Regulation of Investigatory Powers Act (RIPA)Policy

July 2023

Contents

Section		Page
1.	Introduction to RIPA 2000	3
2.	Definitions	4 - 8
3.	The Use of a Covert Human Intelligence Source (CHIS)	9 - 14
4.	Authorisation of Surveillance	15 - 23
5.	Social Networking Sites (SNS)	24 - 26
6.	Non-RIPA Surveillance Activity	27 - 28
7.	Complaints	29

Appendix	Appendix content	
1	Standard Form – Application for authorisation to carry out Directed surveillance	30 - 35
2	Standard Forms – Application for renewal of a Directed Surveillance Authorisation	36 - 39
3	Standard Forms – Cancellation of a Directed Surveillance Authorisation.	40 - 41
4	Standard Forms – Review of a Directed Surveillance Authorisation.	42 - 44
5	List of Senior Authorising Officers Authorising Officers, Senior Responsible Officer and RIPA Monitoring Officer	45
6	RIPA Management Structure	46
7	Flow Chart for Directed Surveillance and CHIS	47
8	Additional Notes for the Use and Management of CHIS	48
9	CHIS Awareness Diagram	49

1. Introduction

Regulation of Investigatory Powers Act 2000

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) provides a 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 The policy should be read in conjunction with the Home Office Codes of Practice on covert surveillance and covert human intelligence sources; acquisition and disclosure of communications data, and any guidance issued by the Investigatory Powers Commissioner's Office (IPCO)

1.3 As a local authority, Thanet District Council ("The council") is only authorised to carry out Directed Surveillance and use Covert Human Intelligence Sources (CHIS), in accordance with section 28 and section 29 of RIPA. This Policy covers the use of Directed Surveillance and the deployment of Covert Human Intelligence Sources by the Council.

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

1.5 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.

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

1.7 The Council will not normally authorise the use of a CHIS. However, in the rarest of circumstances, an investigation may require the use of a CHIS, and in this case, officers should seek the proper authorisation in accordance with this policy.

1.8 It should be noted that any use of activities under RIPA will be as a last resort and council policy is not to undertake such activities unless absolutely necessary.

1.9 The provisions of RIPA do not cover authorisation for the use of overt CCTV surveillance systems. The Council operates an overt policy of providing signage information for all overt CCTV cameras within public places, ensuring the public are aware of their operation and who is responsible for the system.

2. Definitions

2.1 What is Surveillance?

Surveillance is:

- Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications
- Recording anything monitored, observed or listened to in the course of surveillance
- Surveillance by or with the assistance of appropriate surveillance device(s).

Surveillance can be overt or covert.

2.2 Overt Surveillance

2.2.1 Most of the surveillance carried out by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases, officers will be behaving in the same way as a normal member of the public and/or will be going about Council business openly.

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

2.3 Covert Surveillance

2.3.1 Covert Surveillance is defined in Section 26 RIPA as follows:

> "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 form of activity will not usually be regulated under the provisions of RIPA.

2.3.3 The installation of CCTV cameras for the purpose of generally observing activity in a particular area with signage is not surveillance which requires authorisation. Members of the public are aware that such systems are in use, for their own protection and to prevent crime.

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

Part II of RIPA applies to the following conduct:

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

2.4 Directed Surveillance Section 26(2) RIPA

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

2.4.2 Directed surveillance is conducted where it involves the observation of a person or persons with the intention of gathering **private information** to produce a picture of a person's life, activities or associations. However, it does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, enforcement officers would not require authorisation to conceal themselves and observe a suspicious person who they come across in the course of their normal duties. However the longer the observation continues, the less likely it would be considered to be an immediate response.

2.5 Intrusive Surveillance – Section 26(3) RIPA

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

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

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

2.5.4 The covert recording of suspected noise nuisance where the intention is only to record excessive noise levels from adjoining premises and the recording device is calibrated to record only excessive noise levels constitutes neither directed nor intrusive surveillance. In such

circumstances, the perpetrator would normally be regarded as having forfeited any claim to privacy, and an authorisation may not be necessary.

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

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

- he establishes or maintains a personal or other relationship with a person for the *covert purpose* of facilitating one or both of the following;
- he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
- he covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

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

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

2.7 Private Information

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

As a result, private information is capable of including any aspect of a person's private or personal relationship with others, such as family and professional or business relationships.

Information which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, websites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public.

