COVERT SURVEILLANCE

REGULATION OF INVESTIGATORY POWERS ACT 2000

(PART II)

(Directed Surveillance and the use of CHIS)

POLICY & PROCEDURE

CONTENTS

INTRODUCTION AND PURPOSE

Introduction

Since October 2000 when the Human Rights Act 1998 came into force, covert surveillance has become subject to statutory control in the UK. The Regulation of Investigatory Powers Act 2000 (RIPA) provides for the first time a legal framework for covert surveillance activities by public authorities (including local authorities). This was overseen by the Office of Surveillance Commissioners (OSC). However, from 1 Sept 2017 oversight is provided by the Investigatory Powers Commissioner's Office (IPCO) which has been set up as an independent inspection regime to monitor Investigatory Powers which relate to covert activity currently under RIPA. This also includes the accessing of communications data (not contained in this policy).

This document may still make reference to the OSC where quoting their current guidance.

The use of surveillance (both overt and covert) to provide information is a valuable resource for the protection of the public and the maintenance of law and order. To discharge their responsibilities local authorities and law enforcement agencies use unaided surveillance and surveillance devices. RIPA and the codes of practice provide~~s~~ a legal framework and procedure to authorise the use of covert surveillance. Surveillance is covert if it is carried out in a manner that is calculated to ensure that persons who are subject to it are unaware that it is or may be taking place.

In some circumstances, it may be necessary for Council employees, in the course of their duties, to make observations of a person(s) in a covert manner. By their nature, actions of this sort may constitute an interference with that person's right to privacy. This may give rise to legal challenge as a potential breach of “the right to respect for private and family life, home and correspondence" under Article 8 of the European Convention on Human Rights and the Human Rights Act 1998. RIPA provides a procedure to defend the Council against such challenges

Purpose

This policy statement explains how Huntingdonshire District Council will meet legal requirements in relation to the use of covert surveillance. It also seeks to encourage and promote a professional approach in undertaking surveillance so that those affected may have confidence that the Council will act effectively and in a fair and lawful manner. It should be read in conjunction with the Regulation of Investigatory Powers Act 2000 and the

current version of the Code of Practice on the use of Covert Human Intelligence sources and the Code of Practice on Covert Surveillance on the Home Office website:
https://www.gov.uk/government/collections/ripa-codes

STATEMENT OF INTENT

This policy statement applies only to the use of covert surveillance, although it is expected that usually any surveillance activity undertaken by or on behalf the Council will be **overt**.

The RIPA procedure **does not** apply to:

- Covert observations where private information will not be obtained
- Observations that are not carried out covertly, or
- Ad-hoc covert observations that do not involve the systematic surveillance of a specific person(s) such as generally patrolling an area in response to complaints
- Unplanned observations made as an immediate response to events.

The Council intends to fulfil its lawful obligations and use directed surveillance and covert human intelligence sources within the terms of the Regulation of Investigatory Powers Act 2000, the relevant Codes of Practice and the current directions which were issued by the OSC in accordance with its lawful requirements.

The Council will keep its policy and procedures under review and update them as necessary and in accordance with any changes in the Law.

The Council will take necessary steps to ensure that employees whose duties involve investigations or supervision of them are informed of all relevant policy standards, procedures, and legislation.

Employees have a duty to follow this policy and its procedures and any employees knowingly acting outside this policy may be subject to the Council's disciplinary procedures.

All information gathered by surveillance is likely to be classed as Personal Data under the Data Protection Act and therefore has to be managed within that legislation and in accordance with the Council's Document Retention Policy. Therefore, it should be treated as confidential and only disclosed to persons (internal and external) whose authority has been explicitly established and meet the DPA requirements. Employees will be held responsible for any misuse, security breach or unauthorised disclosure while it is in their control.

Documents created as part of surveillance applications including authorisations, reviews and cancellations will be held on the councils Central Register which will be maintained by the RIPA Central Monitoring Officer. They will be held for five years. As per the current guidance.

A reporting structure will be established headed by the RIPA Central Monitoring Officer with a liaison officer for each service division so:

- that authorisation, Judicial application/order form, review, renewal and cancellation forms and procedures are co-ordinated and consistent across the Council and comply with legislation
- All documents are available for inspection by the Investigatory Powers Commissioner's Office (IPCO)
- All problems can be investigated thoroughly

Regular meetings are held, at least once every six months, with the liaison officers to review and update service divisions on changes in the law or Home Office guidance.

Subjects of covert surveillance carried out by or on behalf of the Council therefore can be assured that evidence collected (including personal data) will be processed with care and strictly in accordance with the law.

The Council has no lawful authority to **carry out intrusive surveillance** within the meaning of the Regulation of Investigatory Powers Act 2000. This is covert surveillance carried out in relation to anything taking place on any residential premises or in any private vehicle; and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device capable of providing 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 Council will seek to adhere to the authorisation, review, renewal and cancellation procedure provided for by the RIPA legislation and the codes of practice thereon before conducting any covert surveillance.

The Council will not intentionally gather evidence by covert surveillance from individuals where it is disproportionate or unnecessary in relation to the purposes of the investigation.

Surveillance carried out by a third party on behalf of the Council shall be subject to a contract which stipulates compliance with the law and this policy. Any service that intends to instruct a third party are required to liaise with the Central Monitoring Officer so that an

Authorising Officer can take into account the capability of an agent acting for the Council before any contracts are agreed.

Internal Oversight

To assist with oversight of the Council's RIPA processes, it has appointed Oliver Morley (Director of Services) as the Senior Responsible Officer (SRO) who will be responsible for the integrity of the process. However it must be stressed that all staff involved in the process must take their responsibilities seriously which will assist with the integrity of the Councils processes and procedures.

Lawful purposes

On 1 November 2012 two significant changes came into force that effects how local authorities use RIPA.

