Appendix 1

REGULATION OF INVESTIGATORY POWERS ACT 2000

POLICY & PROCEDURES GUIDANCE

2018 - 2019

Version Control				
Document owner	Published on	Version	Changed on	Amended by
Trevor Kennett	16th January 2017	1.0	01/09/2017	Trevor Kennett
Trevor Kennett	1st September 2017	2.0		
Trevor Kennett	15th September 2017	3.0	15/09/2017	Trevor Kennett
Trevor Kennett	26 July 2018	4.0		Trevor Kennett

Contents

Section		Page
1A.	Introduction to RIPA 2000	3 – 4
1B.	Policy Summary	5
2.	Definitions	6 - 10
3.	The Use of a Covert Human Intelligence Source (CHIS)	11 - 16
4.	Authorisation of Surveillance & Non-RIPA applications	17 - 27
5.	Social Media	27
6.	Complaints	28

Appendix	Appendix content
1	Standard Form – Surveillance Application
2	Standard Forms – Surveillance Renewal
3	Standard Forms – Surveillance Cancellation
4	Standard Forms – Monthly Review
5a	Flow Chart - Authorisation Procedures - General
5b	Flow Chart - Authorisation Procedures - Directed Surveillance
5c	Flow Chart – Authorisation Procedures - CHIS
6	Application for judicial approval – standard form
7	Flow Chart – Procedures relating to judicial approval application

1A. Introduction

Regulation of Investigatory Powers Act 2000 (as amended by the Protection of Freedoms Act 2012)

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) was enacted to provide a clear statutory framework for the operation of certain intrusive investigative techniques, to provide for compliance with the Human Rights Acts 1998. The main purpose of the Act is to ensure that individuals' rights are protected whilst allowing law enforcement and security agencies to do their jobs effectively and act proportionately.

1.2 RIPA covers the interception, acquisition and disclosure of communications data (Part I of RIPA); the carrying out of surveillance and use of covert human intelligence sources (Part II); and the investigation of electronic data protected by encryption (Part III).

1.3 Thanet District Council is included within this framework with regard to **Directed Surveillance** and **Covert Human Intelligence Sources**, in accordance with section 28 and section 29 of the said Act.

1.4 Thanet District Council is **not** empowered to undertake Intrusive Surveillance involving entry on or interference with property or with wireless telegraphy as regulated by the Regulation of Investigatory Powers Act 2000.

1.5 This document will focus on the provisions of Part II of RIPA (as amended by the Protection of Freedoms Act 2012 (POFA) that cover the use and authorisation of directed surveillance and the steps that must be taken by Council Officers to comply with the Act.

1.6 The use of Covert Human Intelligence Sources (CHIS) has not been identified as a normal investigative technique applied and used by the Council. However there may be investigations where it is identified that CHIS may be used and authorisation sought

1.7 For each of the above powers, RIPA (as amended by POFA) ensures that the law clearly covers:

- the purposes for which they may be used;
- which authorities can use the powers;
- who should authorise each use of power;
- the use that can be made of material gained;
- independent judicial oversight and approval;
- a means of redress for the individual.

1.8 Surveillance is not simply for the targeting of criminals but is also a means of protecting the public from harm and preventing crime.

1.9 The provisions of RIPA do not cover authorisation for the use of overt CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime.

1.10 Thanet District Council operate an overt policy of providing signage information for all overt CCTV cameras within public places ensuring the public are aware of their operation and who is responsible for the system.

1.11 RIPA also provides for the appointment of independent Surveillance Commissioners who will oversee the exercise by public authorities of their powers and duties under the Act (Part IV of RIPA) *as amended by the Investigatory Powers Act 2016.*

1.12 Investigatory Powers Commissioner's Office (IPCO) provides independent oversight of the use of investigatory powers by intelligence agencies, police forces and other public authorities under the Investigatory Powers Act 2016.

1.13 **No** request for RIPA authorisation can be progressed without advice, guidance and review from the Council's RIPA Gate-keeper prior to obtaining authorisation from an Authoring Officer or without a URN (Unique Reference Number) being allocated.

1.14 The Council's corporate RIPA Gatekeeper is the Head of Operational Services.

1B. Policy Summary

1.12 Local authorities are required to respect the private and family life of citizens, their homes and correspondence in accordance with the Human Rights Act 1998. This right is qualified where interference is necessary and proportionate and carried out in accordance with the law.

1.13 The Regulation of Investigatory Powers Act 2000 ('RIPA') contains powers for various bodies to carry out covert surveillance and other covert activities. Certain covert powers under RIPA are available to local authorities and can be used in appropriate circumstances in accordance with the requirements of the Act to support the delivery of their functions.

1.14 This Policy covers the use of Directed Surveillance and the deployment of Covert Human Intelligence Sources by the Council.

1.15 In summary, **Directed Surveillance** is surveillance that is covert, is conducted for the purposes of a specific investigation or operation, is likely to result in the obtaining of private information about a person and is conducted otherwise than by way of an immediate response to events.

1.16 In summary, a person is a **Covert Human Intelligence Source** ('CHIS') if they establish or maintain a personal or other relationship and they covertly use the relationship to obtain information or provide access to any information to another person, or they covertly disclose information obtained through that relationship or as a consequence of the existence of that relationship.

1.17 Use of Directed Surveillance (or deployment of a CHIS) could potentially be used by the Council in an investigation as a means of obtaining information. Use of Directed Surveillance or deployment of a CHIS must be authorised. There are designated officers within the Council ('Authorising Officers') who are able to authorise such activity. The Authorising Officer must consider the detailed legal tests when deciding whether to authorise the covert activity. If the Authorising Officer does authorise the activity, it is still subject to a judicial approval process. This means that an application must be made to the Magistrates Court for approval of the authorisation and it cannot take effect until such approval is obtained.

1.18 In practical terms, if officers consider that you might wish to carry out directed surveillance or deploy a CHIS as part of an investigation, (or even if you are not certain whether the activities that you are proposing require a RIPA authorisation), please ensure that you seek advice from the Council's RIPA Gate-keeper and/or legal services early on and consult the Monitoring Officer as appropriate.

1.19 If you do require a RIPA authorisation for your proposed activity, you will then need to contact the Council's RIPA Gate-keeper who maintains a secure Central Register of all requests for authorisation. (You will be issued with a unique reference number URN). The Council's RIPA Gate-keeper also retain all original RIPA forms.

1.20 It is important to be aware that once a RIPA authorisation has been granted by the Authorising Officer and approved by the Magistrates Court, and you are carrying out the

activity, you must still adhere to this Policy & Procedure Guidance. There are ongoing requirements concerning review of the authorisation for example and record keeping requirements.

2.

Definitions

2.1 What is Surveillance?

Surveillance is:

- 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 surveillance
- Surveillance by or with the assistance of appropriate surveillance device(s).

Surveillance can be **overt** or **covert**.

2.2 Overt Surveillance

2.2.1 Most of the surveillance carried out by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. 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.

2.2.2 Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that Officers may visit without notice or identifying themselves to the owner/proprietor to check that the conditions are being met).

2.3 Covert Surveillance

2.3.1 Covert Surveillance as defined in Section 26 RIPA:

> "Surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place".

2.3.2 General observation forms part of the duties of many enforcement officers. Such observation may involve the use of equipment or merely reinforce normal sensory perceptions, such as binoculars or the use of cameras, where this does not involve systematic surveillance of an individual. It forms part of the everyday functions of law enforcement or other public bodies. This low level activity will not usually be regulated under the provisions of RIPA.

2.3.3 The installation of CCTV cameras for the purpose of generally observing activity in a particular area with signage is not surveillance which requires

authorisation. Members of the public are aware that such systems are in use, for their own protection and to prevent crime.

Authorisation may be required if a CCTV camera is being used for a specific type of surveillance.

