NORTHAMPTON
BOROUGH COUNCIL

RIPA POLICY

October 2019

Version Control				
Document owner	Published on	Version	Changed on	Amended by
F Fernandes	03/03/2010	V.1		
F Fernandes	09/02/2015	V.2	17.6.2014	Management Board
F Fernandes	03/11/2015	V.3	29.10.2015 **	Francis Fernandes
F Fernandes	08/07/2016	V.4	08.06.2016	Cabinet
F Fernandes	08/10/2019	V.5	19.07.2019	Francis Fernandes
F Fernandes	17/10/2019	V.6	16.10.2019	Cabinet

** *Please note that the Home Office issued revised Codes of Practice in August 2018:*
- *Covert Surveillance and Property Interference Code of Practice*
- *Covert Human Intelligence Sources Code of Practice*

The Codes of Practice must be considered together with this Policy.

Contents

1A. Introduction

Regulation of Investigatory Powers Act 2000 (as amended)

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 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 Northampton Borough 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 RIPA.

1.4 Northampton Borough Council is not empowered to undertake:

(a) Intrusive Surveillance; or

(b) entry onto or interference with property or wireless telegraphy.

1.5 This document will focus on the provisions of Part II of RIPA (as amended) 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 has not been identified as an investigative technique applied by the Council, and this document does not therefore go into depth on this topic.

1.7 For each of the above powers, RIPA (as amended) 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 The Investigatory Powers Act 2016 (IPA) also provides for the appointment of an independent Investigatory Powers Commissioner and Judicial Commissioners who will oversee the exercise by public authorities of their powers and duties under the Act (Part 8 of IPA)

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') and the Investigatory Powers Act 2016 ('IPA') contain 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 legislation to support the delivery of their functions. The Investigatory Powers Commissioner's Office oversees the use of covert powers under RIPA by local authorities.

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 (but not intrusive), 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 you 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 legal advice from the Council's lawyers 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 Authorising Officer. This should be done via the Borough Secretary's department who maintain a secure Central Register of all requests for authorisation. (You will be issued with a unique reference number). The Borough Secretary's Department 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. 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 Borough 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 (e.g. in the case of most test purchases), and/or will be going about Council business openly (e.g. a market inspector walking through markets).

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(9)(a) 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 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.

2.3.4 An authorisation may be required if a CCTV camera is to be used for surveillance as part of a specific investigation or operation otherwise than as an immediate reaction to events. In such circumstances either the Council or the police may give the necessary authorisation. If an authorisation is given by the police then a record of the authorisation will be kept to ensure any surveillance is within its terms.

2.3.5 Part II of RIPA applies to the following conduct:

- Directed surveillance;
- Intrusive surveillance; and
- The conduct and use of covert human intelligence sources (CHIS)

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.

2.4.3 Below are some examples where directed surveillance is conducted by the Council:

- Monitoring of noise complaints
- Monitoring of benefit claimants who have not declared that they are working/living with a partner etc
- Surveillance for formal investigations

Please note that the above list is not exhaustive. On reading of this document, managers must consider any actions within their department, which could fall within RIPA.

2.4.4 Where it is anticipated that mobile surveillance will be an integral part of any directed surveillance operation Authorising Officers must be satisfied that it is necessary and the need is proportionate to the investigation being undertaken. Mobile surveillance is a specialist skill and should, at all times, be assessed for risks to health and safety of operatives engaged in this activity. At no times should road traffic laws or regulations be ignored by officers engaged in mobile surveillance. Due regard should be afforded to the driving and surveillance skills of operatives engaged in such activity. Under no circumstances will officers engage in high-speed pursuit of vehicles involved in Directed Surveillance operations.

2.4.5 Where surveillance using airborne crafts or devices, for example helicopters or unmanned aircraft (colloquially known as 'drones'), is planned, this could amount to direct (or even intrusive) surveillance and there will be a requirement to determine whether a surveillance authorisation is appropriate. In considering whether the surveillance should be regarded as covert, account should be taken of the reduced visibility of a craft or device at altitude.

2.5 Intrusive Surveillance – Section 26(3) RIPA

2.5.1 **Local Authorities cannot conduct intrusive surveillance** 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. 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.

2.5.3 The 2010 Legal Consultations Order also provides that any directed surveillance that is carried out on premises ordinarily used for legal consultations, at a time when they are being so used, is to be treated as intrusive surveillance.

2.5.4 The covert recording of noise where the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm), or the recording of verbal content which is made at a level that does not exceed that which can be heard from the street outside or adjoining property with the naked ear, are unlikely to constitute either direct or intrusive surveillance. In the latter circumstance, the perpetrator would normally be regarded as having forfeited any claim to privacy.

2.6 **Interference with property and wireless telegraphy**

Local authorities cannot authorise property interference (entry onto or interference with property or with wireless telegraphy) as regulated by the Police Act 1997, the Intelligence Services Act 1994, and in certain respects the Investigatory Powers Act 2016.

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

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

- they establish or maintain a personal or other relationship with a person for the *covert purpose* of facilitating one or both of the following;

- they covertly use such a relationship to obtain information or to provide access to any information to another person; or

- they covertly disclose 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 the use or disclosure in question.

Further information about the use of CHIS is dealt with in section 3 of this policy.

2.8 **Private Information**

"Private information", in relation to a person, includes any information relating to that person's private or family life. As a result this can include any aspect of a person's private or personal relationships with other, such as family and professional or business relationships.