1. Approval **by a Justice of the Peace for** Local Authority Authorisations under RIPA The amendments in the Protection of Freedoms Act 2012 mean that local authority authorisations under RIPA for the use of Directed Surveillance or use of Covert Human Intelligence sources (CHIS) can only be given effect once an order approving the authorisation has been granted by a Justice of the Peace (JP). This applies to applications and renewals only, not reviews and cancellations.

1. **Directed surveillance crime threshold**: Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that a local authority can now only grant an authorisation under RIPA for the use of **Directed Surveillance** where the local authority is investigating criminal offences which attract a custodial sentence of a maximum term of at least 6 months' imprisonment, or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

The RIPA authorisation process can only be used for in connection with the Council's core functions.

The crime threshold, as mentioned is only for Directed Surveillance.

As from 1 November 2012 there is no provision for a Local Authority to use RIPA to conduct covert activities for disorder such as anti-social behaviour unless there are criminal offences involved which attract a maximum custodial sentence of six months.

Employees carrying out covert surveillance as far as practicable shall not interfere with any property or harass any person.

Confidential material

Applications where a significant risk of acquiring confidential material has been identified shall always require the approval of the Head of Paid Service.

Confidential material consists of :

- matters subject to legal privilege (e.g. between professional legal advisor and client)
- confidential personal information (e.g. relating to a person's spiritual, physical or mental health) or
- confidential journalistic material

DEFINITIONS

Unless the context otherwise requires, in this document the expressions in the first column shall have the meaning in the second column and any reference to a statute or statutory instrument or code of practice within the document shall include amendments to it.

Authorising Officer	means a person entitled to give an authorisation for directed surveillance or for the use of a covert human intelligence source in accordance with Section 30 of the Regulation of Investigatory Powers Act 2000 and the Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) Order 2000 SI No. 2417 as adapted to the organisational structure of the Council and who is included in the list of officers designated by the Council for such purposes.
Council	means Huntingdonshire District Council
Surveillance	is defined in Section 48 of the Regulation of Investigatory Powers Act 2000 and includes :

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

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

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

* surveillance does not include references to :

a) any conduct of a covert human intelligence source for obtaining or recording (whether or not using a surveillance device) any information which is disclosed in the presence of the source;

b) the use of a covert human intelligence source for so obtaining or recording information; or

c) any such entry on or interference with property or with wireless telegraphy as would be unlawful unless authorised under Section 5 of the Intelligence Services Act 1994 (warrants for the intelligence services) or Part III of the Police Act 1997 (powers of the police and of customs officers)

Covert Surveillance means surveillance carried out in a manner that is calculated to ensure that persons who are subject to this surveillance are unaware that it is or may be taking place

Directed Surveillance means covert surveillance which is not intrusive and is undertaken :

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

b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one 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 under Part II of RIPA to be sought for the carrying out of surveillance

Intrusive Surveillance

Intrusive surveillance is defined in section 26(3) of the 2000 Act as covert surveillance that:

a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and
b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

Where surveillance is carried out in relation to anything taking place on any residential premises or in any private vehicle by means of a device, without that device being present on the premises, or in the vehicle, it is not intrusive unless the device 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.

Private Information

Private information includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships.

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of *private information*. This is likely to be the

	case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a *public authority* of that person's activities for future consideration or analysis. Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute *private information* even if individual records do not. Where such conduct includes surveillance, a directed surveillance *authorisation* may be considered appropriate.
Private Vehicle	means any vehicle that is used primarily for the private purpose of the person who owns it or of a person otherwise having the right to use it (except where the right to use the vehicle derives only from his having to pay, or undertake to pay for the use of the vehicle and its driver for a particular journey)
Residential Premises	means so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation (including hotel or prison accommodation that is so occupied or used)
Surveillance Device	means any apparatus designed or adapted for use in surveillance
Covert Human Intelligence Source	means a person who establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within Section 26(8)(b) or (c) Regulation of Investigatory Powers Act 2000 namely :

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

c) to covertly disclose information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship

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.

SCOPE OF PROCEDURE

The RIPA procedure **does not** apply to :

- Covert observations where private information will not be obtained
- Observations that are not carried out covertly, or
- Ad-hoc covert observations that do not involve the systematic surveillance of a specific person(s)
- Unplanned observations made as an immediate response to events.

should always remember that any actions taken must be justified and recorded.
In cases of doubt, the authorisation procedure described below should be followed.

AUTHORISATION PROCEDURE

General

As mentioned earlier on 1 November 2012 two significant changes came into force that effects how local authorities use RIPA.

1. **Approval of Local Authority Authorisations under RIPA by a Justice of the Peace**: The amendments in the Protection of Freedoms Act 2012 mean that local authority authorisations under RIPA for the use of Directed Surveillance or use of Covert Human Intelligence sources (CHIS) can only be given effect once an order approving the authorisation has been granted by a Justice of the Peace (JP). **This applies to applications and renewals only, not reviews and cancellations.**

2. **Directed surveillance crime threshold**: Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that a local authority can now only grant an authorisation under RIPA for the use of Directed Surveillance where the local authority is investigating criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

This crime threshold, as mentioned, is only for Directed Surveillance.

Application, Review, Renewal and Cancellation procedure

No covert activity covered by RIPA or the use of a CHIS should be undertaken at any time unless it meets the legal criteria (see above) and has been authorised by an Authorising Officer and approved by a JP/Magistrate as mentioned above. The activity conducted must be in strict accordance with the terms of the authorisation.

All the forms, namely the Authorisation (this also contains the application section), Review, Renewal and Cancellation will be the Home Office Model approved forms downloaded from the Home Office Website and approved by the Council's RIPA Central Monitoring Officer. (See the List in the Annex).Forms should only be downloaded from the Home Office website : https://www.gov.uk/government/collections/ripa-forms--2

Home Office forms, codes of practice and supplementary material will be available through the Council Intranet, the RIPA Central Monitoring Officer and the Home Office Website: https://www.gov.uk/government/collections/ripa-codes

The effect of the above legislation means that all applications/authorisations and renewals for covert RIPA activity will have to have a JP's approval. It does not apply to Reviews and Cancellations which will still be carried out internally.