Part II of RIPA applies to the following conduct:

Directed surveillance
Intrusive surveillance
The conduct and use of covert human intelligence sources

2.4 Directed Surveillance Section 26(2) RIPA

2.4.1 Surveillance will be covert where it is carried out in a manner calculated to ensure that the person or persons subject to the surveillance are unaware that it is or may be taking place.

2.4.2 Directed surveillance is conducted where it involves the observation of a person or persons with the intention of gathering **private information** to produce a detailed picture of a person's life, activities and associations. However, it 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, enforcement officers would not require authorisation to conceal themselves and observe a suspicious person who they come across in the course of their normal duties. However the longer the observation continues, the less likely it would be considered to be an immediate response.

2.5 Intrusive Surveillance – Section 26(3) RIPA

2.5.1 **Local Authorities cannot conduct intrusive surveillance** involving entry on or interference with property or with wireless telegraphy as regulated by the Regulation of Investigatory Powers Act 2000.

2.5.2 Surveillance is intrusive, only if it is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle. This kind of surveillance may take place by means either of a person or device located inside residential premises or a private vehicle of the person who is subject to the surveillance or by means of a device placed outside which consistently provides a product of equivalent quality and detail as a product which would be obtained from a device located inside.

2.5.3 Therefore, use of a device is only "intrusive" if it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the residential premises or in any private vehicle. Thus, an observation post outside premises, which provides a limited view and no sound of what is happening inside the premises, would not be considered as intrusive surveillance.

2.5.4 The covert recording of suspected noise nuisance where the intention is only to record excessive noise levels from adjoining premises and the recording device is calibrated to record only excessive noise levels constitutes neither directed nor intrusive surveillance. In such circumstances, the perpetrator would normally be regarded as having forfeited any claim to privacy and an authorisation may not be necessary.

2.6 Covert Human Intelligence Source (CHIS) – Section 26(8) RIPA

A person is a covert human intelligence source (CHIS) if:

- he establishes or maintains a personal or other relationship with a person for the *covert purpose* of facilitating one or both of the following;

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

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

In establishing or maintaining a relationship, a *covert purpose* exists where the relationship is conducted in such a manner that it is calculated to ensure that one of the parties to the relationship is unaware of its purpose.

Further information about the use of CHIS is dealt with in the next section of this policy.

2.7 Private Information

"Private information", in relation to a person, includes any information relating to his private or family life.

2.8 Private Vehicle

"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. This does not include a person whose right to use the vehicle derives only from his having paid, or undertaken to pay, for the use of the vehicle and its driver for a particular journey. A vehicle includes any vessel, aircraft or hovercraft.

2.9 Confidential Material

This consists of:

- **Matters subject to legal privilege** - for example oral and written communications between a professional legal adviser and his client or any person representing his client, made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications. Communications and items held with the intention

of furthering a criminal purpose are not subject to legal privilege where there is evidence that the professional legal advisor is intending to hold or use them for a criminal purpose.

- **Confidential personal information** - which is information held in confidence concerning an individual (living or dead) who can be identified from it, and relating to a) his physical or mental health or b) to spiritual counselling or other assistance given or to be given, and which a person has acquired or created in the course of any trade, business, profession or other occupation, or for the purposes of any paid or unpaid office. It includes oral and written information and also communications as a result of which personal information is acquired or created. Information is held in confidence if:

  It is subject to a restriction on disclosure or an obligation of secrecy contained in existing or future legislation

- **Confidential journalistic material** - which includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to an undertaking.

2.10 Residential Premises

"Residential premises" means any premises occupied or used, however temporarily, for residential purposes or otherwise as living accommodation.

2.11 Right to Privacy

Great care is required as the right to privacy (Article 8 Human Rights Act 1998) can also extend to business premises or residential premises used for business purposes. It is essential that Authorising Officers should seek legal guidance on this matter prior to authorisation.

2.12 Collateral Intrusion

This is interference with the privacy of a person other than the surveillance subject.

2.12.1 Before authorising applications for directed surveillance, the authorising officer should also take into account the risk of obtaining private information about persons who are not subjects of the surveillance activity.

2.12.2 Measures should be taken, wherever practicable, to avoid or minimise the unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance activity. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided the intrusion in considered proportionate to what is sought to be achieved. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

2.13 Authorising Officer

This is the person designated, for the purpose of the Act, to grant authorisation for directed surveillance.

2.14 ***Investigatory Powers Commissioners Office (IPCO)***

The Investigatory Powers Commissioner and Judicial Commissioners are responsible for overseeing the use of investigatory powers by public authorities which include law enforcement, the intelligence agencies, prisons, local authorities and other government agencies (e.g. regulators).

3. The use of a Covert Human Intelligence Source (CHIS)

The concept of "covertness" is very similar to that used in relation to directed surveillance. Here, however, it is used at two stages, both of which must be met for an authorisation to be required: the *covert purpose* of the relationship; and the *covert actions* of obtaining or providing access to information and of disclosing such information. **If a person has a relationship with another person which is not established or maintained for a covert purpose, the fact that he or she does in fact *covertly* disclose information to the local authority will not require an authorisation and that person will not be a CHIS.**

There is no use of CHIS merely because a person offers information to the local authority that may be material to the investigation of an offence, but there would be if the authority asks the person to obtain further information.

3.1 The use of Covert Human Intelligence Sources

Authorisation for the use and conduct of a source is required prior to any tasking, i.e. an assignment given to the source. There will normally be two persons involved in the process of the authorisation of the person carrying out the surveillance. There will be the person who completes and signs the application form by which authorisation is applied for and the Authorising Officer (legal advice must be sought via the Council's RIPA Gatekeeper before embarking on a CHIS authorisation) to whom the form must be submitted for consideration. In the case of the use of CHIS, whilst it is not unlawful for the source to make the application him or herself, **the extensive welfare provisions that have to be made for him or her make this inappropriate**.

Where confidential material is likely to be particularly sensitive (see below) then the Authorising Officer should be the Director/Head of Service, or in his/her absence the Monitoring Officer.

The test is set out in Section 29(2) RIPA and is listed for convenience in the authorisation. Included in the requirements under Section 29 are that sufficient arrangements must be made to ensure that the source is independently managed, records are kept of the use made of the source, and that the identities of the source are protected from those who do not need to know it (see below).

3.2 Authorising a CHIS – See flow chart at Appendix 5c

3.2.1 This is similar to the authorisation of directed surveillance. Firstly, **the authorisation must be *necessary*** on the same ground as for directed surveillance, for the purpose of preventing or detecting crime or preventing disorder.

3.2.2 Secondly, **the authorised conduct or use of the source must be proportionate to the goal sought**. In this connection, and on the question

of proportionality, it may be considered that the chances of collateral intrusion are particularly significant in the case of the use or conduct of CHIS. The Home Office Code of Practice recommends that the application includes a risk assessment for collateral intrusion.

3.2.3 As with the authorisation of directed surveillance, the forms themselves set out clearly what information is required from the applicant and also from the Authorising Officer in order to give a valid authorisation. (Both the person applying for the authorisation and the Authorising Officer must complete the forms in handwriting).

3.2.4 **From November 2012 the authorisation process for use of a CHIS has been subject to judicial approval meaning that any authorisation granted will require the approval of a Justice of the Peace, which necessitates making an application to the Magistrates Court.**

3.2.5 The Authorising Officer must be satisfied that arrangements exist for the proper oversight and management of the source that satisfy the requirements of section 29(5) of the Act and such other requirements as may be imposed by order made by the Secretary of State.