Although people may have a reduced expectation of privacy in public places, those persons may still have a reasonable expectation of privacy, and covert surveillance of a person's activities in public may still result in obtaining private information. The same principle applies to public areas of the internet, in particular social media sites (concerning which see section 5 of this policy for further guidance).

2.9 **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.

2.10 **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.

2.11 Residential Premises

"Residential premises" means any premises occupied or used, however temporarily, for residential purposes or otherwise as living accommodation. This includes a hotel room or prison accommodation that is occupied or used for residential purposes, but does not include common areas that a person has access to in common with others and in connection with their use of accommodation.

2.12 Right to Privacy

The right to respect for private and family life is enshrined in Article 8 which is set out in Part I of Schedule 1 of the Human Rights Act 1998 as follows:

"Everyone has the right to respect for his private and family life, his home and his correspondence."

The right to privacy is not absolute but is qualified, meaning that it can be interfered with where this is necessary and in accordance with the law. RIPA authorisation amounts to an approved interference.

Great care is required as the right to privacy can also extend to business premises or residential premises used for business purposes. It is essential that Authorising Officers seek legal guidance on this matter prior to authorisation.

2.13 Collateral Intrusion

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

2.13.1 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.

2.13.2 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.

2.14 Authorising Officer

This is the person designated, for the purpose of the Act, to grant authorisation for directed surveillance (which is then subject to judicial approval).

2.15 Investigatory Powers Commissioner's Office

The Investigatory Powers Commissioner's Office is responsible for reviewing our activities carried out under RIPA 2000. All authorities are subject to review and inspection. Inspection will cover policy and procedures as well as individual investigations.

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.

Reference should be made to the more detailed guidance in the Home Office Code of Practice

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 Borough Secretary 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** (see below).

Where confidential material is likely to be particularly sensitive (see below) then the Authorising Officer should be the 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 1st 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. (See paragraph 3.6 for further detail).**

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 a 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 RIPA 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 CHIS.**

This is governed by the Regulation of Investigatory Powers (Juveniles) Order 2000. A person under 16 cannot be used as a 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; and

- 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 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 two-stage process. First, an authorisation must be obtained from an Authorising Officer. Secondly, 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 below). 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.

3.8 **Reviews**

Regular reviews of authorisations should be undertaken by the Authorising Officer to assess whether it remains necessary and proportionate to use a CHIS and whether the authorisation remains justified. The review should include:

(a) the use made of the CHIS during the period authorised

(b) the tasks given to the CHIS

(c) the information obtained from the CHIS

(d) if appropriate to the Authorising Officer's remit, the reasons why executive action is not possible at this stage

The results of a review should be retained for at least five years and particular attention should be given to the need to review authorisations frequently where they involve a high level of intrusion into private life or significant collateral intrusion, or the use of a CHIS may provide access to particularly sensitive information. At the point the Council is considering applying for an authorisation, it must have regard to whether the level of protection to be applied in relation to information obtained under the authorisation is higher because of the particular sensitivity of that information.

In each case, unless specified by the Secretary of State or Investigatory Powers Commissioner, the Authorising Officer within should determine how often a review should take place. This should be as frequently as is considered necessary and proportionate, but should not prevent reviews being conducted in response to changing circumstances.

In the event that there are any significant and substantive changes to the nature of the operation during the currency of the authorisation, the Council should consider whether it is necessary to apply for a new authorisation.

3.9 **Renewals**

CHIS authorisations can be renewed on more than one occasion if necessary and provided that they continue to meet the criteria for authorisation. Before an authorising officer renews an authorisation, they must be satisfied that a review has been carried out of the use of a CHIS and that the results have been considered.

All renewals are subject to authorisation from a Justice of the Peace, and take effect at the time at which the authorisation would have ceased to have effect but for the renewal. Documentation of the renewal should be retained for at least five years.

When deciding if the relevant source is authorised as part of the 'same investigation or operation' in calculating the period of total or accrued deployment or cumulative authorisation periods, the following should be considered:

- common subject or subjects of the investigation or operation
- the nature and details of relationships established in previous or corresponding relevant investigations or operations
- whether or not the current investigation is a development of or recommencement to previous periods of authorisation, which may include a focus on the same crime group or individuals
- previous activity by the relevant source that has a bearing by way of subject, locality, environment or other consistent factors should be considered in calculating the period
- the career history of the relevant source.

All applications for the renewal of an authorisation should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously
- any significant changes to the information in the initial application
- the reasons why it is necessary for the authorisation to continue
- the use made of the CHIS in the period since the grant or, as the case may be, latest renewal of the authorisation
- the tasks given to the CHIS during that period and the information obtained from the use or conduct of the CHIS; and
- the results of regular reviews of the use of the CHIS

3.10 **Cancellation**

The Authorising Officer who granted or renewed the authorisation must cancel it satisfied that the use or conduct of the CHIS no longer satisfies the criteria for

authorisation, or that arrangements for the CHIS's case no longer satisfy the requirements described in section 29 of the 2000 Act. Where the Authorising Officer is no longer available, this duty will fall to the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer.

Where necessary and practicable, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled, and risk assessments should be maintained. The Authorising Officer will wish to satisfy themselves that all welfare matters are addressed, and should make appropriate comment in their written commentary.