The procedure is as follows;

All applications and renewals for Directed Surveillance and use of a CHIS will be required to have a JP's approval as mentioned earlier.

Applications/Authorisations

All applications for directed surveillance authorisation will be made on **Form 1** (reference ***RIPA 1 DS authorising*** form) and will be in the first instance sent to the RIPA Coordinating

Officer- See **Gate Keeping Section**. The names and posts of such officers may be found recorded in a list held for that purpose by the RIPA Coordinating Officer (see the List in the Annex). Authorising Officers will be, as a minimum, Heads of Service. Any nomination of such an officer in that list empowers those officers in line above them to act in their place. Officers responsible for management of an investigation will normally be no lower than Activity Manager.

Authorising officers shall ensure they are fully aware of their responsibilities and comply with the requirements of the law including the relevant codes of practice, OSC procedures and Guidance information and the Council's policies and procedures in respect to the authorisation, review, renewal and cancellation of authorisations for covert surveillance. They shall ensure a satisfactory risk assessment, including the Health and Safety of staff is completed in respect of each authorisation.

Authorising Officers must record on the appropriate form the matters they took into account in reaching their decision and they must be satisfied that :

- **no overt means** are suitable for the purpose
- the authorisation is for a prescribed lawful purpose (see above)
- account has been taken of the likely degree of intrusion into the privacy of persons other than those directly implicated/targeted in the operation or investigation (**collateral intrusion**)
- measures are be taken, where ever practical, to avoid unnecessary intrusion into the lives of those affected by collateral intrusion.
- the authorisation is necessary.
- the authorised surveillance proposed is proportionate;
- any equipment to be used and its technical capabilities is specified

Necessity

Surveillance operations shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective(s).

Effectiveness

Surveillance operations shall be undertaken only by suitably trained or experienced employees (or under their direct supervision).

Proportionality

Explain why this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion

outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means?

The codes provide guidance relating to proportionality:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

Equipment

The technical capabilities of any equipment being used during the surveillance will need to be considered with regard to the privacy issues. This will impact on the proportionality test.

Authorisation

All directed surveillance shall be authorised in accordance with this procedure.

Where an application for authorisation is refused the Authorising Officer shall record the refusal on the application and the reasons for it on the case file and supply a copy of it to the RIPA Coordinating Officer as with other authorisations. The Authorising Officer shall also ensure that any supplementary information and supporting documents submitted with any application for authorisation, review, renewal or cancellation are recorded and retained on the case file as required by the codes of practice or other legal requirement.

Applicants or some other officer should complete a risk assessment prior to the completion of the application form. Each application should be completed on its own merits of the case. **Cutting and pasting or using template entries should not take place as this would leave the process open to challenge.**

Gate Keeping

The applicant will complete the relevant sections of the form with sufficient information for the Authorising Officer to consider Necessity, Proportionality and the Collateral Intrusion issues. All applications will then be submitted firstly to the RIPA Coordinating Officer for quality control prior to its submission to the Authorising Officer and would enable The Coordinating Officer to tender advice if required. It would then be submitted to the Authorising Officer and after grant or refusal of authorisation, should be referred back to the

Coordinating Officer when it may be further reviewed and arrangements made for a magistrates court attendance for approval. At each of these stages the central record can be updated and thereby remain current.

If authorised the Authorising Officer will complete the authoriation section of the form. The applicant will now complete the required section of the judicial application/order form. Although this form requires the applicant to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well.

Applications whether authorised or refused will be issued with a unique number by The Councils RIPA Coordinating Officer (Corporate Fraud Manager).
It will then be necessary within Office hours to arrange with Her Majesty's Courts & Tribunals Service (HMCTS) administration at the magistrates' court to arrange a hearing. The hearing will be in private and heard by a single JP.

The Authorising Officer will be required to present the application at these proceedings and will need to be formally designated by the Council under section 223 of the Local Government Act 1972 to appear, be sworn in and present evidence or provide information as required by the JP.

Upon attending the hearing, the Authorising Officer must present to the JP the partially completed judicial application/order form, a copy of the RIPA authorisation form, together with any supporting documents setting out the case, and the original authorisation form.

The original RIPA authorisation should be shown to the JP but will be retained by the local authority so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT).

The JP will read and consider the RIPA authorisation and the judicial application/order form. They may have questions to clarify points or require additional reassurance on particular matters. These questions are supplementary to the content of the application form**. However the forms and supporting papers must by themselves make the case. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported in the papers provided**.

The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition they must be satisfied that the person who granted the

authorisation or gave the notice was an appropriate designated person within the local authority and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

The JP may decide to

Approve the Grant or renewal of an authorisation
The grant or renewal of the RIPA authorisation will then take effect and the local authority may proceed to use the technique in that particular case.

Refuse to approve the grant or renewal of an authorisation
The RIPA authorisation will not take effect and the local authority may **not** use the technique in that case.

Where an application has been refused the applicant may wish to consider the reasons for that refusal. If more information was required by the JP to determine whether the authorisation has met the tests, and this is the reason for refusal the officer should consider whether they can reapply, for example, if there was information to support the application which was available to the local authority, but not included in the papers provided at the hearing.

For, a technical error, the form may be remedied without going through the internal authorisation process again. The officer may then wish to reapply for judicial approval once those steps have been taken.

Refuse to approve the grant or renewal and quash the authorisation
This applies where the JP refuses to approve the authorisation or renew the authorisation and decides to quash the original authorisation. The court must not exercise its power to quash the authorisation unless the applicant has had at least 2 business days from the date of the refusal in which to make representations. If this is the case the officer will inform the Legal section who will consider whether to make any representations.

Whatever the decision the JP will record their decision on the order section of the judicial application/order form. The court administration will retain a copy of the local authority RIPA authorisation form and the judicial application/order form. The officer will retain the original authorisation and a copy of the judicial application/order form.

