject of the investigation or covered by the authorisation in some other way, the investigating officer should inform the Authorising Officer immediately.

8.5 Judicial Approval of Provisional Authorisations and Renewals

Except in relation to communication data, the Council is only able to grant a "provisional" authorisation or renewal to make use of any of the RIPA powers. All provisional authorisations and renewals must be approved by the Magistrates Court before the use of the RIPA power in the investigation commences.

The Council must apply to the local Magistrates Court for judicial approval of an authorisation or a renewal of an authorisation. The Council does not need to give notice of the application to the person(s) subject to the application, or their legal representatives. If the Magistrates Court refuse to approve the application, they may also make an order quashing the provisional authorisation.

The local authority will provide the magistrate(s) with a copy of the original RIPA provisional authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the magistrate(s) and should contain all the information that is relied upon. The local authority will provide the magistrates with a partially completed judicial application form containing a brief summary of the circumstances of the case. This is supplementary and does not replace the need to supply the provisionally authorised RIPA authorisation, or renewal, as well.

The Magistrates will consider the provisionally authorised application or renewal, and will need to satisfy themselves that:

(a) At the time of provisional authorisation, there were reasonable grounds for believing that the tests of necessity and proportionality were satisfied in relation to the authorisation, and that those grounds still exist;

(b) That the person who granted provisional authorisation was an appropriately designated person;

(c) The provisional grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under RIPA; and

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

The Authorising Officer is responsible for tabling the application IN WRITING for judicial approval in the Magistrates Court before the use of the RIPA powers commence. The order section of the application form will be completed by the magistrate(s) and will be the official record of the magistrate(s) decision.

The local authority will need to obtain judicial approval for all initial RIPA authorisations / applications and renewals and the local authority will need to retain a copy of the judicial application order form after it has been signed by the magistrate(s). There is no need for the magistrate(s) to consider either cancellations or internal reviews.

The hearing is a 'legal proceeding' and therefore the local authority officers need to be formally designated to appear and present evidence or provide information as required by the magistrate(s).

8.6 Special Procedure for Provisional Authorisation of and Issuing of Notices in respect of Communications Data

The Act provides two different ways of provisionally authorising access to communications data; through a provisional authorisation under Section 22(3) and by a provisional notice under Section 22(4). A provisional authorisation would allow the authority to collect or retrieve the data itself. A provisional notice is given to a postal or telecommunications operator and requires that operator to collect or retrieve the data and provide it to the authority serving the notice. An Authorising Officer decides whether or not a provisional authorisation should be granted, or a provisional notice given.

A Section 22(3) provisional authorisation may be appropriate where:

- the postal or telecommunications operator is not capable of collecting or retrieving the communications data;

- it is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;
- there is a prior agreement in place between the authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of data.

Applications for the obtaining and disclosure of communications data may only be made by officers of the Council.

Provisional notices and, where appropriate, provisional authorisations for communications data must be channelled through single points of contact ("SPoCs"). The Council currently uses an on-line SPoC service provided by the National Anti-Fraud Network (NAFN) that can be used in accordance with the terms of our agreement.

It is the responsibility of the Isle of Wight Council to obtain both provisional authorisation and judicial approval of an application before NAFN are requested to obtain the required communications data.

The SPoC:

(a) where appropriate, assesses whether access to the communications data is reasonably practical for the postal or telecommunications operator;

(b) advises applicants and authorising officers on the practicalities of accessing different types of communications data from different postal or telecommunications operators;

(c) provides safeguards for authentication;

(d) assesses the cost and resource implications to both the authorisation and postal or telecommunications operator.

Applications to obtain communications data should be made on the standard form available from Legal Services and submitted in the first instance to the SpoC. The SpoC will forward the application to the Authorising Officer for either the provisional authorisation of conduct, or the issuing of a provisional notice. If satisfied that the proposed investigation is both necessary and proportionate, the Authorising Officer will return the provisional authorisation or provisional notice to the SPoC who will then liaise with the postal telecommunications company, after the appropriate Judicial Approval has been obtained.