4. Authorisation (see flowchart at appendix 5b)

4.1 Authorisation of Surveillance

4.1.1 Since 1st 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 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 two-stage process. First, an authorisation must be obtained from an Authorising Officer. Secondly, approval of the authorisation must be obtained from a Justice of the Peace. This involves applying to a Magistrates Court. Further detail about the judicial approval process is set out in paragraphs 4.1.18 to 4.1.23.

4.1.3 Authorising Officers will be nominated in writing 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 for local authorities

- 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 Borough 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

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

- the nature of the surveillance

- 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 and why such intrusion is justified

- the likelihood of acquiring any confidential or privileged material, and the details of such material

- where the purposes include obtaining information subject to legal privilege, as an explanation as to why there are exceptional and compelling circumstances that make this necessary.

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

- 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. In this respect the Authorising Officer should complete any relevant forms by hand.

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 4.1.17 of this document.

4.1.16 Authorising Officers should not be responsible for authorising their own activities, i.e. those directly involved in undertaking surveillance.

4.1.17 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.	Director, Head of Service , Service Manager or equivalent (SI 2010/521) Officers specifically designated by the Monitoring Officer as Authorising Officers
2	Written authorisation to conduct investigations using Directed Surveillance likely to obtain confidential information.	Head of Paid Service or in his absence, the acting Head of Paid Service

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 he or she is satisfied that they have had appropriate training to undertake the role.

Contact Details for Authorising Officers:

Name	Job Title	E-mail Address	Tel. No.
Phil Harris	Head of Housing and Wellbeing	pharris@northampton.gov.uk	01604 838537
Ruth Austen	Environmental Health and Licensing Manager	rausten@northampton.gov.uk	01604 837794
George Candler	Chief Executive	gcandler@northampton.gov.uk	01604 838725

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

- 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 to 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 of three months beginning with the day on which it took effect

4.2.2 An authorisation for a CHIS will cease to have effect at the end of a period of twelve months beginning with the day it took effect. However, an authorisation concerning a juvenile CHIS will cease to have effect after four months from the date it took effect

4.2.3 An authorisation under which it is intended to obtain, provide access to or disclose knowledge of matter subject to legal professional privilege is instead 3 months for the Council

4.2.4 Urgent oral authorisations will unless renewed cease to have effect after 72 hours

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, as listed in section 4.1.5 above together with

(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 or the conduct of the CHIS 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. Further, where necessary and practicable, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled, and risk assessments maintained. In the context of CHIS the Authorising Officer will want to satisfy themselves that all welfare matters are addressed, and should make appropriate comment in their written commentary.

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 Investigatory Powers Commissioner.

4.5 Reviews

4.5.1 Authorising Officers will review all "Directed Surveillance" and CHIS applications and authorisations that they have granted regularly to assess whether they remain necessary and proportionate. 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:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously

- 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 three 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 A record of the following information pertaining to all authorisations shall be centrally retrievable within the Council for a period of at least three years from the ending of each authorisation. This information should be regularly updated whenever an authorisation is granted, renewed or cancelled and should be made available to the Investigatory Powers Commissioner and inspectors who support the work of the Commissioner upon request. More guidance on the recording of magistrates' decisions is available in Home Office-issued guidance available on the .gov.uk website.

- the type of authorisation/warrant

- the date the authorisation was given

- name and rank/grade of the authorising officer

- the unique reference number (URN) of the investigation or operation (if applicable)

- the title of the investigation or operation, including a brief description and names of subjects, if known

- whether the urgency provisions were used, and if so why

- details of attendances at the magistrates' court to include the date of attendances at court, the determining magistrate, the decision of the court and the time and date of that decision

- the dates of any reviews

- if the authorisation has been renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer

- whether the authorised activity is likely to result in obtaining confidential or privileged information

- whether the authorisation was granted by an individual directly involved in the investigation

- the date the authorisation was cancelled

- where any application is refused, the grounds for refusal as given by the issuing authority or Judicial Commissioner

- a record of whether, following a refusal of any application by a Judicial Commissioner, there is an appeal to the Investigatory Powers Commissioner

- where there is such an appeal and the Investigatory Powers Commissioner also refuses the issuing of an application, the grounds for refusal given

4.6.4 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.

4.6.5 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.

4.6.6 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.

4.6.7 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.

4.6.8 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.

4.6.9 A copy of all authorisations must be sent to the Borough Secretary, so that there is a central record maintained, and so that in his role as the Monitoring Officer he can ensure the Act is being complied with.

Authorisation forms are also open to inspection by the Investigatory Powers Commissioners.

4.7 Monitoring of Authorisations

Information must be supplied to the Monitoring Officer using the forms attached to this guidance. The Monitoring Officer 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 Monitoring Officer 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 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 Investigatory Powers Commissioner's Office has a duty to keep under review the exercise and performance of the Council of its surveillance powers. The Investigatory Powers Commissioner's Office 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 **Errors**

Regular reviews of errors will be undertaken with a written record made of each review.

An error must be reported if it is a "relevant error", which is defined under section 231(9) of the IPA as being any error by the Council in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This would include compliance by public authorities with Part II of RIPA. Examples of relevant errors occurring would include circumstances where:

- Surveillance or Covert Human Intelligence Source activity has taken place without lawful authority

- There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Codes

All relevant errors made by the Council of which it is aware must be reported to the IPC as soon as reasonably practicable, and no later than ten working days (or as agreed with the Commissioner). Where the full facts of the error cannot be ascertained within that time, an initial notification must be sent with an estimated timescale for the error being reported in full and an explanation of the steps being undertaken to establish the full facts of the error.