If approved by the JP, the date of the approval becomes the commencement date and the three months duration will commence on this date. The officers are now allowed to undertake the activity.

The original RIPA authorisation form and the copy of the judicial application/order form should be forwarded to the RIPA Coordinating Officer so it can be entered onto the Central Register and a copy retained by the applicant and by the AO. This will enable the AO to check what was authorised and monitor any reviews and cancellation to determine if any errors occurred and if the objectives were met.

There is no complaint route for a judicial decision unless it was made in bad faith. If the applicant has any issues they must contact the Legal Department for advice. A local authority may only appeal a JP decision on a point of law by Judicial Review. If such a concern arises, the Legal team will decide what action if any should be taken.

Reviews

The reviews are dealt with internally by submitting the review form to the authorising officer. There is no requirement for a review form to be submitted to a JP.

All applications for review of directed surveillance authorisation will be made on **Form 2** (reference ***RIPA 2 DS review*** form**)**.

Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

In each case the Authorising Officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable and they will record when they are to take place on the application form. This decision will be based on the circumstances of each application. Reviews will be conducted on a monthly or less basis to ensure that the activity is managed. It will be important for the Authorising Officer to be aware of when reviews are required following an authorisation to ensure that the applicants submit the review form on time.

Applicants should submit a review form by the review date set by the Authorising Officer. They should also use a review form for changes in circumstances to the original application so that the need to continue the activity can be reassessed. However if the circumstances or the objectives have changed considerably or the techniques to be used are completely different, a new application form may be required to be submitted. If this is the case the procedure to be followed is the same for the initial If in doubt seek advice... The applicant does not have to wait until the review date if it is being submitted for a change in circumstances.

Managers or Team Leaders of applicants should also make themselves aware of when the reviews are required to ensure that the relevant forms are completed on time.

Renewal

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. Should it be necessary to renew a Directed Surveillance or CHIS authorisation this must be approved by a JP

All applications for directed surveillance renewals will be made on **Form 3** (reference ***RIPA 3 DS* renewal** form).

Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the applicant must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant authorising officer and a JP to consider the application).

The applicant should complete all the sections within the renewal form and submit the form to the authorising officer.

Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

If the authorising officer refuses to renew the application the cancellation process should be completed. If the AO authorises the renewal of the activity the same process is to be followed as mentioned earlier for the initial application.

A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

Cancellation

Where authorisation ceases to be either necessary or proportionate the Authorising Officer or appropriate deputy will cancel an authorisation using **Form 4** (reference ***RIPA 4 DS cancellation*** form). In reality this means that the objectives have been achieved or can't be achieved for whatever reason. **DO NOT WAIT UNTIL THE 3 MONTHLY DATE. IT SHOULD BE CANCELLED IMMEDIATELY.**

The cancellation form is to be submitted by the applicant or another investigator in their absence. The Authorising Officer who granted or last renewed the authorisation must cancel it if they are satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. 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

As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the central record of authorisations (see paragraphs 5.18 in the Codes of Practice). **It will also be necessary to detail the amount of time spent on the surveillance .**

The officer submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and what if any images were obtained and any images containing third parties. The Authorising Officer should then take this into account and issue instructions regarding the management and disposal of the images etc.

The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what they stated was necessary in the application form. This check will form part of the oversight function. Where issues are identified they will be brought to the attention of the line manager and the Senior Responsible Officer (SRO). This will assist with future audits and oversight.

Immediate response to events

There may be occasions when officers come across events unfolding which were not pre planned which then requires them to carry out some form of observation. This will not amount to Directed Surveillance. Officers must not abuse the process and be prepared to explain their decisions in court should it be necessary. Therefore they should document their decisions, what took place, what evidence or information was obtained.

Joint Agency Surveillance

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

Council employees on behalf of the Police, authorisation would be sought by the police. If it is a joint operation involving both agencies the lead agency should seek authorisation.

Council staff involved with joint agency surveillance are to ensure that all parties taking part are authorised on the application to carry out the activity. When staff are operating on another organisation's authorisation they are to ensure they see what activity they are authorised to carry out and make a written record. They should obtain a copy of the authorisation page which should contain the unique number, a copy of which should be forwarded to The RIPA Central Monitoring Officer for filing so that the total amount of Surveillance by Council staff can be recorded. They should also inform the RIPA Central Monitoring Officer of the agencies involved and the name of the officer in charge of the surveillance. This will assist with oversight of the use of Council staff carrying out these types of operations.

Documentation and Central Record

Authorising Officers or Managers of relevant enforcement departments may keep whatever records they see fit to administer and manage the RIPA application process. This will not replace the requirements under the Codes of Practice for the Council to hold a centrally held and retrievable record.

A centrally retrievable record of all authorisations will be held by the RIPA Coordinating Officer and updated whenever an authorisation is refused, granted, renewed or cancelled. The record will be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners, upon request. These records should be retained for at least five years from the ending of the authorisation or for the period stipulated by the Council's document retention policy, whichever is greater.

Use of CCTV

The use of the CCTV systems operated by the Council do not normally fall under the RIPA regulations. However it does fall under the Data Protection Act 1998 and the Council's CCTV policy**.** Should there be a requirement for the CCTV cameras to be used for a specific purpose to conduct surveillance it is likely that the activity will fall under Directed Surveillance and therefore require an authorisation.

On the occasions when the CCTV cameras are to be used in a Directed Surveillance situation either by enforcement officers from relevant departments within the Council or outside Law Enforcement Agencies such as the Police, either the CCTV staff are to have a copy of the application form in a redacted format, or a copy of the authorisation page. If it is an urgent oral authority, a copy of the applicant's notes are to be retained or at least some other document in writing which confirms the authorisation and exactly what has been

authorised. It is important that the staff check the authority and only carry out what is authorised. A copy of the application or notes is also to be forwarded to the Central Monitoring Officer for filing. This will assist the Council to evaluate the authorisations and assist with oversight.