3.3 Covert Human Intelligence Sources may only be authorised if the following arrangements are in place:

Section 29(5) requires:

- that there will at all times be an officer within the local authority who will have day to day responsibility for dealing with the source on behalf of the authority, and for the source's security and welfare (section 29(5)(a));

- that there will at all times be another officer within the local authority who will have general oversight of the use made of the source (section 29(5)(b));

- that there will at all times be an officer within the local authority who has responsibility for maintaining a record of the use made of the source (section 29(5)(c));

- that the records relating to the source maintained by the local authority will always contain particulars of all matters specified by the Secretary of State in Regulations.

  (The current regulations are The Regulation of Investigatory Powers (Source Records) Regulations 2000). These particulars are:

  (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 (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, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the Act (see bullet points above) 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 of the source's activities for the benefit of that or any other relevant investigating authority

- that records maintained by the local authority that disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.

These requirements make it very unlikely that an investigation could involve the use of CHIS without there having been prior planning within the investigating department/section. It is important to realise that it may well be a member of staff of the department and, indeed, an investigator him or herself, who becomes the source, depending on the manner of working used. It is not only persons outside the employ of the local authority who may be used as a source. If it is intended to

make use of CHIS, then appropriate and specific training should be arranged for the officers responsible for the functions under section 29(5) (a) to (c) of the Act and also for any officer of the Council who is to be the CHIS.

It is very important that the two forms of authorisation are not confused, because of the important welfare provisions listed above attaching to the CHIS. Whilst those requirements are detailed and specific, it is recognised that they fall into line with the approach that the Council takes for the welfare of its staff. The Council recognises a duty of care to its covert sources and it is important that a risk assessment and management approach is taken with regard to the welfare of the source**.** The risks to the source may not only be physical but also psychological, for example, relating to stress caused by the very activity itself.

It must be made clear that the source is not also engaging in criminal activity (excluding activity that would be criminal but is rendered lawful by authority under the Act – e.g. the lawful interception of communications).

3.4 Juveniles and vulnerable persons as a CHIS.

This is governed by the Regulation of Investigatory Powers (Juveniles) Order 2000. A person under 16 cannot be used as CHIS if the relationship that would be covertly used is between the juvenile and his/her parent or person with parental responsibility for him/her. (Whether or not a person who is not a parent has parental responsibility for a child may only be determined by having sight of documentation, e.g. a court order providing for that person to have parental responsibility. Further, a person may have parental responsibility for a juvenile, even though they no longer live together).

The Regulations also provide in the case of a source under 16 that there is at all times a person within the local authority responsible for ensuring that an appropriate adult (parent or guardian, any other person who has assumed responsibility for the juvenile's welfare, or where there are no such persons, any responsible person over 18 who is not a member or employee of the local authority – therefore a local authority social worker is *not* eligible to act as appropriate adult) is present at meetings between the juvenile source and any person representing the investigating authority.

Where the source is under 18, authorisation may not be granted or renewed unless there has been made or updated a risk assessment sufficient to demonstrate that the nature and magnitude of any risk of physical injury or psychological distress to the juvenile arising out of his or her use as a source has been identified and evaluated.

The Authorising Officer must have considered the risk assessment and satisfied him/herself that the risks are justified and have been properly explained to and understood by the source. The Authorising Officer must also be clear whether or not the covert relationship is between the juvenile and any relative, guardian or person who has assumed responsibility for his/her welfare and, if it is, has given particular consideration to whether the authorisation is justified ("necessary" and "proportionate") in the light of that fact.

The Code of Practice on Covert Human Intelligence Sources also makes provision for vulnerable persons. These are individuals who are or may be in need of community care services by reason of mental or other disability, age, illness or who are unable to take care of themselves or unable to protect themselves against significant harm or exploitation**.** Any such individual should only be used as a source in the most exceptional circumstances. As with confidential information, the authorisation of the Chief Executive, or the Monitoring Officer in their absence, is required to use a juvenile or vulnerable person as a source.

With juveniles and vulnerable persons, particular emphasis must be placed on the operation of the provisions for the source's welfare.

3.5 What Conduct of a CHIS is Authorised by an Authorisation?

- any conduct that is comprised in any such activities as are *specified or described* in the authorisation; and

- any conduct by or in relation to the source *specified or described* in the authorisation;

- which is carried out for the purposes of or in connection with the investigation or operation that is *specified or described*.

3.6 Judicial Approval of CHIS authorisations

3.6.1 The Protection of Freedoms Act 2012 amended RIPA 2000 to make local authority authorisation of a CHIS subject to judicial approval. The change means that local authorities need to obtain an order from a Justice of the Peace, approving the grant or renewal of an authorisation, before it can take effect. If the Justice of the Peace is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the grant or renewal for the use of the technique as described in the application.

3.6.2 **This new judicial approval mechanism is in addition to the existing authorisation process. The requirements to internally assess necessity and proportionality, complete the RIPA authorisation/application forms and seek approval from an Authorising Officer remain. Therefore, there is a three-stage process. First, advice and URN will need to be obtained from the Council's RIPA Gate-keeper. Secondly, an authorisation must be obtained from an Authorising Officer. Thirdly, approval of the authorisation must be obtained from a Justice of the Peace. This involves applying to a Magistrates Court.**

3.6.3 A Justice of the Peace will only give approval to the granting of an authorisation for use of a CHIS if they are satisfied that:

- at the time the Authorising Officer granted the authorisation, there were reasonable grounds for believing that the authorisation was necessary and that the activity being authorised was proportionate, that arrangements existed that satisfied section 29(5) (see paragraph 3.3),

that the Authorising Officer was a designated person for the purposes of section 29 of RIPA, that the grant of the authorisation was not in breach of any restrictions imposed by virtue of section 29(7)(a) or 30(3) of RIPA, that any other conditions provided for by any Order were satisfied; and

- that there remain reasonable grounds for believing that the necessary and proportionate tests are satisfied and that any other requirements provided for by Order are satisfied.

3.7 CHIS Record Keeping

Records should be kept as prescribed by the Code of Practice (please see paragraph on Records and Documentation above). Where a source wearing or carrying a surveillance device is invited into residential premises or a private vehicle and records activity taking place inside those premises or vehicle, authorisation for use of that covert source should be obtained in the usual way.

The source should not use an invitation into residential premises or private vehicle as a means of installing equipment. If equipment is to be used other than in the presence of the covert source, an intrusive surveillance authorisation is necessary which **cannot be granted by the local authority**.

4.

Authorisation (see flowchart at appendix 5b)

4.1 Authorisation of Surveillance

4.1.1 Since November 2012, when the Protection of Freedoms Act 2012 amended RIPA 2000, the framework governing how local authorities use RIPA has changed. Authorisation of the use of certain covert powers, including the use of directed surveillance, will only have effect once an order approving the authorisation has been granted by a Justice of the Peace. This new judicial approval mechanism is in addition to the existing authorisation process. The current processes of assessing necessity and proportionality, completing the RIPA application forms and seeking authorisation from an Authorising Officer remain the same.

4.1.2 Therefore, there is a three-stage process. First, advice and URN will need to be obtained from the Council's RIPA Gate-keeper. Secondly, an authorisation must be obtained from an Authorising Officer. Thirdly, approval of the authorisation must be obtained from a Justice of the Peace. This involves applying to a Magistrates Court.

4.1.3 Authorising Officers will be nominated by the Monitoring Officer following the Monitoring Officer being satisfied they are appropriately trained to undertake the task.

4.1.4 Written authorisations must be completed whenever an investigation involves the use of Directed Surveillance. This provides lawful authority to carry out covert surveillance. Authorisation must be sought before surveillance is undertaken.

4.1.5 All applications for authorisation of **Directed Surveillance** must be in writing and record:

- the grounds on which authorisation is sought (i.e. for the prevention and detection of crime and disorder only); NB The power to authorise surveillance exists only for the prevention and detection of crime and disorder and no other purpose

- an assessment of **the Directed Surveillance Crime Threshold**. Directed surveillance can only be authorised under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment. (There are certain specified offences related to the underage sale of alcohol or tobacco which are exempt from the directed surveillance crime threshold. However, investigation of these offences does not form part of the District Council's functions).