2.8 Private Vehicle

"Private Vehicle" means any vehicle that is used primarily for the private purpose of the person who owns it or of a person otherwise having the right to use it. This does not include a person whose right to use the vehicle derives only from his having paid, or undertaken to pay, for the use of the vehicle and its driver for a particular journey. A vehicle includes any vessel, aircraft or hovercraft.

2.9 Confidential Material

This consists of

- **Matters subject to legal privilege** - for example, oral and written communications between a professional legal adviser and his client or any person representing his client, made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications. Communications and items held with the intention of furthering a criminal purpose are not subject to legal privilege where there is evidence that the professional legal advisor intends 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.

- 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.

2.10 Collateral Intrusion

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

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

2.12.2 Measures should be taken, wherever practicable, to avoid or minimise the unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance activity. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided the intrusion is 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.

2.11 Authorising Officer

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

2.12 The Investigatory Powers Commissioners Office (IPCO)

IPCO 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)

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 covert activity. There will be the person who completes and signs the application form by which authorisation is applied for and the Authorising Officer (legal advice must be sought via the Council's RIPA Gate-keeper before embarking on a CHIS authorisation) to whom the form must be submitted for consideration.

Where confidential material is likely to be acquired then the Authorising Officer must be the Head of Paid Service, or in his/her absence the person acting as the Head of Paid Service 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

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 The authorisation process for use of a CHIS must be approved by 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 CHIS without there having been prior planning within the investigating department/section. It is important to realise that it may well be a member of staff of the department and, indeed, an investigator him or herself, who becomes the source, depending on the manner of working used. It is not only persons outside the employ of the local authority who may be used as a source. If it is intended to make use of CHIS, then appropriate and specific training should be arranged for the officers responsible for the functions under section 29(5) (a) to (c) of the Act and also for any officer of the Council who is to be the CHIS.

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

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

3.4 Children as Juvenile CHIS and vulnerable adults as CHIS.

This is governed by the Regulation of Investigatory Powers (Juveniles) Order 2000.

Special safeguards apply to the authorisation of children as CHIS. These safeguards recognise that children are likely to be more vulnerable than adults due to their age and level of maturity, and that enhanced protections are appropriate to ensure their safety and welfare.

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

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

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

The need to safeguard and promote the best interests of the child is a primary consideration in all such CHIS deployments, both when deciding whether to grant the authorisation and during the conduct of any subsequent operation.

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.

Special safeguards apply to the authorisation of a vulnerable adult as a CHIS.

A vulnerable adult is a person aged 18 or over who by reason of mental disorder or vulnerability, other disability, age, or illness, is or may be unable to take care of themselves or unable to protect themselves against significant harm or exploitation.

Where it is known or suspected that an adult may be vulnerable, they should only be authorised to act as a CHIS in exceptional circumstances.

As with confidential information, the authorisation of the Head of Paid Service, or the person acting as the Head of Paid Service 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.

The Investigatory Powers Commissioner must be informed within seven working days of a CHIS authorisation of a vulnerable adult or a juvenile source.

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

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

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

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

3.6 Judicial Approval of CHIS authorisations

3.6.1 Local authorities must obtain an order from a Justice of the Peace to approve the grant or renewal of an authorisation. 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 The requirements to internally assess necessity and proportionality, complete the RIPA authorisation/application forms and seek approval from an Authorising Officer remain. Therefore, there is a three-stage process. First, advice and URN will need to be obtained from the Council's RIPA Gatekeeper. Secondly, an authorisation must be obtained from an Authorising Officer. Thirdly, approval of the authorisation must be obtained from a Justice of the Peace. This involves applying to a Magistrates Court.

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

- at the time the Authorising Officer granted the authorisation, there were reasonable grounds for believing that the authorisation was necessary and that the activity being authorised was proportionate, that arrangements existed that satisfied section 29(5) (see paragraph 3.3), that the Authorising Officer was a designated person for the purposes of section 29 of RIPA, that the grant of the authorisation was not in breach of any restrictions imposed by virtue of section 29(7)(a) or 30(3) of RIPA, that any other conditions provided for by any Order were satisfied; and

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

3.7 CHIS Record Keeping

Records should be kept as prescribed by the Code of Practice (please see paragraph on Records and Documentation above). Where a source wearing or carrying a surveillance device is invited into residential premises or a private vehicle and records activity taking place inside those premises or vehicles, 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 vehicles as a means of installing equipment. If equipment is to be used other than in the presence of the covert source, an intrusive surveillance authorisation is necessary, which cannot be granted by the local authority.