Operators of the Councils CCTV system need to be aware of the RIPA issues associated with using CCTV and that continued, prolonged systematic surveillance of an individual may require an authorisation.

The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what they stated was necessary in the application form. This check will form part of the oversight function. Where issues are identified they will be brought to the attention of the line manager and the Senior Responsible Officer (SRO). This will assist with future audits and oversight.

Use of a Covert Human Intelligence Source (CHIS)

The use of CHIS should only be considered in exceptional cases and after consulting the Legal Section to ensure it is appropriate and all safeguards needed are in place. If authorised a CHIS authorisation lasts for 12 months before a renewal would be required.

Proper records must be kept of the authorisation and use of a source as required by the Regulation 3 of the Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI no 2725) namely :

a) the identity of the source;

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

c) any relevant investigating authority other than the authority maintaining the records;

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 (e) 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, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);

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 each relevant investigating authority by the conduct or use of the source;

m) any dissemination by that authority 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 or the source's activities for the benefit of that or any other relevant investigating authority.

In addition the Code of Practice requires records to be kept of:

- a copy of the authorisation together with the supporting documentation and notification of the approval given by the authorising officer;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the reason why the person renewing an authorisation considered it necessary to do so;
- any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
- any risk assessment made in relation to the source;
- the circumstances in which tasks were given to the source;
- the value of the source to the investigating authority;
- a record of the results of any reviews of the authorisation;
- the reasons, if any, for not renewing an authorisation;
- the reasons for cancelling an authorisation;
- the date and time when any instruction was given by the authorising officer to cease using a source.

Authorising Officers must not grant an authorisation for a CHIS unless they believe that there are arrangements in place to ensure there is at all times a person responsible for maintaining a record of the use of that source.

All applications for authorisation for the use or conduct of a CHIS will be made on **Form 5** (reference ***RIPA 5 CHIS authorising*** form). The applicant in all cases should complete this.

The application process is the same as described earlier with the authorisation (if authorised) requiring the approval of a Justice of the Peace.

All applications for review of authorisation for the use or conduct of a CHIS will be made on **Form 6** (reference ***RIPA 6 CHIS review*** form). The applicant in all cases should complete this where the investigation/operation is to be continued.

All applications for authorisation for the use or conduct of a CHIS renewal will be made on **Form 7** (reference ***RIPA 7 CHIS renewal*** form). The applicant in all cases should complete this where the surveillance requires to continue beyond the previously authorised period (including previous renewal). The renewal will require approval of a Justice of the Peace and lasts for a further 12 months.

Where authorisation ceases to be either necessary or appropriate the Authorising Officer or appropriate deputy will cancel an authorisation using **Form 8** (reference ***RIPA 8 CHIS cancellation*** form).

Any person giving an authorisation for the use of CHIS must record on the appropriate form matters taken into account in reaching their decision and must be satisfied that :

- **no overt means** are suitable for the purpose
- the authorisation is for a prescribed lawful purpose (see above)
- account has been taken of the likely degree of intrusion into the privacy of persons other than those directly implicated/targeted in the operation or investigation (**collateral intrusion**)
- measures must be taken, where ever practical, to avoid unnecessary intrusion into the lives of those affected by collateral intrusion.
- the authorisation is necessary.
- the authorised surveillance proposed is proportionate;
- any equipment to be used is specified

Necessity

Surveillance operations shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective(s).

Effectiveness

Surveillance operations shall be undertaken only by suitably trained or experienced employees (or under their direct supervision).

Proportionality

The use of surveillance shall not be excessive but shall be in proportion to the significance/harm of the matter being investigated. (i.e. don't use a sledge hammer to crack a nut).

Authorisation

All directed surveillance shall be authorised in accordance with this procedure.

Persons who repeatedly provide information

It is possible that members of the public repeatedly supply information to Council staff on either one particular subject or investigation or a number of investigations. It is important that Council staff make the necessary enquiries with the person reporting the information to ascertain how the information is being obtained. This will not only assist with evaluating the information but will determine if the person is establishing or maintaining a relationship with a third person to obtain the information, and then provide it to the Council staff. If this is the case, the person is likely to be acting as a CHIS and there is a potential duty of care to the individual which a duly authorised CHIS would take account of. Therefore Council staff should ensure that they are aware of when a person is potentially a CHIS by reading the above sections.

DURATION TIME OF AUTHORISATIONS

Directed Surveillance	3 Months
Renewal	3 Months
Covert Human Intelligence Source	12 Months
Renewal	12 months
Juvenile Sources	1 Month

All authorisations commence from the date approved by the Justice of the PEACE.

All Authorisations must be cancelled by completing a cancellation form. They must not be left to simply expire.

Surveillance outside of RIPA

As a result of the change in the law from the 1st November 2012 Directed Surveillance under RIPA will only apply to the detection and prevention of a criminal offence that attracts a penalty of 6 months imprisonment or more or relate to the sale of alcohol or tobacco to children. This essentially takes out surveillance of a lot of offences that the Council may investigate such as disorder (unless it has 6 months custodial sentence) and most summary offences such as littering, dog fouling etc.

This change does not mean that our enforcement officers cannot undertake such surveillance, but because it is **not now** regulated by the Office of Surveillance Commissioners, they have placed the responsibility to regularly monitor this type of activity on the Councils Senior Responsible Officer (SRO). As a result we need procedures in place to ensure that we can prove that we have given due consideration to necessity and proportionality which are central tenets of European Law and the likely grounds of any challenge that we may receive.