From the point at which the Council identifies that a relevant error may have occurred, it must take steps to confirm the fact of an error as quickly as it is reasonably practicable to do so. Where it is subsequently confirmed that an error has occurred and that error is notified to the Commissioner, the Council must also inform the Commissioner of when it was initially identified that an error may have taken place.

A full report must be sent to the Investigatory Powers Commissioner as soon as reasonably practicable in relation to any relevant error, including details of the

error and, where it has not been possible to provide the full report within ten working days (or as agreed with the Commissioner) of establishing the fact of the error, the reasons this is the case. The report should include information on the cause of the error; the amount of surveillance conducted and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

The Investigatory Powers Commissioner may issue guidance as necessary, including guidance on the format of error reports. The Council must have regard to any guidance on errors issued by the Investigatory Powers Commissioners.

4.10 **Serious Errors**

If the Investigatory Powers Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error, they must inform them. An error is a serious error where it is considered to have caused significant prejudice or harm to the person concerned.

In deciding whether it is in the public interest for the person concerned to be informed of the error, the Commissioner must in particular consider:

- The seriousness of the error and its effect on the person concerned
- The extent to which disclosing the error would be contrary to the public interest or prejudicial to:
    - national security
    - the prevention or detection of serious crime
    - the economic well-being of the United Kingdom
    - the continued discharge of the functions of any of the security and intelligence services

Before making his or her decision, the Commissioner must ask the Council to make submissions on the matters concerned, and the Council must take all such steps as notified to them by the Investigatory Powers Commissioner to help identify the subject of a serious error.

When informing a person of a serious error, the Commissioner must inform the person of any rights that the person may have to apply to the Investigatory Powers Tribunal, and provide such details of the error as the Commissioner considers to be necessary for the exercise of those rights.

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 he/she may notify the Investigatory Powers Commissioner immediately

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

5.4 Where it is intended to access a social media or other online account to which the Council has been given access with the consent of the owner, the Council will still need to consider whether the account(s) may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for a directed surveillance authorisation should be considered, particularly (though not exclusively) where it is intended to monitor the account going forward.

5.5 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.

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

- Whether the investigation or research is directed towards an individual or organisation

- Whether it is likely to result in obtaining private information about a person or group of people

- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile

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

5.6 The Home Office Codes of Practice on covert surveillance and CHIS contain essential guidance in relation to online covert activity and must be consulted.

5.7 To ensure that no unauthorised online covert activity takes place within the Council, please ensure that legal advice is sought from LGSS Law.

6. Safeguards

6.1 Material obtained through surveillance may include private information, legally privileged information, or other confidential material including journalistic material and constituency business of Members of Parliament.

6.2 The Council must ensure that any information it obtains through surveillance is handled in accordance with the safeguards the Council has put in place, any relevant frameworks (such as data protection), and the Home Office Codes.

6.3 Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. Something is necessary for the authorised purposes where the material:

(a) is (or is likely to become) necessary for the surveillance purposes set out in the legislation

(b) is necessary for facilitating the carrying out of the functions of the Council under the surveillance legislation

(c) is necessary for facilitating the carrying out of any functions of the Commissioner or Investigatory Powers Tribunal

(d) is necessary for the purposes of legal proceedings

(e) is necessary for the performance of the functions of any person by or under any enactment

Evidence

6.4 When information obtained under a surveillance authorisation is used evidentially, the Council should be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

6.5 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements.

Reviews

6.6 As set out at sections 3.8 and 4.5 of this document and within the Home Office Codes, regular reviews of all authorisations should be undertaken during their lifetime to assess the necessity and proportionality of the conduct. Particular attention should be given to the need to review authorisations frequently where they involve a high level of intrusion into private life or significant collateral intrusion, or particularly sensitive information is likely to be obtained.

Dissemination of information

6.7 The Council will likely need to share information obtained through surveillance within the Council and between the Council and other public bodies where legally necessary. This must be limited to the minimum necessary. If a summary of the information will be sufficient to meet necessity, no more than that should be disclosed.

6.8 When sharing this type of information the Council will ensure that it has appropriate safeguards and agreements in place to ensure compliance.

Copying

6.9 Information and material obtained through surveillance must only be copied to the extent necessary. Copying includes direct copies as well as summaries and extracts.

Storage

6.10 All information and material obtained through surveillance and all copies, extracts or summaries must be stored securely to minimise the risk of theft or loss. Only those with appropriate legal authority and security clearance should be able to access the information.

6.11 The Council will ensure that it has in place:

(a) physical security to protect premises where the information is stored or can be accessed

(b) IT security to minimise risk around unauthorised access to IT systems

(c) An appropriate security clearance regime to provide assurance that those who have access to the information are reliable and trustworthy

Destruction

6.12 Information obtained through surveillance, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose(s). If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid.

Confidential or privileged information

6.13 Where the material contains information that is legally privileged, confidential journalistic material or where material identifies a journalist's source, where material contains confidential personal information or communications between a Member of Parliament and another person on constituency business, authorisations can only be granted by the Head of Paid Service.

6.14 Where there is a renewal application in respect of an authorisation which has resulted in the obtaining of confidential or legally privileged items, that fact should be highlighted in the renewal application.

Confidential personal information and confidential constituent information

6.15 Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relates to his or her physical or mental health or to spiritual counselling. Such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or any legal obligation of confidentiality. For example, confidential personal information might include consultations between a health professional and a patient, or information from a patient's medical records.