4. Authorisation

4.1 Authorisation of Surveillance

4.1.1 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 advice from the Council's RIPA Gate-keeper and/or legal services early on and consult the Monitoring Officer as appropriate.

4.1.2 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 is an additional step after assessing necessity and proportionality, completing the RIPA application forms and seeking authorisation from an Authorising Officer.

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

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

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

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

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

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

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

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

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

- an account of the investigation or operation;

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

- any potential for collateral intrusion;

- the likelihood of acquiring any confidential material.

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

Standard Document: See Appendix 1 – Surveillance Application Form

4.1.6 The Directed Surveillance Crime Threshold means that the Council may continue to authorise the use of Directed Surveillance in more serious cases provided the other tests are met (i.e. 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 are 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 be satisfied 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 consider 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 subject 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 harm;
- explaining how and why the methods adopted will cause the least possible intrusion on the subject and others
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; and
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

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

4.1.11 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.

4.1.15 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 normally be responsible for authorising operations in which they are directly involved,

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.	CEX, Corporate Director, Service Director as Authorising Officers
2	Written authorisation to conduct investigations using Directed Surveillance likely to obtain confidential information.	CEX only or in their absence, or (in their absence) the person acting as the 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".

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. 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.

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

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

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

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

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

4.1.20 Authorising Officers must be aware that each authorisation (or renewal of an authorisation) will be subject to judicial approval.

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

4.1.22 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 flowchart 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 unless otherwise directed by the court at the time of authorising the application.

4.3 Renewals

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

4.4 Cancellations

4.4.1 The Authorising Officer must cancel an authorisation if he/she is satisfied that the Directed Surveillance no longer meets the criteria for authorisation. When cancelling an authorisation, an Authorising Officer

must ensure that proper arrangements have been made for the activity's discontinuance, including the removal of technical equipment and directions for the management of the product.

Standard Document: See Appendix 3 – Surveillance Cancellation form.

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

4.5 Reviews

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

4.5.2 Reviews of authorisation for Directed Surveillance must record:

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

Standard Document: See Appendix 4 – Monthly Review Form

4.6 Records and Documentation

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

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

4.6.3 If there is any reason to believe that the results obtained during the course of the investigation might be relevant to that investigation or to another investigation or to pending or future civil or criminal proceedings then it should not be destroyed but retained in accordance with established disclosure requirements. Particular attention is drawn to the requirements

of the Code of Practice issued under the Criminal Procedure and Investigations Act 1996, which requires that material should be retained if it forms part of the unused prosecution material gained in the course of an investigation or which may be relevant to an organisation.

4.6.4 Authorising Officers are reminded of the importance of safeguarding confidential and sensitive information. They must also ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities in the handling and storage of material. Where material is obtained by surveillance, which is wholly unrelated to a criminal or other investigation or to any person who is subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be destroyed immediately. Consideration of whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer.

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

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

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

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

4.6.8 A copy of all authorisations must be sent to the Council's RIPA Gatekeeper, so that there is a central record maintained.,

Authorisation forms are also open to inspection by IPCO.

4.7 Monitoring of Authorisations

Information must be supplied to the Council's RIPA Gatekeeper using the forms attached to this guidance. The Gatekeeper will maintain a Central Register of all forms completed by the Authorising Officer.

A review will be carried out regularly to ensure all forms have been sent for inclusion in this Central Register.

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.
    - Authorising officers, through the Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 2018

The Gate-keeper/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 Commissioners Officer (IPCO) has a duty to keep under review the exercise and performance of the Council of its surveillance powers. The Investigatory Powers Commissioners Office will regularly inspect the Council and may carry out spot checks unannounced.

4.8 Material acquired under RIPA - Review, Retention & Destruction (RRD)

All material obtained under a RIPA authorisation must be reviewed to determine if it needs to be retained or destroyed. Covertly obtained material can be retained if there are ‘relevant grounds’ for doing so or destroyed if the material acquired is no longer needed.

If an initial decision is made to retain the material, then a rolling three-year review period will be used to consider whether the material should be retained or destroyed.
All covertly obtained must be managed in accordance with the relevant Code of Practice.