If it is necessary for the Council to undertake surveillance which does not meet the criteria to use the RIPA legislation, such as in cases of disciplinary investigations against staff or surveillance relating to Anti-Social Behavior appertaining to disorder, the Council must still meet its obligations under the Human Rights Act and be able to demonstrate that its actions to breach someone's article 8 rights to privacy are necessary and proportionate, which includes taking account of the intrusion issues. To demonstrate this accountability, the decision making process and the management of such surveillance must be documented. Therefore should staff have a requirement to undertake a covert surveillance which would meet the test of Directed Surveillance save for the fact that it does not meet the legal criteria relating to a criminal offence which have a sentence of 6 months imprisonment, or relate to the sale of alcohol and tobacco to children they should complete the Non RIPA Surveillance form and submit it to one of the RIPA Authorising Officers listed within this policy to be considered for authorisation before any activity can be undertaken. There will be no requirement to have the authorisation approved by a Justice of the Peace. Should the activity be approved the procedures to be followed will be the same as any RIPA authorised activity. Therefore the Council expects that the procedure and management from the initial surveillance assessment, through to completion and cancellation to be managed appropriately at the same level that the RIPA legislation and guidance requires. For further advice contact the RIPA central Monitoring Officer Loraine Martin.

Using the Internet to Conduct Online Covert Activity

The internet is a useful investigative tool, giving access to a large amount of information which could not otherwise be obtained. The techniques and websites used change frequently and so it is difficult for definitive guidance to be written by the OSC as, by the time it is published, it may be obsolete. There is also a lack of definitive case law in this area.

However, there is no doubt that these types of enquiries pose a risk to the council for breaches of privacy and non-compliance with RIPA.

The codes of practice at 2.29 now provide guidance regarding the use of the internet to conduct covert enquiries. Therefore, the guidance provided in the codes of practice have been replicated in full to avoid confusion.

The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. Whenever a public authority intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought as set out elsewhere in this Code. Where an investigator may need to communicate covertly online, for example contacting individuals using social media websites, a CHIS authorisation should be considered.

Officers may find the following rule of thumb guidance helpful:

> *Access to open source material does not require a RIPA authorisation unless there are repeated visits to the same site. These normally occur when an attempt is being made to build a profile of the account operator. In that case directed surveillance authorisation **is** required. If the privacy controls are breached (eg. By becoming a "friend"), and a pseudo account is used, ensuring that the officer's identity as a council employee is hidden, then at least directed surveillance authorisation **will** be required. If direct contact is made with the account owner/operator and a relationship commences CHIS authorisation will be required. In the latter case it is a statutory requirement of RIPA that a controller, handler and record keeper are appointed to manage the operation and a risk assessment is created.*

Previous OSC guidance has stated that a computer is a surveillance device and have issued specific guidance regarding these types of enquiries.

If it does not meet the Directed Surveillance criteria, it is essential that detailed notes be made by any officer viewing material on the internet explaining what they were seeking, why it was necessary and proportionate to do so and why prior authorisation was not sought. Where material is printed or saved, consideration must be given to the management of the material as it is likely to contain private information about individuals not the subject of the enquiry.

There is other guidance available issued by the OSC which can be provided should staff require additional information.

RECORD KEEPING, TRAINING AND MONITORING

Security and Retention of Records

Each service division or discrete location within a division, must maintain a record of all applications for authorisations (including refusals), Judicial application/order form, renewals, reviews and cancellations on the appropriate form. Each individual form must be given a unique reference number issued by the RIPA Central Monitoring Officer. Such unique reference numbers should follow on in sequential order from that used for previous forms. The Authorising Officer in that service division or that location may maintain records for directed surveillance and covert human intelligence sources for their own records.

The Authorising Officer shall retain together the original authorisation, copy of the Judicial application/order form, review and renewal forms, copies being provided to the Central Monitoring Officer, until cancelled. On cancellation, the original application, review, renewal and cancellation forms and any associated documents shall be sent to the Central Monitoring Officer and retained in a file in a secure place for five years after cancellation, as required by the Act.

The codes do not affect any other statutory obligations placed on the Council to keep records under any other enactment such as the Criminal Procedure and Investigations Act 1996 (CPIA) This requires that material which is obtained in the course of an investigation and which may be relevant to the investigation must be recorded, retained and revealed to the prosecutor.

Training

The Senior Responsible Officer will have responsibility for ensuring appropriate training for staff mentioned within this policy and for retaining a record of that training. They must supply a copy of the record to the RIPA Cordinating Officer at regular intervals. Refresher training for both applicants and Authorised Officers will be conducted at 18 monthly intervals and additional training for designated CHIS handlers at the same frequency.

Central Register

The RIPA Coordinating Officer will maintain the Central Register of Authorisations. Authorising Officers shall notify the RIPA Coordinating Officer within 48 hours of the grant, renewal or cancellation of any authorisation and the name of the applicant officer to ensure the accuracy of the central register.

Errors

There is a requirement to report all covert activity that was not properly authorised to IPCO in writing as soon as the error is recognised. An initial e-mail alerting IPCO should be followed by a report from the SRO detailing the circumstances and remedial action taken. An error includes activity which should have been authorised but wasn't or which was conducted beyond the directions provided by the authorising officer. It is therefore important that when an error has been identified it is brought to the attention of the SRO in order to comply with this guidance. The Council has a responsibility to report to the Inspector at the commencement of an inspection all activity which should have been authorised but wasn't. This is to confirm that any direction provided by the Chief Surveillance Commissioner has been followed. This will also assist with the oversight provisions of the Councils' RIPA activity.

This does not apply to covert activity which is deliberately not authorised because an authorising officer considers that it does not meet the legislative criteria, but allows it to continue. This would be surveillance outside of RIPA. (See oversight section below)

Senior Responsible Officer

Overall oversight within the Council will fall within the responsibilities of the Senior Responsible Officer (SRO) for the Council. The SRO is responsible for:

- the integrity of the process in place within the *public authority* to authorise directed surveillance
- compliance with Part II of the 2000 Act, Part III of the 1997 Act and with this code;
- engagement with the Commissioners and inspectors when they conduct their inspections, and

where necessary, overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner

Reporting to Members Annual returns of all surveillance activity undertaken by Council staff including joint surveillance and Directed Surveillance using the CCTV system will be compiled by the RIPA Coordinating Officer and provided to the Corporate Governance Panel annually in line with the current advice in the Codes of Practice. Members will review on a yearly basis the policy to assess whether the activity undertaken is in line with this policy.