6.16 Confidential constituent information is information relating to communications between a Member of Parliament and a constituent in respect of constituency business. Again, such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

6.17 The reasons for acquiring information of this type must be clearly documented and the specific necessity and proportionality of doing so must be carefully considered.

6.18 Material which has been identified as confidential personal or confidential constituent information should be retained only where it is necessary and proportionate to do so in accordance with the authorised purpose or where otherwise required by law. It should be securely destroyed when its retention is no longer needed for those purposes.

6.19 Where confidential personal or constituent information is retained or disseminated to an outside body, reasonable steps should be taken to mark the information as confidential. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of confidential information, advice should be sought from a legal adviser to the Council before any further dissemination of the material takes place.

6.20 Any case where confidential personal or constituent information is retained, other than for the purpose of destruction, and disseminated should be reported to the Investigatory Powers Commissioner as soon as reasonably practicable, and any material which has been retained should be made available to the Commissioner on request so that the Commissioner can consider whether the correct procedures and considerations have been applied.

Applications to acquire material relating to confidential journalistic material and journalist sources

6.21 There is a strong public interest in protecting a free press and freedom of expression in a democratic society, including the willingness of sources to provide information to journalists in confidence.

6.22 Confidential journalistic material 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 such an undertaking. Confidentiality can continue to attach to confidential journalistic material when it is sent to or held by a person who is neither the journalist nor the source (for example, a news editor who has been sent some notes by a journalist).

6.23 An application for authorisation where the purpose, or one of the purposes, of the authorisation is to authorise the acquisition of material of this type must contain a statement in those terms. The person to whom the application is made may issue the authorisation only if they consider that appropriate safeguards relating to the handling, retention, use and disclosure of the material are in place.

6.24 When this type of material is retained and disseminated to an outside body, reasonable steps should be taken to mark it as confidential. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of such information, advice should be sought from a legal adviser to the Council before any further dissemination of the content takes place.

6.25 Where this type of information has been obtained and retained, other than for the purposes of destruction, the matter should be reported to the Commissioner as soon as reasonably practicable.

Items subject to legal privilege

6.26 The acquisition of material subject to legal privilege is particularly sensitive and is therefore subject to additional safeguards which provide for three different circumstances where legally privileged items will or may be obtained. They are:

(a) where privileged material is intentionally sought

(b) where privileged material is likely to be obtained

(c) where the purpose or one of the purposes is to obtain items that, if they were not generated or held with the intention of furthering a criminal purpose, would be subject to privilege

6.27 Further details and guidance about each of the above circumstances are set out in the Home Office Codes.

Covert surveillance of legal consultations

6.28 The 2010 Legal Consultations Order provides that surveillance that is carried out in relation to anything taking place on so much of any premises specified in article 3(2) of the Order as is, at any time during the surveillance, used for the purposes of 'legal consultations', shall be treated for the purposes of Part II of RIPA as intrusive surveillance. **As a result, such authorisations are not available to the Council.**

Lawyers' material

6.29 Where a lawyer, acting in this professional capacity, is the subject of surveillance, it is possible that a substantial proportion of any material which will or could be acquired will be subject to legal privilege. In addition to considering the applicability of the 2010 Legal Consultations Order, the Council will need to consider which of the three circumstances that apply when items subject to legal privilege will or may be obtained is relevant, and what processes should therefore be followed.

6.30 Any case involving lawyers' material should also be notified to the Commissioner during their next inspection, and any material which has been retained should be made available to the Commissioner on request.

Handling, retention, and deletion of legally privileged material

6.31 Additional arrangements apply to legally privileged items where the intention is to retain them for a purpose other than their destruction:

(a) A legal adviser to the Council must be consulted and is responsible for determining whether that material is privileged;

(b) Material which has been identified as legally privileged (and is being retained for purposes other than its destruction) should be clearly marked as subject to legal privilege; and

(c) the Investigatory Powers Commissioner must be notified of the retention of the items as soon as reasonably practicable.

7. Complaints

7.1 **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 legislation.

Contravention of the RIPA or the IPA (and associated legislation) may be reported to the Investigatory Powers Commissioner at:

Investigatory Powers Commissioner's Office
PO Box 29105
London
SW1V 1ZU

Email: info@ipco.org.uk

Telephone: 0207 389 8999

7.2 Contravention of the Data Protection Act 2018 and/or GDPR may also be reported to the Information Commissioner.

7.3 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. To request a complaints form, please contact the Monitoring Officer/Complaints Officer, Northampton Borough Council, The Guildhall, St Giles Square, Northampton NN1 1DE or telephone 01604 837334.

Please ensure that this Guidance and the Home Office Codes of Practice are available at all offices involved in surveillance operations, and also available for public inspection in each department.

APPENDIX 1

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.
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).***
8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. 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?
10. Confidential information. **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. **Explain <u>why</u> you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out.**

14. (Confidential Information Authorisation) Supply detail demonstrating compliance			
Date of first review			
Programme for subsequent reviews of this authorisation: 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)			

Operation Reference Number* (*Filing Ref)	

APPENDIX 2

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**

Operation Reference Number* (*Filing Ref)	

APPENDIX 2

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.

Operation Reference Number* (*Filing Ref)	

APPENDIX 2

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>

Operation Reference Number* (*Filing Ref)	

APPENDIX 2

9. Authorising Officer's Statement.	
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 Date
Signature	
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

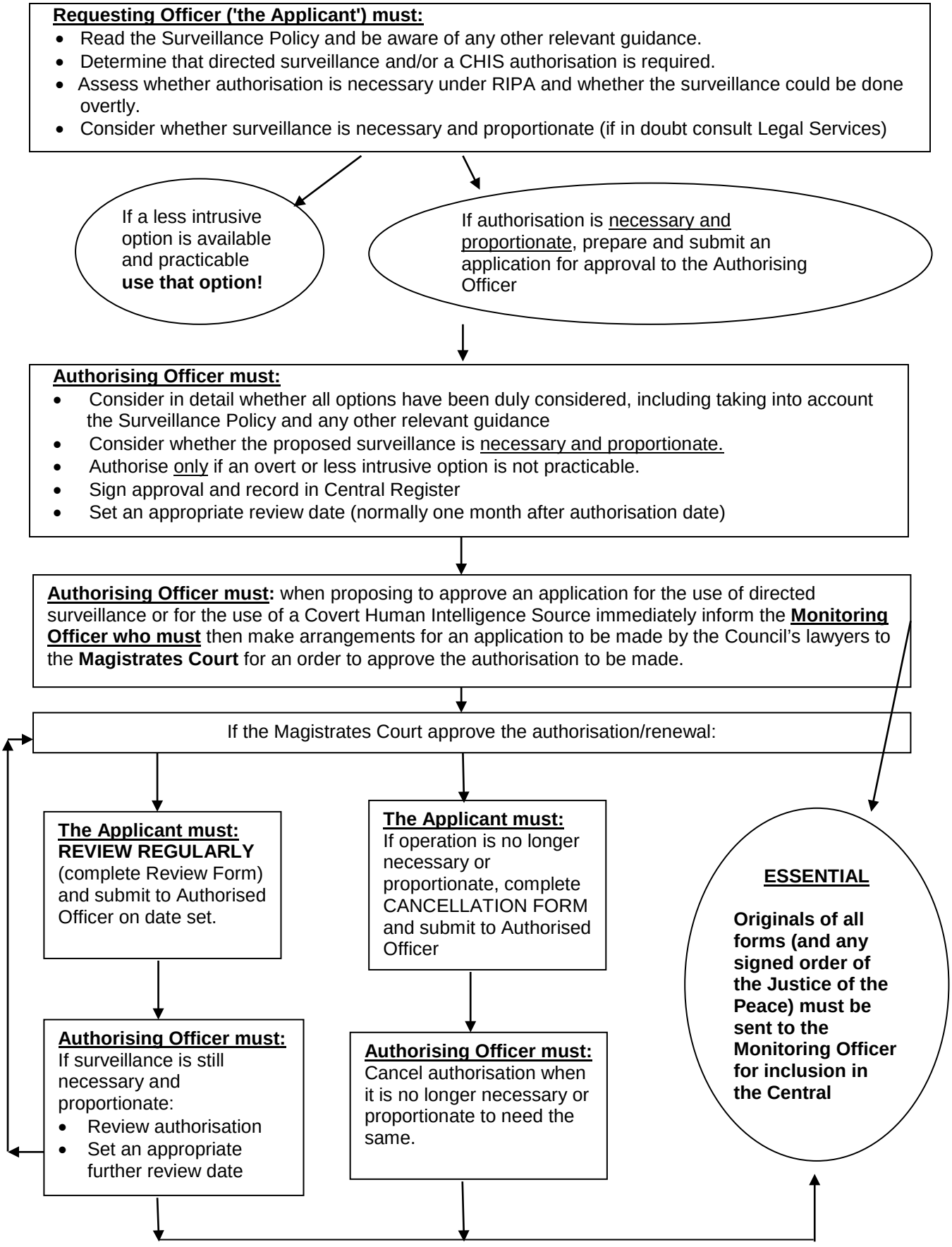
7. Applicant's Details			
Name (Print)		**Tel No**	
Grade/Rank		**Date**	
Signature			

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.	

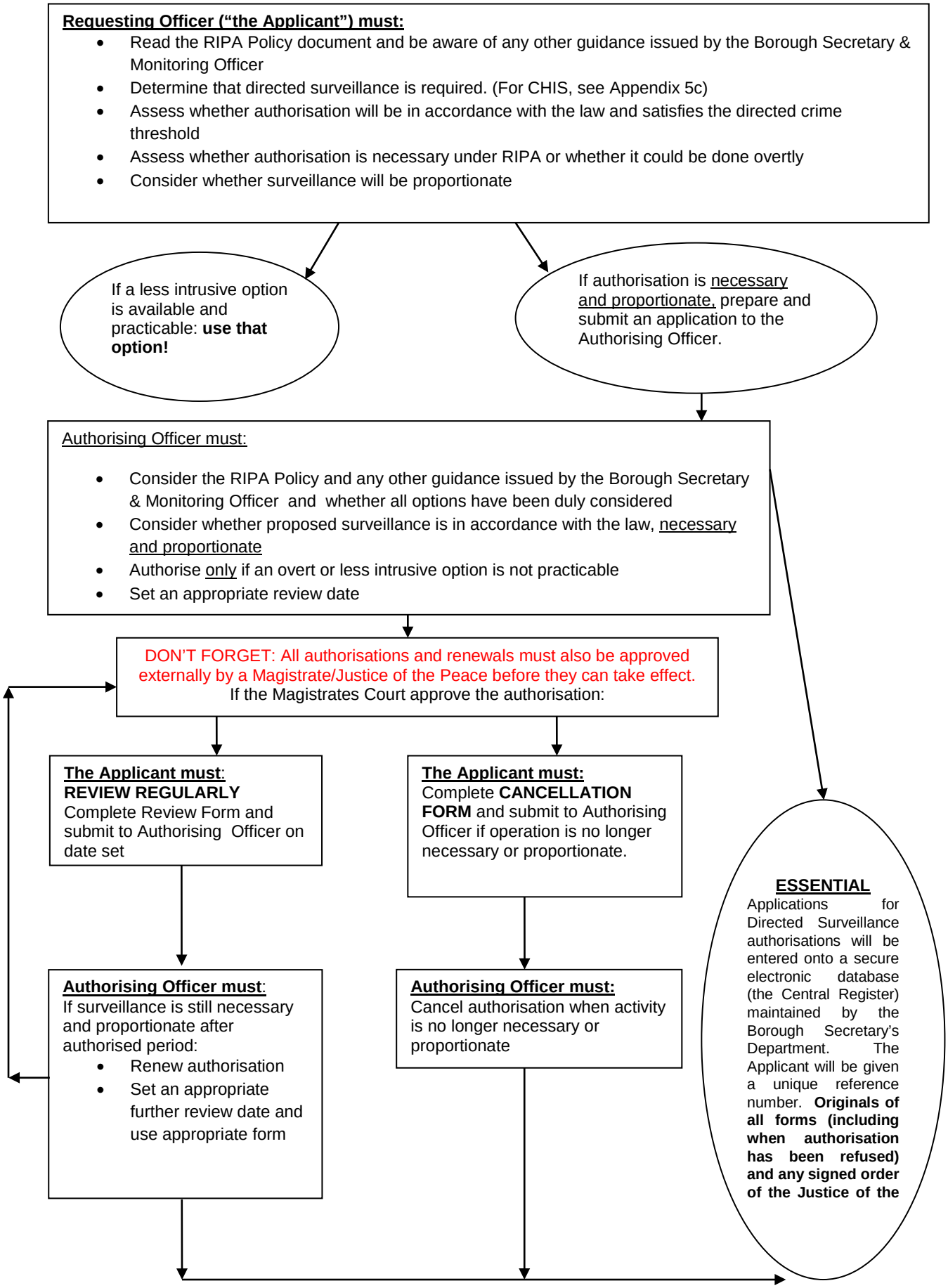
FLOW-CHART – AUTHORISATION PROCEDURES - GENERAL **APPENDIX 5a**



NB: If in doubt, seek advice from the Borough Solicitor / Monitoring Officer BEFORE any directed surveillance and or CHIS is authorised, renewed, cancelled, or rejected.

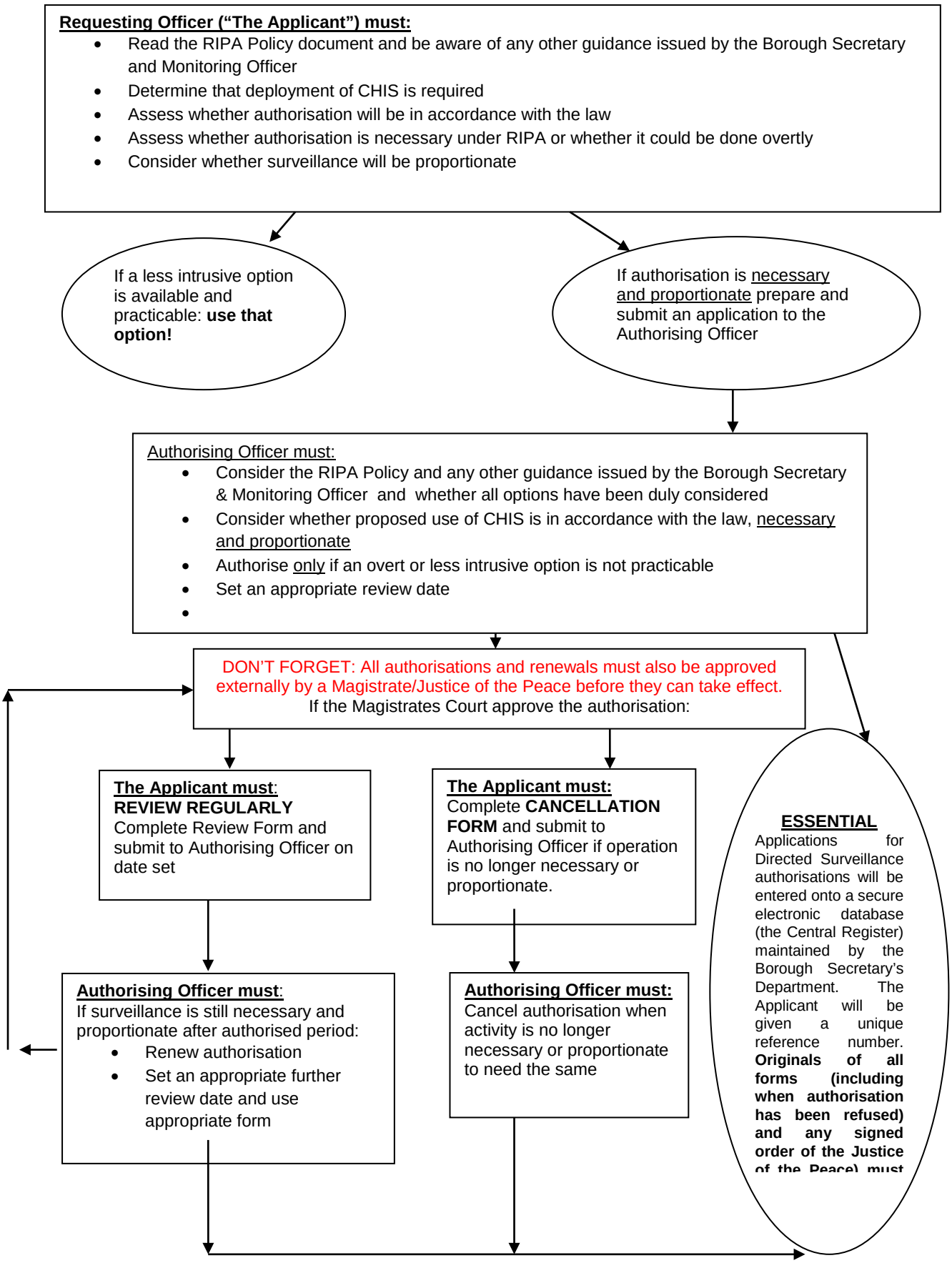
FLOW-CHART – DIRECTED SURVEILLANCE AUTHORISATION PROCEDURES

APPENDIX 5b



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.....

.....

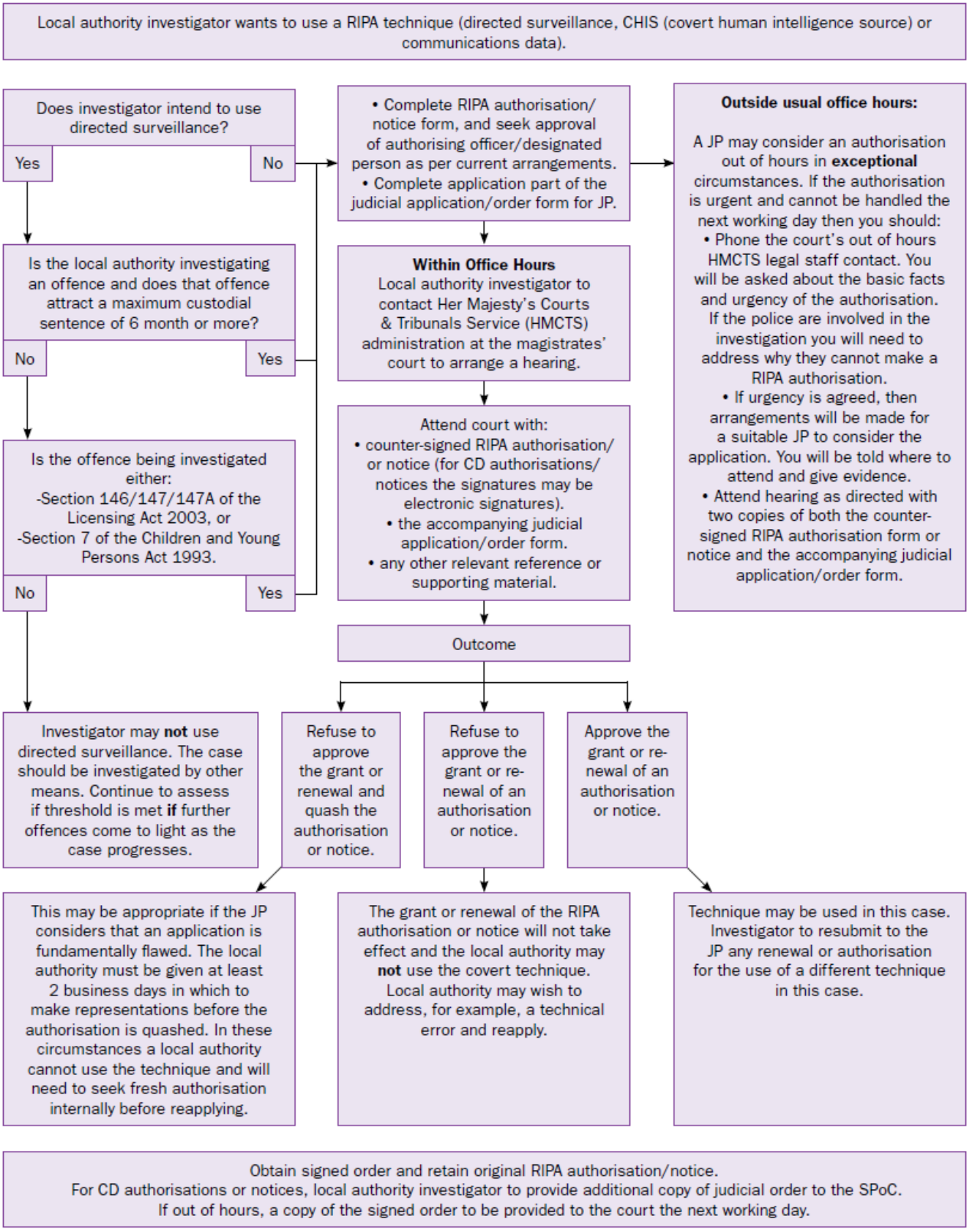
Contact telephone number …….....

Contact email address (optional) …….....

Local authority reference …….....

Number of pages …….....

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".*