IPCO has also introduced their Data Assurance Programme, which will form part of all future inspections undertaken by them. The purpose of the IPCO Data Assurance Programme applies to data obtained under the Investigatory Powers Act (IPA) 2016 and the Regulation of Investigatory Powers Act (RIPA) 2000 and which is, therefore, the subject of oversight by IPCO. This programme is intended

to promote compliance with the IPA and RIPA and the Codes of Practice and with other legal obligations, including the Data Protection Act (DPA) 2018.

IPCO has set six areas which will be inspected upon and the council will ensure that these are all considered when undertaking the covert activity. These are:
1. Review the safeguarding obligations in the relevant Code of Practice for any powers used by your authority.
2. Ensure that internal safeguard policies for retaining, reviewing and disposing of any relevant data are accurate and up-to-date.
3. Ensure that the authorising officer for your authority has a full understanding of any data pathway used for RIPA or IPA data.
4. Ensure that all data obtained under IPA and RIPA is clearly labelled and stored on a data pathway with a known retention policy.
5. Review the wording of safeguards in any applications to obtain data under IPA and RIPA and ensure that they accurately reflect the retention and disposal processes at your authority.
6. Review whether data obtained under previous authorisations is being retained for longer than is necessary and, if appropriate, consider disposing of retained data.

Responsibility for ensuring that material is managed correctly rests with the Authorising Officer that granted the authorisation or in the event they are no longer performing that role, the person that took over their role.

4.9 Refusals

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

4.10 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 (see following)

5. Social Networking Sites (SNS)

5.1 The Home Office Revised Code of Practice on Covert Surveillance and Property Interference, published in 2018, provides the following guidance in relation to online covert activity:

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

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, as set out elsewhere in this code. 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 (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

As set out below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

Where information about an individual is placed on a publicly accessible database, for

example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

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

5.3 It is recognised that the use of SNS can provide useful information for council staff carrying out investigations. These investigations may relate to the various enforcement functions within the council, for example, fraud, planning enforcement, licensing or environmental health/crime.

5.4 SNS can take many forms. This makes defining SNS difficult, however, there are some facets which will be common to all forms of SNS. They will always be a web-based service that allows individuals and/or businesses to construct a public or semi-public profile. Beyond this, SNS can be very diverse but will often have some, or all, of the following characteristics:

- The ability to show a list of other users with whom they share a connection, often termed “friends” or “followers”;
- The ability to view and browse their list of connections and those made by others within the system;
- Hosting capabilities allowing users to post audio, photographs and/or video content that is viewable by others; and
- Take the form of community-based web sites, online discussion forums, chatrooms and other social spaces online.

5.5 Current examples of the most popular forms of SNS, and therefore the most likely to be of use when conducting investigations into alleged offences, include: Facebook; Twitter; YouTube; Instagram; LinkedIn; and Google.

5.6 The Council may utilise SNS when conducting investigations into alleged offences. Whilst the use of SNS to investigate an alleged offence is not automatically considered covert surveillance, its misuse when conducting investigations can mean that it crosses over into the realms of covert and/or directed surveillance, even when that misuse is inadvertent. It is, therefore, crucial that the Home Office Code of Practice and provisions

within the RIPA, as they relate to covert and directed surveillance, are always followed when using SNS information in investigations.

5.7 It is the aim of this Policy to ensure that investigations involving the use of SNS are done so lawfully and correctly so as not to interfere with an accused's human rights and to protect officers carrying out the investigation, and to ensure where RIPA authorisation if required, is obtained in advance of the evidence being gathered.

5.8 When it is discovered that an individual under investigation has set their SNS account to private, Council officers should not attempt to circumvent those settings under any circumstances. Such attempts would include, but are not limited to:

- sending "friend" or "follow" requests to an individual for the purpose of gathering information;
- setting up or using bogus Social Media profiles to gain access to the individual's private profile,
- contacting the individual through any form of instant messaging or chat function requesting access or information,
- asking family, friends, colleagues or any other third party to gain access on their behalf, or otherwise using the SNS accounts of such people to gain access;
- or any other method which relies on the use of subterfuge or deception.

5.9 A distinction is made between one-off and persistent viewing of an individual's SNS profile. Under Part II of RIPA, authorisation must be sought in order to carry out directed surveillance against an individual. Whilst one-off visits are unlikely to be considered "directed surveillance" for the purposes of RIPA, persistent viewing or frequent visits may cross over into becoming "directed surveillance" requiring RIPA authorisation. A person's SNS profile should not, for example, be routinely monitored on a daily or weekly basis in search of updates, as this will require RIPA authorisation. Similarly, if an officer intends to engage with others online without disclosing their identity a CHIS (Covert Human Intelligence Source) authorisation may be needed. For further guidance on these points, officers should contact the Council's SRO.

5.10 Regardless of whether the Social Media profile belonging to a suspected offender is set to public or private, it should only ever be used for the purposes of evidence gathering. Interaction or conversation of any kind should be avoided at all costs, and at no stage should a Council officer seek to make contact with the individual through the medium of social media. Any contact that is made may lead to accusations of harassment or, where a level of deception is employed by the officer, entrapment, either of which would be detrimental or potentially fatal to any future prosecution that may be considered.

6. Non-RIPA Surveillance Activity

6.1 As mentioned earlier in this policy, RIPA applications can only be made for directed surveillance where:

- it is for the purpose of preventing or detecting crime; and
- that crime is punishable by at least 6 months imprisonment or relates to the sale of tobacco, nicotine inhaling products or alcohol to underage children.

- In all other cases, an authorisation for directed surveillance under RIPA cannot be obtained.

6.2 This section sets out the procedure to be followed where the staff propose to undertake surveillance to investigate a criminal offence which cannot be authorised under RIPA.

It does not cover surveillance carried out for other purposes, such as part of an investigation into an employment issue. In such cases, advice should be sought from HR or Legal Services.

6.3 Surveillance which is authorised under section 27 of RIPA as part of an investigation, will be deemed lawful for all purposes.

Surveillance which is conducted outside of the RIPA regime is not in itself unlawful, but its admissibility can be questioned. It is, therefore, important that staff consider why the surveillance is required, whether or not the information can be obtained in some other way and how the surveillance can be conducted in order to minimise the intrusion into the privacy of those who are not the intended subjects of the surveillance activity.

It is only where the matter being investigated falls outside of RIPA that the procedure in this section of the policy can be followed. Even where this policy is followed, it is important to remember that the Council's actions could be challenged both by claiming that the evidence obtained through non-RIPA surveillance is inadmissible or that the Council has infringed a person's human rights. This could lead to action being against the Council in the civil courts or lead to a complaint being made to the Investigatory Powers Tribunal.

It is therefore very important that non-RIPA surveillance is only considered in appropriate cases and this policy is followed.
6.4 As local authorities can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment or are related to the underage sale of alcohol, tobacco or nicotine inhaling products this means that any offence which does not fit into this cannot be authorised under RIPA.

As a result, most breaches of planning notices cannot be investigated using RIPA-authorised surveillance, nor can anti-social behaviour, dog fouling or littering.

6.5 The procedure for obtaining authorisation for non-RIPA directed surveillance is the same as applying for authorisation under RIPA, except there is no requirement to obtain judicial approval and staff should follow the policy set out above in this policy for full

details of how to apply for authorisation. The applicant must make it clear on the form that the application is for ‘NON-RIPA DIRECTED SURVEILLANCE’.

To ensure there is an alignment of processes, all material that is obtained under a non-RIPA authorisation will be managed in exactly the same way as material that has been obtained under a RIPA authorisation.

7. Complaints

7.1 Procedure

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

Contravention of the RIPA Act may be reported to the Investigatory Powers Tribunal (IPT). The IPT is an independent tribunal. It decides complaints under the Regulation of Investigatory Powers Act 2000 (RIPA) and claims under the Human Rights Act 1998 (HRA). It considers allegations of unlawful intrusion by public bodies, including the Security and Intelligence Agencies (SIAs), the Police and local authorities.

www.ipt-uk.com

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

APPENDIX 1
BEFORE COMPLETING THESE FORMS YOU MUST TALK TO THE COUNCIL'S RIPA GATE-KEEPER

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

APPLICATION FOR AUTHORISATION TO CARRY OUT DIRECTED SURVEILLANCE

Public Authority *(including full address)*			
Name of Applicant		Department	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person other than the applicant)			
DETAILS OF APPLICATION			
1. Give position of Authorising Officer			

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).*** **(Code paragraphs 3.3 and 5.8)**
8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. (Bear in mind Code paragraphs 3.8 to 3.11) **Describe precautions you will take to minimise collateral intrusion.**

9. Explain <u>why</u> this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means? (Code paragraph 3.4 to 3.7)
10. **Confidential information. (Code paragraphs 4.1 to 4.31)** **Indicate the likelihood of acquiring any confidential information:**
11. Applicant's Details.

Name		**Tel No**	
Position		**Date**	
Signature			

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

14. (Confidential Information Authorisation) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31.			
Date of first review			
Programme for subsequent reviews of this authorisation: (Code paragraph 3.23 and 3.24). Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.			
Name		**Position**	
Signature		**Date and time**	
Expiry date and time (eg authorisation granted on 1 April 2022 – expires on 30 June 2022, 23:59)			

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

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

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

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

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

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

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

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

7. Applicant's Details			
Name		**Tel No**	
Position		**Date**	
Signature			

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

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 ..... Position Signature Date
Renewal From: Time: Date:

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

APPENDIX 3
PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000

CANCELLATION OF A DIRECTED SURVEILLANCE AUTHORISATION

Public Authority *(including full address)*			
Name of Applicant		**Department**	
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) ..... Position .....   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		**Department**	
Full Address			
Contact Details			
Operation Name			
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		**Tel No**	
Position		**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	Position
Signature	Date

10. Date of next review.	

Appendix 5 – List of Senior Authorising Officers Authorising Officers, Senior Responsible Officer and RIPA Monitoring Officer

Post Title	Current Post Holder	RIPA post	Contact Details
Head of Paid Service	Colin Carmichael	Senior Authorising Officer / Senior Responsible Officer	Tel - 01843 577008 Call phone (01843 577008) Cecil Street Margate, CT9 1XZ
Director of Corporate Services & S151 officer	Chris Blundell	Authorising Officer/ Senior Authorising Officer in the absence of the Head of Paid Service	Tel - 01843 577722 Call phone (01843 577722) Cecil Street Margate, CT9 1XZ
Head of Legal Services & Monitoring Officer	Ingrid Brown	RIPA Monitoring Officer	Tel – 01843 577455 Cecil Street Margate, CT9 1XZ
Head of Neighbourhoods	Penny Button	Authorising Officer	Tel - 01843 577 425 Cecil Street Margate, CT9 1XZ
Enforcement & Multi Agency Task Force Manager)	Eden Geddes (Enforcement & Multi Agency Task Force Manager)	Authorising Officer	Tel - 01843 577608 Cecil Street Margate, CT9 1XZ

Appendix 6 - RIPA MANAGEMENT STRUCTURE

Directed Surveillance

Court

Authorising Officers

Colin Carmichael
Head of Paid Service

Chris Blundell
Director of Corporate Services

Penny Button
Head of Neighbourhoods
Eden Geddes
Enforcement & Multi Agency Task Force Manager)

Applying Officer

Ingrid Brown - Head of Legal & Monitoring Officer
RIPA Monitoring Officer

CHIS

Court

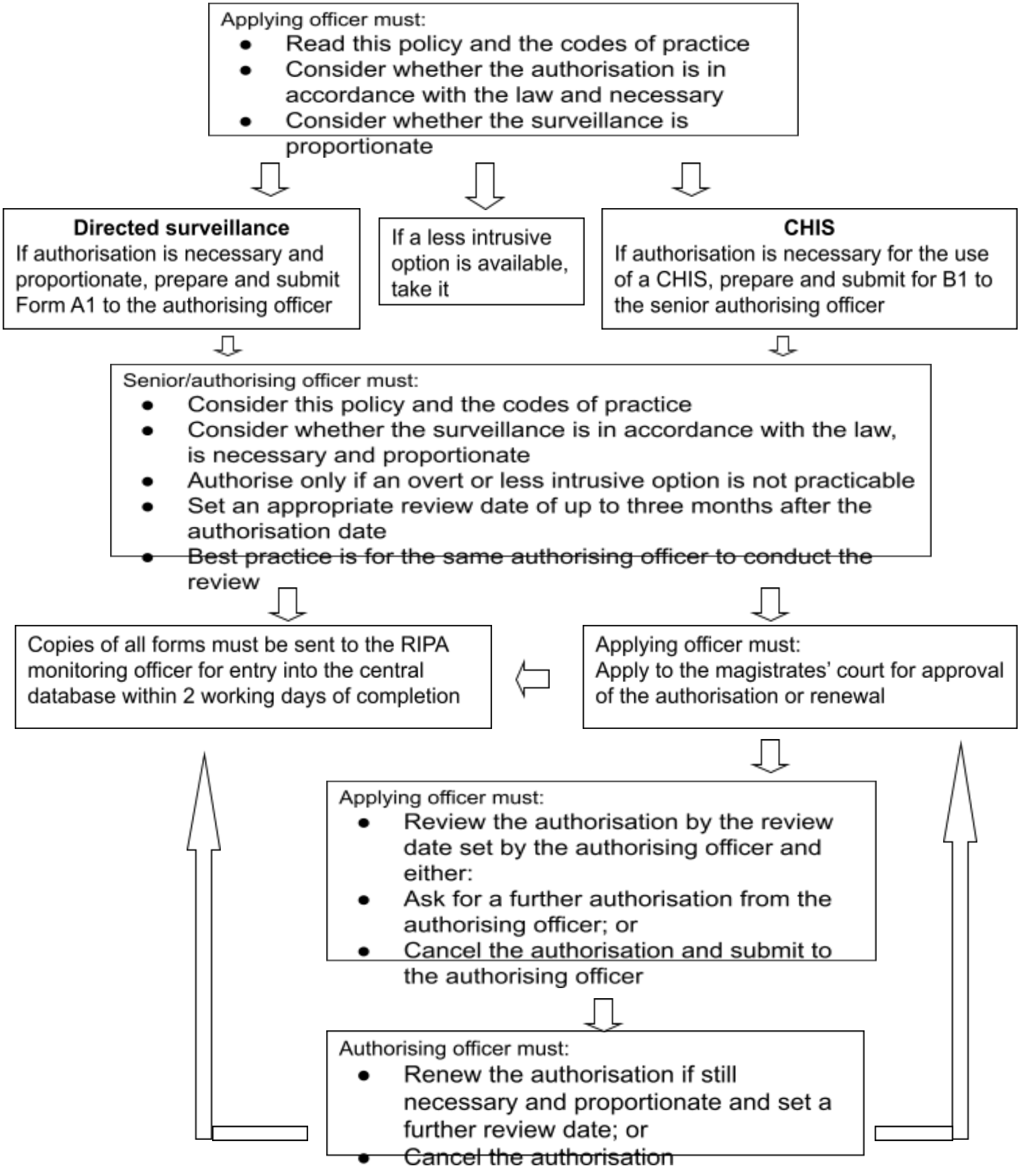
Colin Carmichael
Head of Paid Service

Or

Chris Blundell
Director of Corporate Services

Applying Officer

Appendix 7 – Flow Chart for Directed Surveillance and CHIS



Applying officer – the person who makes a request to use RIPA powers;
Authorising officer – the person who considers whether or not to grant an authorisation;
Senior authorising officer – the senior person who considers whether or not to grant an authorisation for the use of a CHIS

Appendix 8 – Additional Notes for the Use and Management of a CHIS

Tasking

1 "Tasking" is the assignment given to the CHIS by the persons defined in sections 29(5) (a) and (b) of RIPA, asking him/her to obtain information, provide access to information or to otherwise act incidentally, for the benefit of the relevant public authority.

2 Authorisation for the use or conduct of a CHIS must be obtained prior to any tasking where such tasking requires the CHIS to establish or maintain a personal or other relationship for a covert purpose.

3 The person referred to in section 29(5) (a) of RIPA will have day to day responsibility for:

- Dealing with the CHIS on behalf of the Council
- Directing the day to day activities of the CHIS
- Recording the information supplied by the CHIS, and
- Monitoring the CHIS's security and welfare

4 The person referred to in section 29(5) (b) of the 2000 Act will be responsible for the general oversight of the use of the CHIS.

5 The authorisation should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. The authorisation could cover the broad terms of the CHIS's task.

6 The persons mentioned in paragraphs 3 and 4 above must take great care to ensure that actions are recorded in writing and must also keep the authorisation under review to ensure that it covers what the CHIS is actually doing. During the course of a task, unforeseen events may occur which mean that the authorisation may need to be cancelled and applied for again.

7 The Corporate Director – Strategy as Head of Paid Service of the Council has the power to appoint officers to act under s29(5)(a) and (b) of RIPA.

8 In relation to health and safety, before tasking a CHIS, the relevant Officers will ensure that a risk assessment is carried out which determines the risk to the CHIS and to others in carrying out the task. The ongoing security and welfare of the CHIS after the task has been completed should also be considered.

9 Further advice on good practice is contained within the CHIS Code of Practice.

Appendix 9
CHIS Awareness Diagram