The Investigatory Powers Commissioner's Office

The Investigatory Powers Commissioner's Office provides an independent overview of the use of powers contained within the Regulation of Investigatory Powers Act 2000. This scrutiny includes inspection visits to local authorities by inspectors appointed by the IPCO

and the provision of annual reports by the Council to the IPCO on all relevant surveillance activity undertaken as part of this policy.

It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information he requires for the purpose of enabling him to carry out his functions.

The Investigatory Powers Commissioner's Office may be contacted at :

Investigatory Powers Commissioner's Office
PO Box 29105
London SW1V 1ZU
Telephone : 020 7035 8543
https://ipco.org.uk/

The Regulation of Investigatory Powers Act 2000 also establishes an independent tribunal, the **Investigatory Powers Tribunal**. This has full powers to investigate and decide any cases within its jurisdiction.

ADVICE

If you require further advice about covert surveillance, please contact the RIPA Central Monitoring Officer. In particular advice should be sought before considering the use of a covert human intelligence source where considerations of risk assessment, insurance, managing tasking the source and ensuring confidentiality require specific consideration.

POLICY UPDATING PROCEDURE

Proposed amendments to this Policy must be forwarded to the Head of Legal and Democratic Services be authorised to make any amendments to the policies in the future after consultation with the Chairman of the Corporate Governance Panel and subject to the matter being reported to the next meeting of the Corporate Governance Panel.

.

The Policy shall be reviewed annually as suggested in OSC guidance. This will enable the Council to ensure it remain up to date and fit for purpose.

FURTHER INFORMATION ENQUIRIES AND COMPLAINTS

The RIPA Coordinating Officer is the first point of contact on any of the matters raised in this policy statement. Enquiries should be addressed to:

The RIPA Coordinating Officer
Corporate Fraud Section
Huntingdonshire District Council
Pathfinder House
St Mary's Street
Huntingdon
Cambridgeshire
PE29 3TN
Tel : (01480) 388388 or direct dial (01480) 388861

The RIPA Coordinating Officer is the Council's Corporate Fraud Manager and will be responsible for dealing with all internal and external enquiries and complaints. All complaints should be in writing, dated and include details of the complaint and also an account of the nature of the problem.

The Council will attempt to complete internal investigations within 20 working days. An acknowledgement of the complaint should be despatched to the complainant as soon as possible after its receipt.