The disclosure of data under a notice will only be made to the Authorising Officer or to the Council's SPoC. Communications data, and all copies, extracts and summaries of it must be handled and stored securely. The requirements of Data Protection Act legislation and the principles of the Criminal Procedure and Investigations Act 1996 must be strictly followed.

8.7 Urgency

Urgent authorisation authorisations are no longer available in relation to the use of the RIPA powers.

8.8 Standard Forms

All authorisations must be in writing.

The local authority will provide the magistrate(s) with a partially completed judicial application form that will also contain a brief summary of the circumstances of the case. This is supplementary and does not replace the need to supply the provisionally authorised RIPA authorisation or renewal as well.

Standard forms for seeking use of the RIPA powers are available from Legal Services. The authorisation shall be sought using the standard forms, as amended from time to time.

9. ACTIVITIES BY OTHER PUBLIC AUTHORITIES

The investigating officer shall make enquiries of other public authorities, e.g. the police, whether they are carrying out similar activities if he considers that this is a possibility. This will ensure that there is no conflict between the activities of this Council and those other public authorities.

10. JOINT INVESTIGATIONS

When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this document and the forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

When some other agency (e.g. police, Customs & Excise, Inland Revenue etc.):

(a) wish to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes, he must obtain the details and purpose of the surveillance and evidence of the RIPA authorisation and any required judicial approval (if required) for the purposes of protecting the Council and the use of its resources.

(b) wish to use the Council's premises for their own RIPA action, the officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. In such cases, the Council's own RIPA forms should not be used as the Council is only assisting and not being involved in the RIPA activity of the external agency.

In terms of (a), if the police or other agency wish to use the Council's resources for general surveillance, as opposed to specific RIPA authorisations, an appropriate letter requesting the proposed use, remit, duration, details of who will be undertaking the general surveillance and the purpose of it must be obtained from the police or other agency before any Council resources are made available for the proposed use.

11. NON-RIPA ACTIVITY

Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 means that a Local Authority can only grant an authorisation under RIPA where the Local Authority is investigating criminal offences which attract a maximum custodial sentence of at least six months or criminal offences relating to the underage sale of alcohol or tobacco.

However, there may be exceptional circumstances where there is a necessity for the Council to undertake covert surveillance, which does not meet the legislative threshold, such as in cases of serious disciplinary investigations or anti-social behaviour offences. There are also occasions where Social workers use social media surveillance to determine whether or not a child is in need of protection.
The Council must still meet its obligations under the Human Rights Act and any surveillance outside of RIPA must still be necessary and proportionate having taken account of the intrusion issues. The decision making process and the management of such surveillance must be documented.

The authority considers it prudent to maintain an auditable record of decisions and actions to use covert surveillance without the protection of RIPA and that such activity should be regularly reviewed by the Senior Responsible Officer.

The Senior Responsible Officer will therefore maintain an oversight of non RIPA surveillance to ensure that such use is compliant with Human Rights legislation. The Central nominated Officer will maintain a central record of non RIPA surveillance.

As part of the process of formally recording and monitoring non RIPA surveillance, a non RIPA surveillance application form (see Appendix 2) should be completed and authorised by a Strategic Manager or above.

12. DURATION, RENEWALS AND CANCELLATION OF AUTHORISATIONS

12.1 Duration

Authorisations must be reviewed in the time stated and cancelled once no longer needed. Authorisations last for:

(a) 12 months from the date of the judicial approval for the conduct or use of a source

(b) three months less a day from the date of the last judicial approval for directed surveillance

(c) one month from the date of judicial approval for communications data, or earlier if cancelled under Section 23(8) of the Act.

Whether the surveillance is carried out/conducted or not in the relevant period, this does not mean that the authorisation is spent. Authorisations should not be allowed to expire; they should be reviewed or cancelled if no longer required.

12.2 Reviews

The Authorising Officer shall undertake regular reviews of authorisations to assess whether the surveillance needs to continue. At a minimum these should be carried out monthly from the start date. The results of a review should be recorded on the central record of authorisations. Where the surveillance provides access to confidential information or involves collateral intrusion, the officer should conduct frequent reviews.

Standard review forms for directed surveillance and CHIS are available from Legal Services.

12.3 Renewals

Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisations.

Authorisations can be renewed in writing shortly before the maximum period has expired. An authorisation cannot be renewed after it has expired. The Authorising Officer must consider the matter afresh, taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred. The renewal will begin on the day when the authorisation would have expired, provided the necessary judicial approval has been obtained. A further requirement in relation to renewal of covert human intelligence sources, is that judicial approval will only be granted if the Magistrates are satisfied that a review has been carried out, which considers:

- the use made of the source in the period since authorisation was granted (or the last renewal); and
- the tasks given to the source during that period, and the information obtained from the conduct or use of the source; and for the purposes of making an Order, the Magistrates have considered the results of that review.

The Authorising Officer who granted or last renewed the authorisation must cancel it if he is satisfied that the investigative procedure no longer meets the criteria upon which it was authorised.

Standard renewal forms for the authorisation of directed surveillance and CHIS are available from Legal Services.

12.4 Cancellations

An Authorising Officer shall cancel a notice or authorisation as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. The duty to cancel a notice falls on the Authorising Officer who issued it.

In the case of a notice issued in respect of communications data, the relevant postal or telecommunications operator will be informed of the cancellation.

Standard cancellation forms for communications data, directed surveillance and CHIS are available from Legal Services.

When completing the cancellation form care should be taken to record when the activity ceased, what value the surveillance had been to the investigation and what evidence “products” had been obtained. The Authorising Officer must give direction as to the handling of the product of the surveillance to both minimise collateral intrusion and ensure only relevant information is retained and only for as long as is necessary.

13. RECORDS

The Council must keep a detailed record of all provisional and judicially approved authorisations, reviews, renewals, cancellations and rejections in departments and a Central Register of all such forms will be maintained and contain the following information:

(a) a central register reference number for each authorisation

(b) a unique reference number for the authorisation (URN) - this is usually the investigation or operation case reference

(c) the type of authorisation or notice

(d) the date the provisional authorisation or notice was given;

(e) name and rank/grade of the Authorising Officer;

(f) whether the investigation or operation is likely to result in obtaining confidential information;

(g) whether the provisional authorisation was granted by an individual directly involved in the investigation;

(h) the date that judicial approval was received or refused;

(i) if the authorisation or notice is renewed, when it was provisionally renewed and who authorised the renewal, including the name and rank/grade of the Authorising Officer, and the date that judicial approval was obtained;

(j) the date the authorisation or notice was cancelled;

(k) the outcomes of the use of the powers.

(l) retention, review and disposal cycle

(m) reviews of authorisation

(n) Magistrates actions

The record will be made available to the relevant Commissioner or Inspector from the IPCO.

These records will be retained for a period of at least three years from the ending of the authorisation. A record will be kept of the dates on which the authorisation notice is started and cancelled.

13.1 Maintaining the Central Record of all Authorisations

The nominated officer shall hold and monitor the centrally retrievable record of all provisional and judicially approved authorisations.

Applicants and Authorising Officers are responsible for notifying Legal Services of an authorisation whether approved or not within 1 week of the judicial approval, review, cancellation or rejection. They should also ensure that the original version of all applications, magistrates' approvals, reviews, renewals and cancellation forms are sent to the nominated officer.

Once an authorisation has been cancelled the applicant or Authorising Officer must notify Legal Services of the outcome of the use of the RIPA powers in relation to their investigation.

13.2 Records maintained in the Department

The Authorising Officer shall maintain the following documentation, which need not form part of the centrally retrievable record:

(a) a copy of the signed application and a copy of the provisional authorisation or notice if applicable together with a copy of any order of judicial approval or refusal, as well as any supplementary documentation and notification given by the Authorising Officer;

(b) a record of the period over which the surveillance has taken place;

(c) the frequency of reviews prescribed by the Authorising Officer;

(d) an original signed record of the result of each review of the authorisation or notice;

(e) a copy of the signed renewal of an authorisation or notice, together with the supporting documentation submitted when the renewal was requested;

(f) the date and time when any instruction was given by the Authorising Officer.

Each form must have a unique reference number that is provided at application stage by the litigation team. Rejected forms will also have URNs.

13.3 Other Record of Covert Human Intelligence Sources

Proper records must be kept of the authorisation and use of a source. An Authorising Officer must not grant a provisional authorisation for the use or conduct of a source unless he believes that there are arrangements in place for ensuring that there is, at all times, a person with the responsibility for maintaining a record of the use made of the source.

The records shall contain the following information:

(a) the identity of the source;

(b) the identity, where known, used by the source;

(c) any relevant investigating authority other than the Council;

(d) the means by which the source is referred to within each relevant investigating authority;

(e) any other significant information connected with the security and welfare of the source;

(f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;

(g) the date when, and the circumstances in which, the source was recruited;

(h) the identities of the persons who, in relation to the source;

i. hold day-to-day responsibility for dealing with the source and for the source's security and welfare

ii. have a general oversight of the use made of the source (not to be the person identified in (h)(i))

iii. have responsibility for maintaining a record of the use made of the source

(i) the periods during which those persons have discharged those responsibilities;

(j) the tasks given to the source and the demands made of him in relation to his activities as a source;

(k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

(l) the information obtained by the conduct or use of the source;

(m) any dissemination of information obtained in that way; and

(n) in the case of a source who is not an undercover 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 source's activities for the benefit of that or any other relevant investigating authority.

13.4 Checks on the Integrity of the Process

The nominated officer will carry out periodic reviews of forms, to quality check they are being completed correctly and sufficiently.

14. RETENTION AND DESTRUCTION

Material obtained from properly authorised surveillance or a source may be used in other investigations. Arrangements shall be in place for the handling, storage and destruction of material obtained from covert surveillance, a source or the obtaining or disclosure of communications data. Authorising Officers must ensure compliance with the appropriate data protection requirements and any relevant Corporate Procedures relating to the handling and storage of material.

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

15. CONSEQUENCES OF IGNORING RIPA

RIPA states that if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it shall be lawful for all purposes.

Where there is interference with the right to respect for private and family life, guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority, the consequence of not obtaining an

authorisation under RIPA may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

Officers shall seek an authorisation where the directed surveillance, the use of a source or the obtaining or disclosure of communications data 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.

Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse.

16. SCRUTINY OF INVESTIGATORY BODIES

IPCO has been established under RIPA to facilitate independent scrutiny of the use of RIPA powers by the investigatory bodies that are subject to it. The Commissioner will inspect Councils to ensure compliance with RIPA and can audit/review the Council's policies and procedures, and individual authorisations.

There is also a statutory complaints system. The Investigatory Powers Tribunal has been established under RIPA to deal with complaints from members of the public about the use or conduct by public authorities of these powers. The Tribunal is separate from the IPCO. The Council expects its officers to co-operate fully with these statutory bodies and to bring forward any proposals for improvement that may follow on from an inspection report or a Tribunal hearing.

IF IN DOUBT ADVICE MUST BE SOUGHT FROM THE SRO OR LEGAL SERVICES.

APPENDIX 1

DIRECTED SURVEILLANCE

Authorisation will be required for a proposed activity if the answer is 'Yes' to all of the following questions.

If the answer is 'No' to any of the following questions, the proposed activity will not be entitled to protection under RIPA and authorisation will not be granted so should not be the subject of an application request.

(1) **Is the proposed activity 'surveillance'?** The officer must decide whether the proposed activity will comprise monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications, recording anything monitored, observed or listened to in the course of the proposed activity and whether a surveillance device will be used.

(2) **Is it 'covert'?** The officer must decide whether the proposed activity will be carried out in a manner calculated to ensure that the target(s) will be unaware that it is or may be taking place.

(3) **Is it 'directed'?** The officer must decide whether the proposed activity is for the purposes of a specific investigation/operation.

(4) **Is it likely to result in obtaining private information about a person? The** officer must decide whether any private information is *likely* to be obtained. Private information includes any information a person's private or family life and, as detailed above, this may cover information of a professional or business nature. This test is different from: "Is there the faintest chance that I will obtain private information?"

(5) **Is it a foreseen/planned response'?** The officer must decide whether the **proposed** activity is something other than an immediate response in circumstances where it is not reasonably practicable to get authorisation. If the proposed activity has been planned in advance and not just the immediate reaction to events happening in the course of the officer's work, it is not unforeseen and requires authorisation if all the answers to questions 1 to 4 have also been 'Yes'.

(6) **Is it proportionate?** The officer must believe the surveillance is proportionate to what it seeks to achieve. In making this judgement the officer will consider whether the information can be obtained using other less invasive methods and whether efforts are being made to reduce the impact of the surveillance on other people who are not the subject of the operation. Authorisation will not be granted if the method of investigation is excessive by relation to the seriousness of the crime that is being investigated.

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 as 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 other less intrusive means.

The Authorising Officer will not grant an authority unless he believes that obtaining the data in question by the conduct authorised or required by the authorisation is proportionate to what is sought to be achieved by so doing. Is what might be discovered important enough to warrant this level of invasion? The action being authorised should bring expected benefits to the investigation or operation and should not be disproportionate or arbitrary.

Officers must consider the following elements of proportionality:

1. balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;

2. explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;

3. 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;

4. evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

The Authorising Officer must balance the benefits of undertaking the investigation in the manner proposed for the public at large with the potential invasion of any person's privacy and detrimental impact this may have upon any person. The term "proportionate" is used here in the context of the Human Rights Act which requires interference with a human right to kept to the absolute minimum. Where there is interference it should be measured against the desired outcome. Interference with human rights is only acceptable where the matter being investigated is significant and it is in the public interest to achieve an outcome.

Covert Surveillance may in many cases involve the possibility of collateral intrusion. Authorising officers must consider whether the surveillance being authorised is undertaken with the least impact upon others who are not, or will not be, the subject of the investigation.

(7) The Authorising Officer when deciding if the conduct is necessary should assess if there are overt methods of obtaining the same information for the purposes of preventing or detecting crime or of preventing disorder

(8) Is the information Confidential? Authorising Officers must also assess the extent to which confidential information about the subject will come into the Authority's possession as a result of the investigation. Such information may be relevant to the investigation but protected for example as a result of legal professional privilege or it may be irrelevant but sensitive information for example medical records. Deliberately obtaining (or the use of) confidential information may only be authorised by the **Chief Executive**.

The Authorising Officer must therefore be satisfied that the conduct so authorised is necessary in pursuit of a legitimate aim (no 7 above); fulfils a pressing social need and is proportionate to that aim.

APPENDIX 2

ISLE OF WIGHT COUNCIL

NON-RIPA SURVEILLANCE FORM

Reference Number	

Authority (name and address)	Isle of Wight Council County Hall Newport Isle of Wight

Senior Manager authorising (name and address)	

Investigating/surveillance officer (name and job title)	

Describe the purpose of the investigation and include the operation number (if applicable)
Briefly outline the nature of the matter and what would the benefit of surveillance would be at this stage

Describe the type of surveillance including if equipment to be used (eg camera, video recorder including make and model number), what social media platforms may be used and how it may be reviewed and the expected duration

Identity of the subject of the surveillance (name and address and DoB (if known))	

Explain why the surveillance is necessary
Explain why it is considered that surveillance is necessary ie because there are no other alternative overt means of checking the situation.

Explain why the surveillance is proportionate to what it seeks to achieve
It is considered that surveillance is: • Proportionate in view of the allegations or information relating to the subject, potential value of any claim and the limited scope, duration and nature of the surveillance proposed (see above); • Safeguards will be put in place to minimise the potential of any excessive or disproportionate intrusion into the subject's privacy.

Give details of any potential/collateral intrusion ie how intrusive might the surveillance be on persons other than the subject of the surveillance and the steps taken to minimise this risk

Signed - Applicant		**Date**	

Signed – Senior Manager		**Date**	