- Further information about the implications of the Directed Surveillance Crime Threshold are outlined in paragraph 4.1.6 below

- consideration of why the Directed Surveillance is proportionate to what it seeks to achieve;

- that other options for the gathering of information have been considered and that Directed Surveillance is necessary

- the identity or identities, where known, of those to be the subject of Directed Surveillance;

- the action to be authorised and level of authority required;

- an account of the investigation or operation;

- an explanation of the information which it is desired to obtain as a result of the authorisation;

- any potential for collateral intrusion;

- the likelihood of acquiring any confidential material.

Both the person applying for the authorisation and the Authorising Officer must complete the forms in handwriting.

Standard Document: See Appendix 1 – Surveillance Application Form

4.1.6 The Directed Surveillance Crime Threshold was introduced by The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 which came into force on 1st November 2012. The introduction of this new threshold means that the Council may continue to authorise the use of Directed Surveillance in more serious cases provided the other tests are met (ie. that it is necessary and proportionate and that prior approval from a Justice of the Peace has been obtained). However, it also means that the Council may not authorise the use of Directed Surveillance to investigate disorder that does not involve criminal offences, or to investigate low level offences, which may include, for example, littering, dog control and fly-posting.

4.1.7 Those carrying out the covert surveillance should inform the Authorising Officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way. In some cases the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required.

4.1.8 Any person giving an authorisation should first satisfy him/herself that the authorisation is **necessary** on particular grounds and that the surveillance is **proportionate** to what it seeks to achieve. It is important that sufficient

weight is attached to considering whether the surveillance required is proportionate. These concepts of “necessity” and “proportionality” occur regularly throughout human rights law and RIPA and they must be considered afresh in the case of each authorisation of surveillance. Therefore this will involve balancing the intrusiveness of the surveillance on the target and others who might be affected by it against the need for the surveillance in operational terms. The surveillance will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All surveillance should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

4.1.9 When proportionality is being assessed, the following elements should be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods 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; and
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

4.1.10 The Authorising Officer must be able to produce evidence that the relevant issues have been considered for monitoring purposes, for example a note of the documents and information available to the officer at the time the authorisation is given, together with a note of the date and time authorisation was given. It is essential that the Authorising Officer considers each request for an authorisation on its merits and a rubber stamping approach must never be used.

4.1.11 The fullest consideration should be given in cases where the subject of the surveillance might reasonably expect a higher degree of privacy, for instance in his/her home, or where there are special sensitivities, such as where the surveillance may give access to confidential material or communications between a minister of any religion or faith and another individual relating to that individual relating to that individual’s spiritual welfare.

4.1.12 An authorisation should not be sought or obtained where the sole purpose of the authorisation is to obtain legally privileged material. However, an authorisation may be appropriate for other purposes but which, incidentally, catches legally privileged material.

4.1.13 Particular consideration should be given to collateral intrusion on or interference with the privacy of persons other than the subject(s) of surveillance. Such collateral intrusion or interference would be a matter of greater concern in cases where there are special sensitivities, for example

in cases of premises used by lawyers or for any form of medical or professional counselling or therapy.

4.1.14 An authorisation request should include assessment of any collateral intrusion or interference. This will be taken into account, by the Authorising Officer, particularly when considering the proportionality of the surveillance.

4.1.15 Directed surveillance undertaken by the Council requires the written approval of a post holder identified in 4.1.16 of this document.

4.1.16 The following table identifies appropriate authorisation levels in the Council's staffing structure.

Type of Request		Authorising Officer
1	Written authorisation to conduct investigations using Directed Surveillance.	CEO, Director, Head of Service as Authorising Officers
2	Written authorisation to conduct investigations using Directed Surveillance likely to obtain confidential information.	*CEO only or in their absence, the Deputy Chief Executive or the Monitoring Officer*

NB For the avoidance of doubt, only those Officers outlined above **and** designated and certified (and also notified to the Monitoring Officer) to be "Authorising Officers" for the purpose of RIPA can authorise "Directed Surveillance". The Monitoring Officer will only certify Authorising Officers if they are satisfied that they have had appropriate training to undertake the role.

4.1.18 **Judicial approval**

a) **Where an Authorising Officer has granted an authorisation (for Directed Surveillance, the authorisation is not to take effect until a Justice of the Peace has made an order approving the grant of the authorisation.**

b) A Justice of the Peace will only give approval to the granting of an authorisation for **Directed Surveillance** if they are satisfied that:

- at the time the Authorising Officer granted the authorisation, there were reasonable grounds for believing that the authorisation was necessary and that the surveillance being authorised was proportionate, that the Authorising Officer was a designated person for the purposes of section 28 of RIPA, that the grant of the authorisation was not in breach of any restrictions imposed by virtue of section 30(3) of RIPA, that any other conditions provided for by any Order were satisfied; and

- that there remain reasonable grounds for believing that the necessary and proportionate tests are satisfied.

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

4.1.19 **No activity permitted by the authorisation granted by the Authorising Officer may be undertaken until the approval of the Magistrates Court of that authorisation has been obtained.**

4.1.20 **Authorising Officers must when making authorisations be aware that each authorisation (or renewal of an authorisation) will be subject to judicial approval. The Council is required to make an application without notice to the Magistrates Court to seek judicial approval.**

4.1.21 **Therefore, any Authorising Officer who proposes to approve an application for the use of directed surveillance must immediately inform the Monitoring Officer who will then make arrangements for an application to be made by the Council's lawyers or an appropriate officer to the Magistrates Court for an order to approve the authorisation to be made.**

4.1.22 There is no need for a Justice of the Peace to consider either cancellations or internal reviews.

4.1.23 The Council will provide the Justice of the Peace with a copy of the original RIPA authorisation form and the supporting documents setting out the case. This forms the basis of the application to the Justice of the Peace and should contain all information that is relied upon. In addition, the Council will need provide the Justice of the Peace with a partially completed judicial application/order form, which is shown for information at Appendix 6 of this Policy. The flow-chart at Appendix 7 shows the procedure for making an application to a Justice of the Peace seeking an Order to approve the grant of a RIPA authorisation or notice.

4.2 Duration of authorisations

4.2.1 A written authorisation for directed surveillance will cease to have effect at the end of a period approved by the Magistrates Court beginning with the day on which it took effect, unless otherwise directed by the court at the time of authoring the application.

4.3 Renewals

4.3.1 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/she may approve a renewal in writing for a further period of three months, beginning with the day when the authorisation would have expired but for the renewal.

Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

4.3.2 All requests for the renewal of an authorisation for Directed Surveillance must record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- the information required in the original request for an authorisation;

(a) any significant changes to the information in the previous authorisation;

(b) why it is necessary to continue with the surveillance;

(c) the content and value to the investigation or operation of the information so far obtained by the surveillance;

(d) an estimate of the length of time the surveillance will continue to be necessary.

Standard Document: See Appendix 2 – Surveillance Renewal form

4.3.3 **Renewals of authorisations will also be subject to approval by the Magistrates Court. The Authorising Officer must therefore advise the Monitoring Officer immediately when they are minded to grant a renewal.**

4.3.4 Applications for renewals should not be made until shortly before the original authorisation period is due to expire but officers must take account of factors which may delay the renewal process (eg. intervening weekends or the availability of the Authorising Officer and a Justice of the Peace to consider the application).

4.4 Cancellations

4.4.1 The Authorising Officer must cancel an authorisation if he/she is satisfied that the Directed Surveillance no longer meets the criteria for authorisation. When cancelling an authorisation, an Authorising Officer must ensure that proper arrangements have been made for the activity's discontinuance, including the removal of technical equipment, and directions for the management of the product.

Standard Document: See Appendix 3 – Surveillance Cancellation form.

4.4.2 Authorisations for Directed Surveillance, and any subsequent renewals and cancellations, are subject to review by the Government appointed Surveillance Commissioner.

4.5 Reviews

4.5.1 Authorising Officers will review all “Directed Surveillance” applications and authorisations. The results of a review should be recorded on the appropriate form, and kept in the central record of authorisations. The Authorising Officer should determine how often the review should take place. This should be done as frequently as is considered necessary and practicable, but not later than once a month following the date of authorisation; sooner where the surveillance provides access to confidential material or involves collateral intrusion.

4.5.2 Reviews of an authorisation for Directed Surveillance must record:

- any significant changes to the information in the previous authorisation;
- why it is necessary to continue with the surveillance;
- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- an estimate of the length of time the surveillance will continue to be necessary.

Standard Document: See Appendix 4 – Monthly Review Form

4.6 Records and Documentation

4.6.1 All documentation regarding Directed Surveillance should be treated as confidential and should be kept accordingly.

4.6.2 Records should be maintained for a period of at least five years from the ending of the authorisation. Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable period, commensurate to any subsequent review.

4.6.3 If there is any reason to believe that the results obtained during the course of investigation might be relevant to that investigation or to another investigation or to pending or future civil or criminal proceedings then it should not be destroyed but retained in accordance with established disclosure requirements. Particular attention is drawn to the requirements of the Code of Practice issued under the Criminal Procedure and Investigations Act 1996, which requires that material should be retained if it forms part of the unused prosecution material gained in the course of an investigation, or which may be relevant to an organisation.

4.6.4 Authorising Officers are reminded of the importance of safeguarding confidential and sensitive information. They must also ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities in the handling and storage of material. Where material is obtained by surveillance, which is wholly unrelated to a criminal or other investigation or to any person who is subject

of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be destroyed immediately. Consideration of whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer.

4.6.5 Each Service Department undertaking Directed Surveillance must ensure that adequate arrangements are in place for the secure handling, storage and destruction of material obtained through the use of covert surveillance.

4.6.6 There is nothing in the 2000 Act, which prevents results obtained through the proper use of the authorisation procedures from being used on other Council Department Investigations.

However, the disclosure outside of surveillance results obtained by means of covert surveillance and its use for other purposes should be authorised only in the most exceptional circumstances. Before doing so the Authorising Officer must be satisfied that the release of material outside of the Council, complies with and meets Human Rights Act requirements.

4.6.7 The Director is responsible for ensuring that arrangements exist for ensuring that no information is stored by the authority, except in so far as is necessary for the proper discharge of its functions. Such persons are also responsible for putting arrangements in place to ensure that no information is disclosed except in specified circumstances e.g. where it is necessary for the proper discharge of the authority's functions, for the purpose of preventing or detecting serious crime for the purpose of any criminal proceedings.

4.6.8 A copy of all authorisations must be sent to the Council's RIPA Gate-keeper, so that there is a central record maintained, and so that responsibilities of the Monitoring Officer of ensuring the Act is being complied with.

Authorisation forms are also open to inspection by the Investigatory Powers Commissioners Office (IPCO).

4.7 Monitoring of Authorisations

Information must be supplied to the Council's RIPA Gate-keeper using the forms attached to this guidance. The Gate-keeper will maintain a Central Register of all forms completed by the Authorising Officer. Authorising Officers are responsible for sending **the original authorisation** in the appropriate form for each authorisation, cancellation and renewal granted, to the Gatekeeper for inclusion in the Central Register and keeping a **copy** for their own records in the individual departments.

A review will be carried out regularly to ensure all forms have been sent for inclusion in this Central Register. The Monitoring Officer is required by law to ensure that the Council does not act unlawfully.

Authorising Officers are required to ensure that:-

- Authorisations have been properly cancelled at the end of the period of surveillance

- Surveillance does not continue beyond the authorised period

- Current authorisations are regularly reviewed

- At the anniversary of each authorisation, the destruction of the results of surveillance operations has been considered

- At the fifth anniversary of each authorisation the destruction of the forms of authorisation, renewal or cancellation has been considered.

The Gatekeeper/Monitoring Officer will:

- Monitor the authorisations to ensure correct procedure has been followed

- Receive and investigate complaints by members of the public who reasonably believe they have been adversely affected by surveillance activities carried out by the Council.

The Office of Surveillance Commissioners has a duty to keep under review the exercise and performance of the Council of its surveillance powers. The Office of Surveillance Commissioners will regularly inspect the Council and may carry out spot checks unannounced.

4.8 Refusals

All refusals to grant authority to undertake Directed Surveillance must be recorded and retained for inspection.

4.9 Breach of RIPA

Evidence gathered where RIPA has not been complied with may not be admissible in Court and could lead to a challenge under Article 8 of the Human Rights Act.

Any perceived breach of this policy or the RIPA procedures should be reported to the Monitoring Officer in order that they may notify the Investigatory Powers Commissioner immediately.

4.10 Undertaking Non-RIPA investigations

Obtaining authorisation for directed surveillance and conducting the surveillance in accordance with the authorisation means that the evidence obtained cannot be questioned. Surveillance which is obtained outside of the RIPA regime is not necessarily unlawful but its admissibility can be questioned. It is therefore important that officers consider why the surveillance is required, whether or not the information can be obtained in some other way and how the surveillance can be conducted in order to minimise the intrusion into people unconnected with the investigation.

RIPA authorisation must be obtained prior to undertaking directed surveillance. It is only where the matter being investigated falls outside of RIPA that the procedure in this policy can be followed. Even where this policy is followed, it is important to remember that the council's actions could be challenged both by way of arguing that the evidence obtained is inadmissible or that the council has infringed a person's civil liberties.

This could lead to action being against the council in the civil courts. A person might also complain to the Local Government Ombudsman about the council's actions. It is therefore very important that surveillance is only considered in appropriate cases and this policy is followed.

4.10.1 Examples of non-RIPA investigations

- Where the person under investigation is warned that surveillance is taking place or where the surveillance does not obtain private information (e.g. where noise levels only are recorded) the surveillance does not need to be authorised under RIPA or this policy.
- Non-live or after the event data collection using computerised records. No live tracking or surveillance is allowed under this non-RIPA procedure.

4.10.2 The procedure for obtaining authorisation for non-RIPA directed surveillance is the same as applying for authorisation under RIPA except there is no requirement to obtain judicial approval and officers should refer to the RIPA policy for full details.

4.10.3 As an initial step officers considering non-RIPA applications **must** talk to the Council's RIPA Gate-keeper, **before** proceeding.

5. Social Media

5.1 It is important to be aware that use of social media in an investigation could, depending on how it is used and the type of information likely to be obtained, constitute covert activity that requires authorisation under RIPA.

5.2 The rule of thumb, is that researching 'open source' material would not require authorisation, but return visits in order to build up a profile could change the position – this may constitute directed surveillance depending on the circumstances. Examples of 'open source' material, are materials you could view on social media without becoming a friend, subscriber or follower.

5.3 If privacy controls would be breached, for example by an investigator becoming someone's Facebook "friend", in order to access their profile and activity pages, then a directed surveillance authorisation is required. If any relationship was to be established by the investigating officer, so that their activities went beyond merely reading the site's content, then this would be deployment of a CHIS requiring an authorisation.

5.4 Officers should not use false personae (eg. a false Facebook profile or Twitter handle) to disguise their online activities. False personae should not be used for a covert purpose without authorisation. In accordance with OSC note 289

5.5 Home Office codes of practice on covert surveillance and CHIS contain some guidance in relation to online covert activity.

5.6 To ensure that no unauthorised online covert activity takes place within the Council, please ensure that advice is sought from the Council's RIPA Gate-keeper, Legal services or the Monitoring Officer.

6. Complaints

6.1 Procedure

The Council will maintain the standards set out in this guidance and the current Codes of Practice. The Investigatory Powers Commissioner has responsibility for monitoring and reviewing the way the Council exercises the powers and duties conferred by the Act.

Contravention of the RIPA and/or Data Protection Act 1998 may be reported to the Investigatory Powers Commissioner:

https://www.ipco.org.uk/
PO Box 29105, London, SW1V 1ZU
info@ipco.gsi.gov.uk

However before making such a reference, any person who reasonably believes they have been adversely affected by surveillance activity by or on behalf of the Council may complain to the Monitoring Officer who will investigate the complaint. A complaint concerning a breach of this Policy and Guidance document should be made using the Council's own internal complaints procedure.

APPENDIX 1

BEFORE COMPLETING THESE FORMS YOU MUST TALK TO THE COUNCIL'S RIPA GATE-KEEPER

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000

APPLICATION FOR AUTHORISATION TO CARRY OUT DIRECTED SURVEILLANCE

Public Authority *(including full address)*			
Name of Applicant		**Unit/Branch/Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person other than the applicant)			
DETAILS OF APPLICATION			
1. Give rank or position of Authorising Officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010; No. 521 .			

2. Describe the purpose of the specific operation or investigation.
3. Has the Directed Surveillance crime threshold been reached? How? Please specify the offence that is being investigated. (See paragraph 4.1.5 of the Council's RIPA Policy).
4. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.
5. The identities, where known, of those to be subject of the directed surveillance.
● Name: ● Address: ● DOB: ● Other information as appropriate:
6. Explain the information that it is desired to obtain as a result of the directed surveillance.

7. Explain <u>why</u> this directed surveillance is necessary for the purpose of preventing or detecting crime or of preventing disorder (Section 28(3)(b) RIPA). ***(This is the only statutory ground available to local authorities upon which applications for directed surveillance may be authorised – SI 2010/521).*** **(Code paragraphs 3.3 and 5.8)**
8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. (Bear in mind Code paragraphs 3.8 to 3.11) **Describe precautions you will take to minimise collateral intrusion.**

9. **Explain <u>why</u> 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? (Code paragraph 3.4 to 3.7)**
10. **Confidential information. (Code paragraphs 4.1 to 4.31)** **Indicate the likelihood of acquiring any confidential information:**

11. Applicant's Details.			
Name (print)		**Tel No**	
Grade/Rank		**Date**	
Signature			

12. Authorising Officer's Statement. (Spell out the "5 Ws" – Who; What; Where; When; Why and How – in this and the following box.)
I hereby authorise directed surveillance defined as follows: (*Why is the surveillance necessary? Whom is the surveillance directed against? Where and When will it take place? What surveillance activity/equipment is sanctioned? How is it to be achieved?)*
13. Explain <u>why</u> you believe the directed surveillance is necessary. (Code paragraphs 3.3 and 5.8) **Explain <u>why</u> you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out. (Code paragraph 3.4 to 3.7)**

14. (Confidential Information Authorisation) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31.	
Date of first review	
Programme for subsequent reviews of this authorisation: (Code paragraph 3.23 and 3.24). Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.	

Name (print)		**Grade/Rank**	
Signature		**Date and time**	
Expiry date and time (eg authorisation granted on 1 April 2005 – expires on 30 June 2005, 23:59)			

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000

APPLICATION FOR RENEWAL OF A DIRECTED SURVEILLANCE AUTHORISATION
(Please attach the original authorisation)

Public Authority *(including full address)*			
Name of Applicant		**Unit/Branch/Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Renewal Number			

DETAILS OF RENEWAL	
1. Renewal numbers and dates of any previous renewals.	
Renewal Number	**Date**

2. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.

3. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.

4. Detail why the directed surveillance is still proportionate to what it seeks to achieve.
5. Indicate the content and value to the investigation or operation of the information so far obtained by the directed surveillance.

6. Give details of the results of the regular reviews of the investigation or operation.

7. Applicant's Details			
Name (Print)		**Tel No**	
Grade/Rank		**Date**	
Signature			

8. Authorising Officer's Comments. <u>This box must be completed.</u>

9. Authorising Officer's Statement<u>.</u>

I, [insert name], hereby authorise the renewal of the directed surveillance operation as detailed above. The renewal of this authorisation will last for 3 months unless renewed in writing. This authorisation will be reviewed frequently to assess the need for the authorisation to continue.
Name (Print) ..... Grade/Rank Signature Date
Renewal From: Time: Date:

Date of first review.	
Date of subsequent reviews of this authorisation	

APPENDIX 3

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000

CANCELLATION OF A DIRECTED SURVEILLANCE AUTHORISATION

Public Authority *(including full address)*			
Name of Applicant		**Unit/Branch/Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			

DETAILS OF CANCELLATION
1. Explain the reason(s) for the cancellation of the authorisation:

2. Explain the value of surveillance in the operation:

3. Authorising Officer's statement.			
I, [insert name], hereby authorise the cancellation of the directed surveillance investigation/operation as detailed above.			
Name (Print)		Grade	
Signature	.....	Date	

4. Time and Date of when the Authorising Officer instructed the surveillance to cease.			
Date:		**Time:**	

5. Authorisation cancelled	Date:	Time:

APPENDIX 4

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000

REVIEW OF A DIRECTED SURVEILLANCE AUTHORISATION

Public Authority *(including full address)*			
Name of Applicant		**Unit/Branch/Division**	
Full Address			
Contact Details			
Operation Name		**Operation Number*** ***Filing Ref**	
Date of authorisation or last renewal		**Expiry date of authorisation or last renewal**	
		Review Number	

DETAILS OF REVIEW	
1. Explain the reason(s) for the cancellation of the authorisation:	
Review Number	**Date**

2. Summary of the investigation/operation to date, including what private information has been obtained and the value of the information so far obtained.

3. Detail the reasons why it is necessary to continue with the directed surveillance.

4. Explain how the proposed activity is still proportionate to what it seeks to achieve.

5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring

6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information

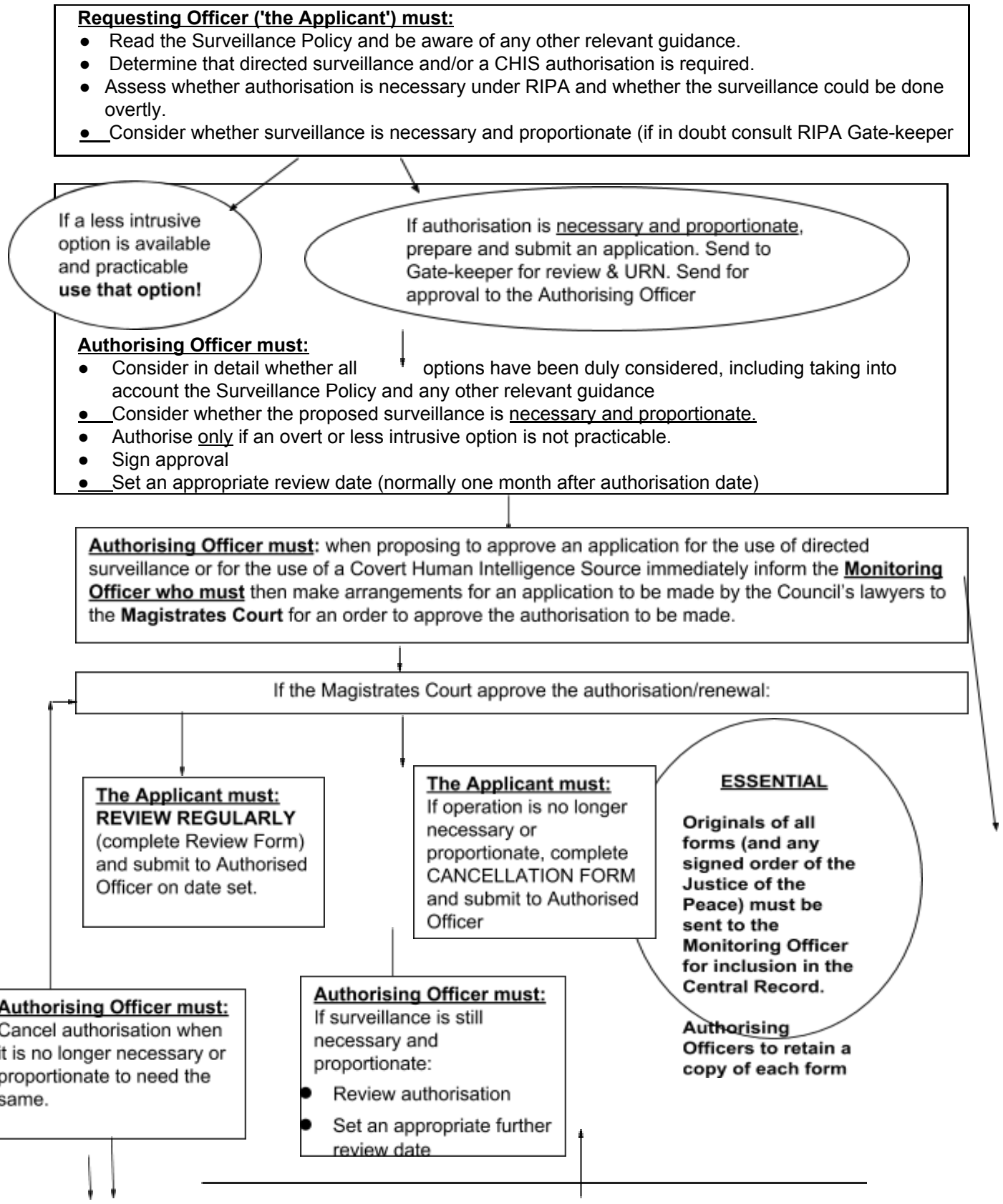
7. Applicant's Details			
Name (Print)		**Tel No**	
Grade/Rank		**Date**	
Signature			

8. Review Officer's Comments, including whether or not the directed surveillance should continue.

9. Authorising Officer's Statement.	
I, [insert name], hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal][it should be cancelled immediately].	
Name (Print)	Grade/Rank
Signature	Date

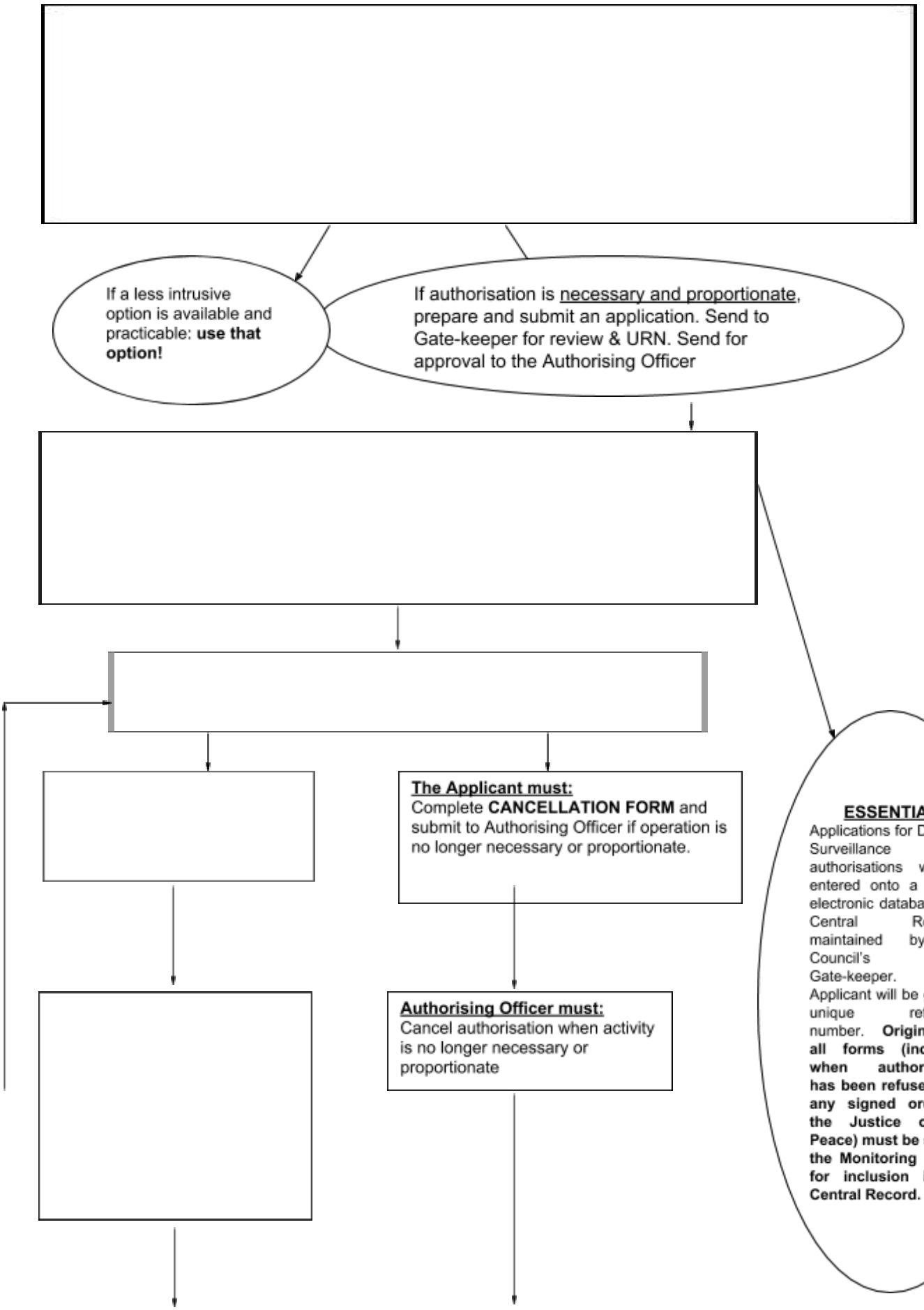
10. Date of next review.	

FLOW-CHART – AUTHORISATION PROCEDURES - GENERAL **APPENDIX 5a**

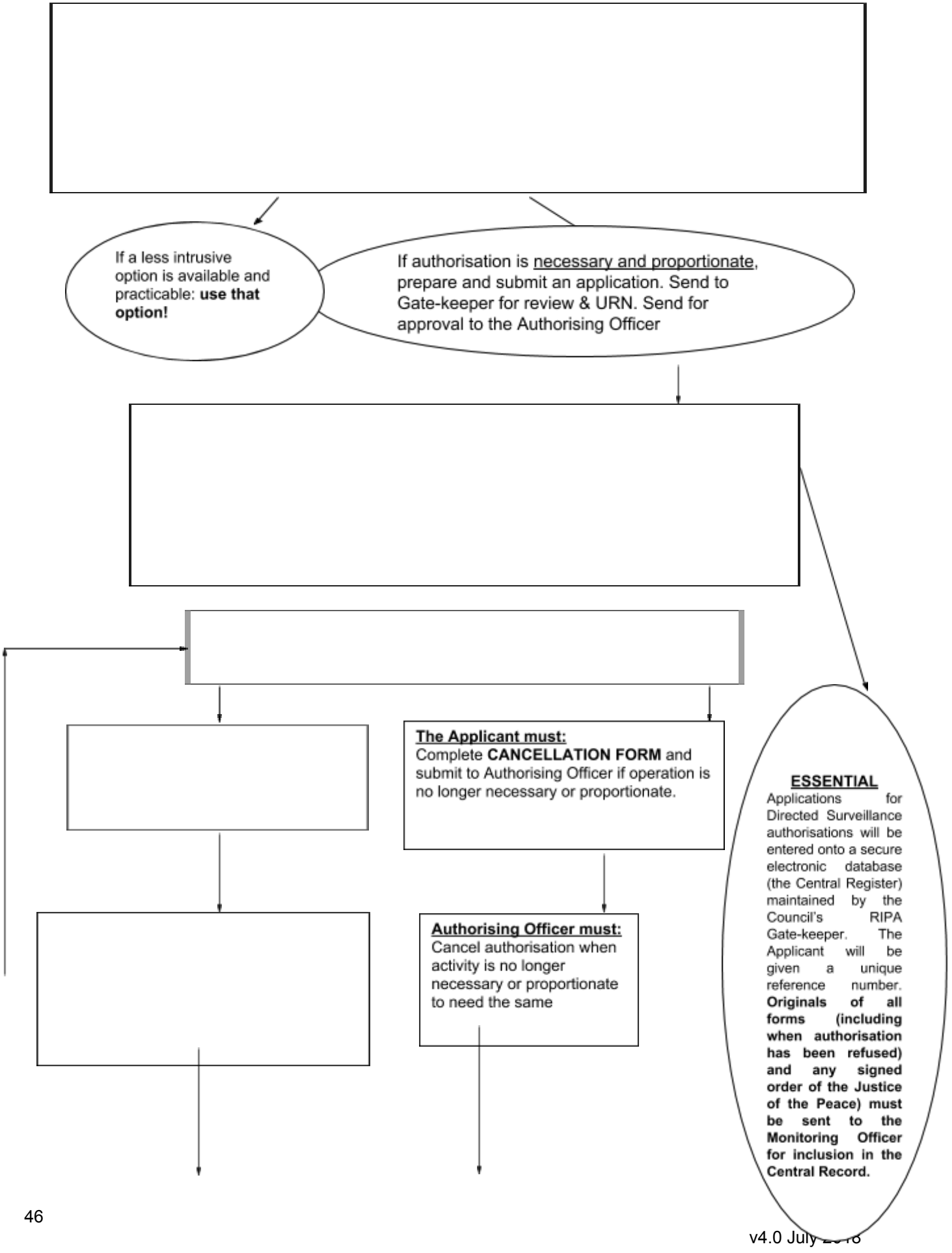


NB: If in doubt, seek advice from the Council's RIPA Gate-keeper, Legal Services or Monitoring Officer BEFORE any directed surveillance and or CHIS is authorised, renewed, cancelled, or rejected.

FLOW-CHART – DIRECTED SURVEILLANCE AUTHORISATION PROCEDURES **APPENDIX 5b**


If a less intrusive option is available and practicable: **use that option!**
If authorisation is necessary and proportionate, prepare and submit an application. Send to Gate-keeper for review & URN. Send for approval to the Authorising Officer
The Applicant must:
Complete **CANCELLATION FORM** and submit to Authorising Officer if operation is no longer necessary or proportionate.
Authorising Officer must:
Cancel authorisation when activity is no longer necessary or proportionate
ESSENTIAL
Applications for Directed Surveillance authorisations will be entered onto a secure electronic database (the Central Register) maintained by the Council's RIPA Gate-keeper. The Applicant will be given a unique reference number. **Originals of all forms (including when authorisation has been refused) and any signed order of the Justice of the Peace) must be sent to the Monitoring Officer for inclusion in the Central Record.**

FLOW-CHART – CHIS AUTHORISATION PROCEDURES **APPENDIX 5C**



APPENDIX 6

Application for judicial approval

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 authority:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of suspect:.....

.....

.....

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:.....

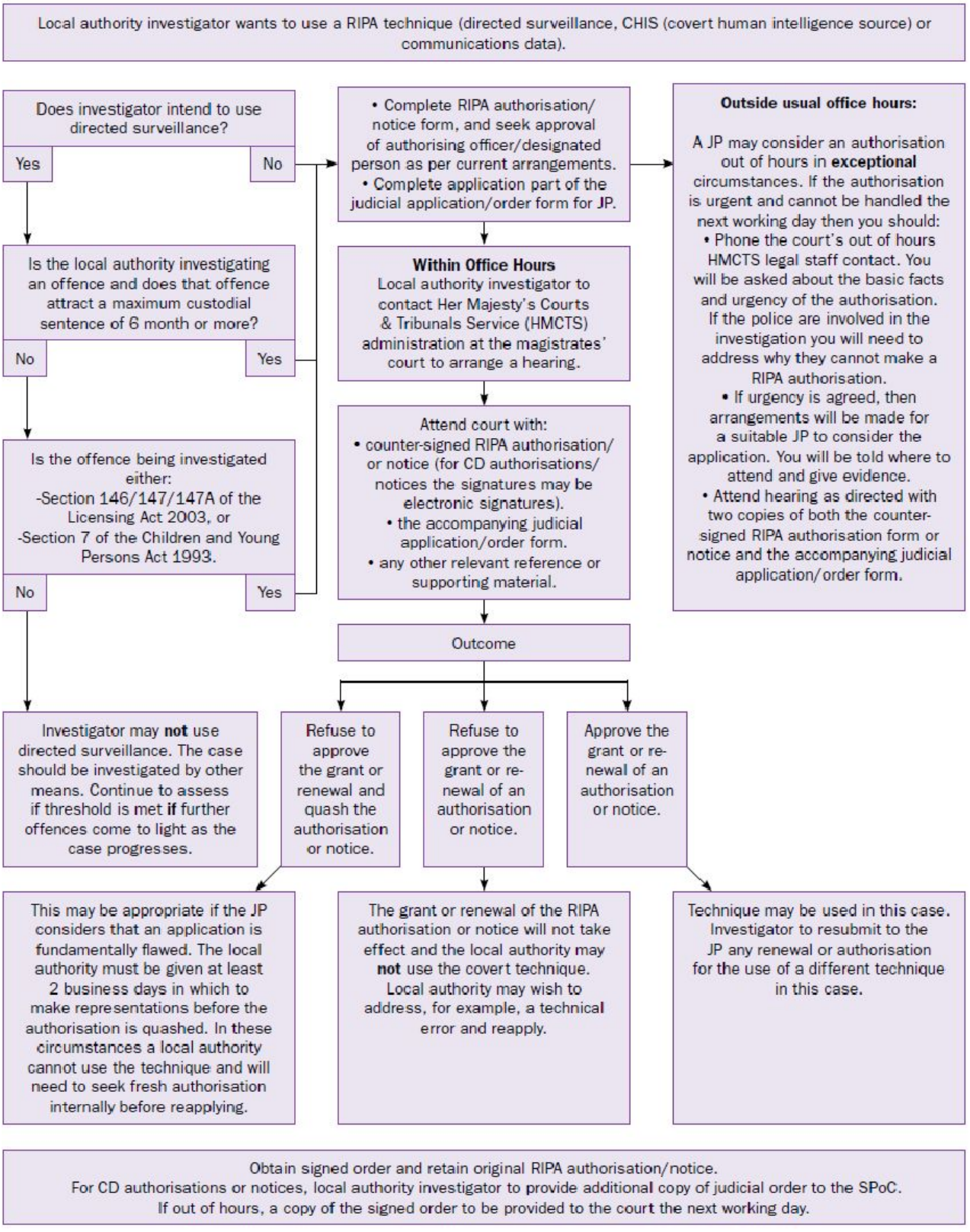
Contact email address (optional):.....

Local authority reference:.....

Number of pages:.....

APPENDIX 7

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



This flow chart is an extract from the October 2012 Home Office publication *"Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA) – Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance".*