Loraine Martin
Corporate Fraud Manager
18.11.20

ANNEX A

HOME OFFICE MODEL FORMS

RIPA 1DS Authorising Form

RIPA 2DS Review Form

RIPA 3DS Renewal Form

RIPA 4DS Cancellation Form

RIPA 5CHIS Authorising Form

RIPA 6CHIS Review Form

RIPA 7CHIS Renewal Form

RIPA 8CHIS Cancellation Form

Note:
DS : Directed Surveillance
CHIS : Covert Human Intelligence Source

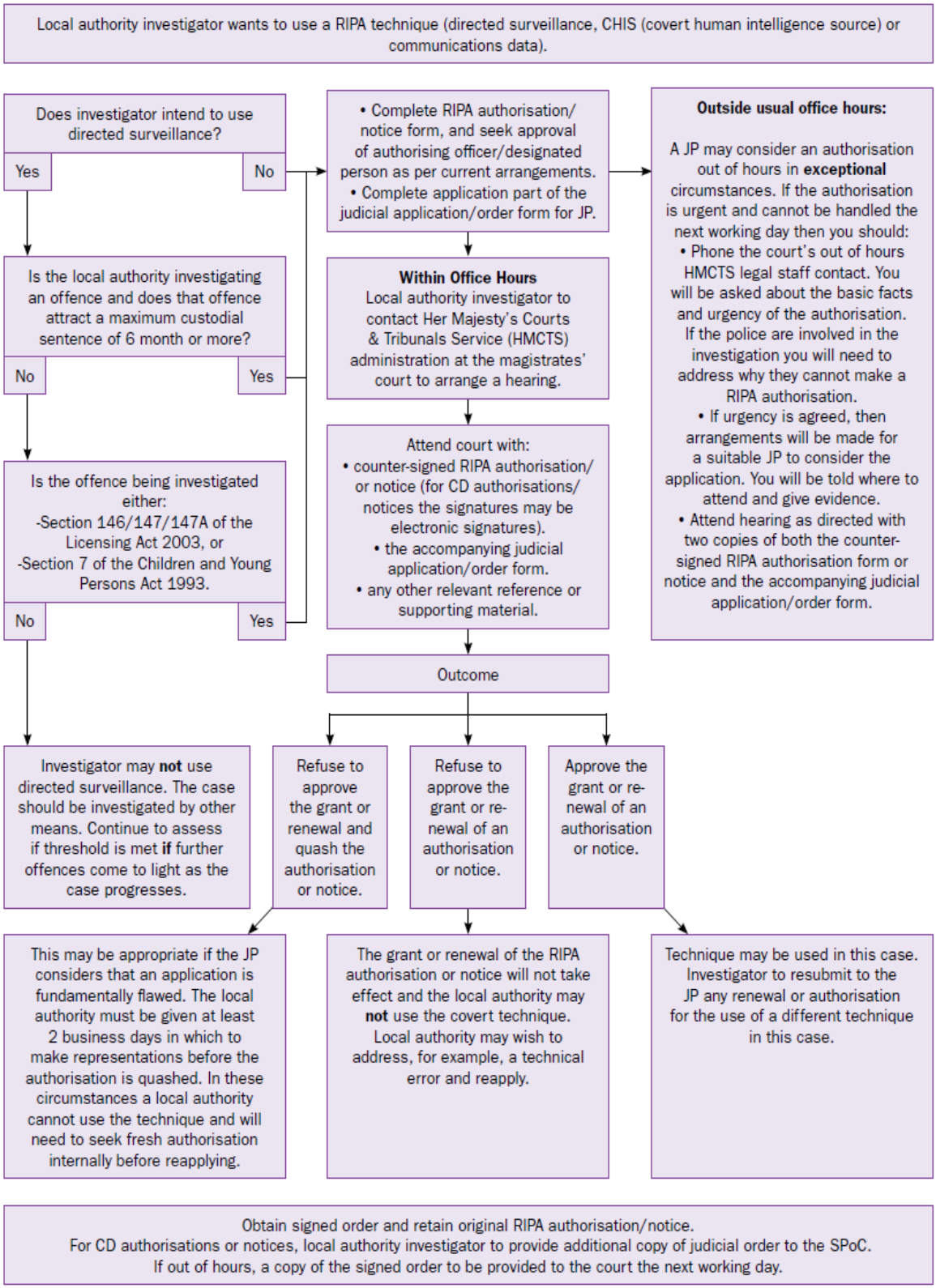
ANNEX B

LIST OF OFFICERS ROLES

ROLE	SERVICE	POST	POST HOLDER
Coordinating Officer	Council-wide	Fraud Manager	Loraine Martin
Senior Responsible Officer/authorising Officer	Council-Wide	Head of Operational Services	Oliver Morley
Senior Authorising Officer	Council-Wide	Chief Executive	Jo Lancaster
Authorising Officer	Customer Services	Head of Customer Service	Amanda Burns
Authorising Officer	Operations	Head of Operations	Neil Sloper
Authorising Officer	Customer Services, Planning, Communities	Chief Operating Officer	John Taylor

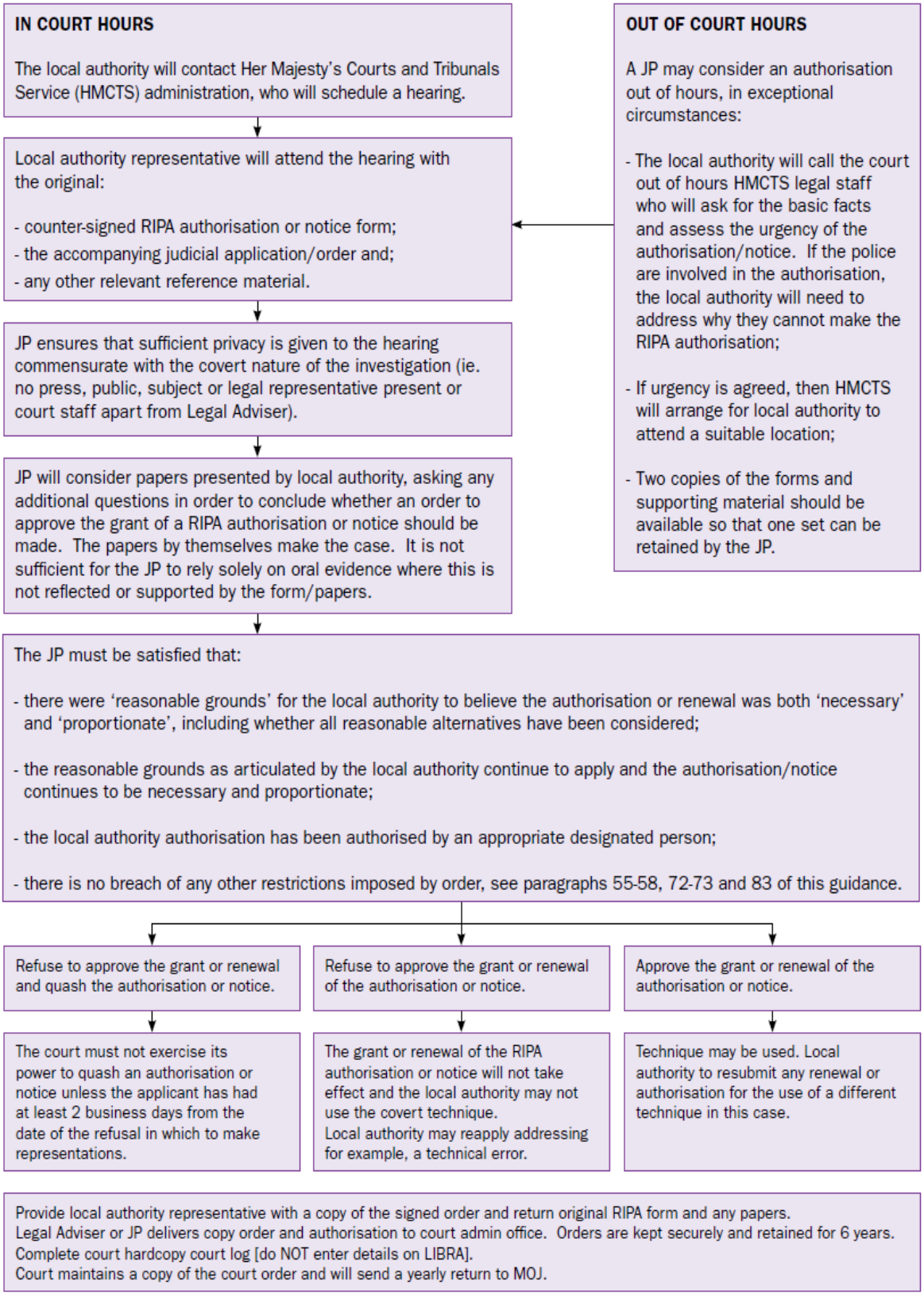
Annex C

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



Annex D

PROCEDURE: LOCAL AUTHORITY APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local thority:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of subject:.....

.....

.....

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

.....

.....

.....

.....

.....

.....

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer:.....

Authorising Officer/Designated Person:.....

Officer(s) appearing before JP:.....

Address of applicant department:.....

.....

Contact telephone number:.....

Contact email address (optional):.....

Local authority reference:.....

Number of pages:.....

Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Magistrates' court:.....

Having considered the application, I (tick one):

☐ am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

.....

.....

.....

.....

.....

Reasons

.....

.....

.....

.....

.....

.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court: