

SOUTH LAKELAND DISTRICT COUNCIL

**GUIDANCE ON SURVEILLANCE
UNDER THE REGULATION OF INVESTIGATORY
POWERS ACT 2000**

January 2022

CONTENTS
1. Introduction
2. Directed Surveillance
3. Covert use of Human Intelligence Source (CHIS)
4. Authorisation, Renewals, Duration and Cancellation
5. CCTV
6. Central Register of Authorisations
7. Codes of Practice
8. Benefits of Obtaining Authorisation under the 2000 Act
9. Scrutiny and Tribunal
Appendix 1- Procedure for Applying for Authorisations
Appendix 2 - Standard Forms and associated Index

1. INTRODUCTION

- 1.1 The Regulation of Investigatory Power Act 2000 (the 2000 Act) regulates covert investigations by a number of bodies, including local authorities. It was introduced to ensure that individuals' rights are protected while also ensuring that law enforcement and security agencies have the powers they need to do their jobs effectively.
- 1.2 South Lakeland District Council ("the Council") is therefore included within the 2000 Act framework with regard to the authorisation of both Directed Surveillance and of the use of Covert Human Intelligence Sources.
- 1.3 The purpose of this guidance is to explain the scope of the 2000 Act and the circumstances where it applies and provide guidance on the authorisation procedures to be followed.
- 1.4 The Council has had regard to the Codes of Practice produced by the Home Office in preparing this guidance and Legal, Governance and Democracy Services have copies to which staff can refer. The relevant codes of practice and associated guidance that relate to authorised Council activity are:
 - (a) Home Office Code of Practice - Covert Surveillance;
 - (b) Home Office Code of Practice - Covert Human Intelligence Sources
 - (c) Guidance from the Office of Surveillance Commissioners
 - (d) Protection of Freedoms Act 2012- changes to provisions under the Regulation of Investigatory Power Act 2000 Home Office Guidance for Magistrates' Courts in England and Wales for a local authority application seeking an order approving the grant or renewal of a RIPA authorisation or notice
- 1.5 In summary the 2000 Act requires that when the Council undertakes directed surveillance or uses "covert human intelligence source" these activities must only be authorised by an officer with delegated powers when the relevant criteria are satisfied. The 2000 Act states that if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it should be "lawful for all purposes". The Council has nominated officers who can grant authorisations. They are as follows:

The Chief Executive, the Director of Strategy, Innovation and Resources, the Director of Customer and Commercial Services, and all Deputy Chief Officers of the Council.
- 1.6 Chapter 2 of Part 2 of the Protection of Freedoms Act 2012 ("the 2012 Act") amends the 2000 Act so as to require the Council to obtain judicial approval for the use of covert investigatory techniques available to them under the 2000 Act. Prior to the 2012 Act authorisations for the use of these techniques were granted internally by an Authorised Officer and were not subject to any independent approval mechanism.
- 1.7 Part 2 of the 2012 Act specifies the grounds for which authorisations can be granted for carrying out both Directed Surveillance and of the use of Covert Human Intelligence Sources. Furthermore the 2012 Act provides that use of the 2000 Act to authorise directed surveillance will have to be confined to cases where the offence under investigation carries a maximum custodial sentence of 6 months or more, save in cases in relation to the sale of alcohol and tobacco to minors where the new threshold would not apply.
- 1.8 The Council will have to apply to the magistrates' court for an order approving the use of the authorisation.
- 1.9 Subject to the need for approval from the Magistrates Court as referred to above, authorisation under the 2000 Act gives lawful authority to carry out surveillance and the use of a source. Obtaining authorisation helps to protect the council and its officers from

complaints of interference with the rights protected by Article 8(1) of the European Convention of Human Rights, which is now enshrined in English law through the Human Rights Act 1998. This is because the interference with the private life of citizens will be “in accordance with the law”, provided activities undertaken are also “reasonable and proportionate” they will not be in contravention of Human Rights legislation.

1.10 There are two types of surveillance:

Directed Surveillance - This is surveillance undertaken for the purpose of a specific operation and in a manner which is likely to result in the obtaining of private information about a person (whether or not that person is the target of the investigation or operation); and is carried out in a planned manner and not by way of an immediate response; and

Intrusive Surveillance - This is surveillance that takes place on residential premises or any private vehicle and involves the presence of an individual on the premises or in the car, or by the use of a surveillance device that although not in the car/ premises, provides data as though it was.

1.11 In no circumstances does the 2000 Act authorise the carrying out of any form of intrusive surveillance by local authorities. It should be noted that the Council cannot authorise “Intrusive Surveillance”.

1.12 Deciding when an authorisation is required involves making a judgment. For example, Environmental Health Specialists might covertly observe and then visit a shop as part of their enforcement functions. Such observations may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras. Where this does not involve systematic surveillance of an individual, it forms a part of the everyday functions of law enforcement authorities or other public bodies. This low-level activity will not usually be regulated under the provisions of the 2000 Act.

1.13 Conversely where systematic covert surveillance is undertaken then an authorisation will be required. Neither the provisions of the 2000 Act or of the Codes of Practice cover the use of overt CCTV surveillance systems. Members of the public are aware that such systems are in use around the town centre and car parks in order to prevent crime. However use of CCTV cameras to target a person, their property or a building would require an Authorisation and this is dealt with in Section 5 of the document. If you are in doubt, seek the advice of an Authorising Officer, if they are in doubt they will seek advice from Legal, Governance and Democracy Services.

2. DIRECTED SURVEILLANCE

2.1 Surveillance is ‘Directed’ for the purposes of the 2000 Act if it is covert, but not intrusive and is undertaken:

- (a) for the purposes of a specific investigation or a specific operation;
- (b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one is specifically identified for the purposes of the investigation or operation); and
- (c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

2.2 Before any officer of the Council undertakes any surveillance of any individual or individuals they need to assess whether the activity comes within the 2000 Act. In order to do this the following key questions need to be asked:

- (a) Is the surveillance covert? Covert surveillance is that carried out in a manner calculated to ensure that subjects of it are unaware it is or may be taking place. If activities are open and not hidden from the subjects of an investigation, the 2000 Act framework does not apply;
- (b) Is it for the purposes of a specific investigation or a specific operation e.g. are town centre and car park CCTV cameras which are readily visible to anyone walking around the area covered? The answer is not if their usage is to monitor the general activities of what is happening in the vicinity. If that usage, however, changes, the 2000 Act may apply. If the CCTV cameras are targeting a particular known individual, and are being used in monitoring their activities, that has turned into a specific operation which will require authorisation.
- (c) Is it in such a manner that is likely to result in the obtaining of private information about a person e.g. if part of an investigation is to observe a person's home to determine their comings and goings then that would be covered. If it is likely that observations will not result in the obtaining of private information about a person, then it is outside the 2000 Act framework. However, the use of 'test purchasers' may involve the use of covert human intelligence sources. If in doubt, it is safer to get authorisation;
- (d) Is it by way of an immediate response to events or circumstances? The Home Office gives the example of anything happening as an immediate response to something occurring during the course of an observer's work which is unforeseeable. If so it is likely that an authorisation is not required. However, if as a result of an immediate response, a specific investigation subsequently takes place, that brings it within the 2000 Act framework.

3. COVERT USE OF HUMAN INTELLIGENCE SOURCE

3.1 A person is a Covert Human Intelligence Source ("a CHIS") if they establish or maintain a personal or other relationship with a person for the covert purpose of using such a relationship either to obtain information or provide access to information about another person. A relationship is covert, if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of that purpose.

3.2 The above clearly covers the use of professional witnesses to obtain information and evidence. It can also cover "entrapment" cases.

3.3 Special safeguards apply to the granting of authorisations where the CHIS would be a juvenile (under 18 years of age). Authorisations cannot be granted unless the provisions within The Regulation of Investigatory Powers (Juveniles) Order 2000 are satisfied. Only the Chief Executive (or in their absence, the Director of Strategy, Innovation and Resources or the Director of Customer and Commercial Services) can authorise the use of a juvenile CHIS. If any Council officer intends to use juvenile CHIS, advice and guidance should be sought from Legal, Governance and Democracy Specialists before any steps are taken.

4. AUTHORISATIONS, RENEWALS, DURATION AND CANCELLATION

4.1 For directed surveillance no officer shall grant an authorisation for the carrying out of

directed surveillance unless they believe that an authorisation is necessary and proportionate to what is sought to be achieved by carrying it out.

- 4.2 The 2012 Act provides that an authorisation is necessary only if it is for the purpose of preventing or detecting crime. The onus is therefore on the person authorising such surveillance to satisfy themselves it fulfils this criteria.
- 4.3 In order to ensure that authorising officers have sufficient information in order to make an informed decision and so that a sound case is presented when seeking the approval of the Magistrates Court, it is important that detailed records are maintained. As such the standard forms in the Appendix 2 are to be completed where relevant. It is also sensible to make any authorisation sufficiently wide enough to cover all the means required as well as being able to prove effective monitoring of what is done against that is authorised.
- 4.4 For urgent grants or renewal, oral authorisations are acceptable. In all other cases, authorisations must be in writing using the appropriate standard form RIPA 1 (Directed Surveillance) or RIPA 5 (CHIS). Appendix 2 to this guidance contains copies of all the standard forms which are to be used by all Council Operational Areas.
- 4.5 Although it is possible to combine two authorisations in one, the Council's practice is for separate forms to be completed to maintain the distinction between Directed Surveillance and the use of a CHIS.
- 4.6 Authorisations lapse, if not renewed
- (a) within 72 hours if either granted or renewed orally, (or by a person whose authorisation was confirmed to urgent cases) beginning with the time of the last grant or renewal; or
 - (b) 12 months, if in writing/ non-urgent , from date of last renewal if it is for the conduct of use of a covert human intelligence source; or
 - (c) in the case of Directed Surveillance 3 months from the date of their grant or latest renewal.
- 4.7 Furthermore, as is the case with an Authorisation, renewal needs the approval of the Magistrates Court.
- 4.8 Forms RIPA 2 (Directed Surveillance) and RIPA 7 (CHIS) must be used for all renewals. The following should also be noted:-
- (a) All authorisations must be reviewed every 4 weeks and Forms RIPA 3 (Directed Surveillance) or RIPA 7 (CHIS) completed;
 - (b) When an authorisation is cancelled a Form RIPA 4 (Directed Surveillance) or RIPA 8 (CHIS) must be completed.
- 4.9 An authorisation can be renewed using the Renewal Form RIPA 2 (directed surveillance) or RIPA 6 (CHIS) at any time before it ceases to have effect by any person entitled to grant a new authorisation in the same terms. In the case of a CHIS, a person should not renew (using form RIPA 6) unless a review has been carried out (using form RIPA 7) and that person has considered the results of the review when deciding to renew or not. A review must cover what use has been made of the CHIS, the tasks given to them and information obtained.
- 4.10 Authorising Officers are responsible for ensuring that authorisations undergo timely reviews for which a RIPA 3 (Directed Surveillance) or RIPA 7 (CHIS) form must be completed. Also that they are cancelled promptly if the Directed Surveillance activity (using form RIPA 4) or use of a CHIS (using form RIPA 8) is no longer necessary.
- 4.11 Cancellation of the authorisation and completion of Form RIPA 4 (Directed Surveillance) or RIPA 8 (CHIS) must be carried out in all cases as soon as the actual surveillance activity for which authorisation was specifically granted ceases. Authorisations must not be allowed to

continue in force until they reach the stated expiry date without cancellation if the surveillance activity or use of a source is no longer in operation. However should this occur formal cancellation must be carried out and evidenced by the completion of Form RIPA 4 (Directed Surveillance) or RIPA 8 (CHIS) as soon as this is detected even though this will result in a cancellation date after the expiry date.

- 4.12 Cancellation should wherever possible be carried out by the same person that granted the original request or renewal. If that person is no longer available to do this then it should be completed by the person appointed to replace them or by one of the other authorised officers.
- 4.13 A copy of the Form RIPA 4 (Directed Surveillance) or RIPA 8 (CHIS) completed to evidence the cancellation must be sent to the Legal, Governance and Democracy Services to be recorded on the central register and the original held securely within the originating unit.
- 4.14 Any person giving an authorisation should give particular consideration to collateral intrusion i.e. 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.
- 4.15 An application for an authorisation should include an assessment of the risk of any collateral intrusion or interference. This will be taken into account by the authorising officer, particularly when considering the proportionality of the surveillance.
- 4.16 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.
- 4.17 Any person giving an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place or of similar activities being undertaken by other public authorities which could impact on the development of the surveillance.
- 4.18 No operations will be undertaken in circumstances where investigators believe that surveillance will lead to them to intrude on spiritual counselling between a Minister and a faith member. In this respect, spiritual counselling is defined as conversations with a Minister of Religion acting in their official capacity where the person being counselled is seeking or the Minister is imparting forgiveness, or absolution of conscience.
- 4.19 The 2000 Act refers to 'confidential material' namely:
 - (a) matters subject to legal privilege;
 - (b) confidential personal information; or
 - (c) confidential journalistic material.
- 4.20 The Act does not provide any special protection for 'confidential material'. Nevertheless, such material is particularly sensitive, and is subject to additional safeguards under this code. In cases where the likely consequence of the conduct of a source would be for any person to acquire knowledge of confidential material, the deployment of the source should be subject to special authorisation. In such circumstances only the Chief Executive, or in their absence the Director of Strategy, Innovation and Resources or the Director of Customer and Commercial Services can grant an authorisation.

- 4.21 In general, any application for an authorisation which is likely to result in the acquisition of confidential material should include an assessment of how likely it is that confidential material will be acquired. Special care should be taken where the target of the investigation is likely to be involved in handling confidential material. Such applications should only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises.
- 4.22 The following general principles apply to the acquisition of confidential material:
- (a) Confidential material should not be retained or copied unless it is necessary for a specified purpose;
 - (b) Confidential material should be disseminated only where an appropriate officer is satisfied that it is necessary for a specific purpose;
 - (c) The retention or dissemination of such information should be accompanied by a clear warning of its confidential nature; and appropriate safeguards as to its security must be implemented;
 - (d) Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.
- 4.23 In cases of joint working, for example, with other agencies on the same operation only one authorisation is required. Duplication of authorisations does not affect the lawfulness of the activities to be conducted, but may create an unnecessary administrative burden on the agencies.
- 4.24 Applications for Directed Surveillance or the use of a source are to be retained by the Authorised Officer, for a period of 5 years. Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period commensurate to any subsequent review.
- 4.25 Authorising Officers must ensure compliance with the appropriate data protection requirements and the relevant codes of practice in the handling and storage of material. Where material is obtained by surveillance, which is wholly unrelated to a criminal or other investigation not to any person who is the 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.
- 4.26 There is nothing in the 2000 Act that prevents material obtained through the proper use of the authorisation procedures from being used in other investigations. However, the use outside the authority that authorised surveillance, of any material obtained by means of covert surveillance and, other than in pursuance of the grounds on which it was obtained, should be authorised only in the most exceptional circumstances.
- 4.27 The Council will not use an external or professional source for the purpose of obtaining information. It is not the Council's general practice to seek, cultivate or develop a relationship with a potential external or professional source. It is possible, though highly unlikely, that the role of a Council employee may be that of a source, for example in 'entrapment cases'
- 4.28 The Authorising Officer must consider the safety and welfare of an employee acting as a source, and the foreseeable consequences to others of the tasks they are asked to carry out. A risk assessment should be carried out before authorisation is given. Consideration from the

start for the safety and welfare of the employee, even after cancellation of the authorisation, should also be considered.

- 4.29 The Council's practice is not to use an employee acting as a source to infiltrate existing criminal activity, or to be a party to the commission of criminal offences, even where this is within the limits recognised by law.
- 4.30 Further details about the Council's Procedures for seeking authorisations are set out in Appendix 1.

5. CCTV

- 5.1 Use of the Council owned or operated CCTV cameras to target a person, their property or a building would be directed surveillance. Before an officer of the Council undertakes such activity, an Authorisation is required in accordance with the procedures set out in this document. The only exception that applies is where an emergency situation applies and there are good reasons why an urgent application could not be made. The reasons for the operation and its emergency nature should be noted by the CCTV operator and a RIPA application made as soon as possible.
- 5.2 When there is use of the Council owned or operated CCTV cameras by an external organisation to target a person, their property or a building it is for that organisation to obtain their own RIPA authorisation. A copy of this Authorisation must be passed to the appropriate responsible Council officer before such activity can be carried out. If in the judgement of the CCTV operator the request is urgent they can authorise the use of the Council's CCTV cameras but only upon receiving a written assurance from an officer of the organisations that authorisation will be obtained. Details of the request should be then be recorded by the operator and a copy of the authorisation sought as soon as is reasonably practicable.

6. CENTRAL REGISTER OF AUTHORISATIONS

- 6.1 The 2000 Act requires a central register of all authorisations to be maintained. The Legal, Governance and Democracy Lead Specialist (Monitoring Officer) maintains this register.
- 6.2 Whenever an authorisation is granted the Authorising Officer must arrange for a copy of the authorisation to be forwarded to the Legal, Governance and Democracy Services. In addition copies of any other forms completed, as listed in Appendix 2, must also be so forwarded. Copies of the orders of the Magistrates Court approving or refusing the grant or renewal of an authorisation will also be placed on the Central Register of Authorisations.
- 6.3 It is the responsibility of each Operational Area to arrange for the secure retention of all authorisations that are generated by them. Authorisation should only be held for as long as it is necessary and in line with the Council's Records Retention Policy and Records Retention Schedule. Once the investigation is closed (bearing in mind cases may be lodged some time after the initial work) the records held by the Operational Area should be disposed of in line with the Council's Confidential Waste Disposal Protocol (e.g. destroyed).

7. CODES OF PRACTICE

- 7.1 There are Home Office Codes of Practice referred to in paragraph 1.4 above, that expand on this guidance. The codes do not have the force of statute, but are admissible in evidence in any criminal and civil proceedings.

8. BENEFITS OF OBTAINING AUTHORISATION UNDER THE 2000 ACT

- 8.1 The Home Office Codes of Practice say councils should appoint a Senior Responsible Officer. This person is responsible for the integrity of the surveillance process, ensuring the Council complies with RIPA and relevant legislation, and also engaging with the Inspectors when they conduct their inspections. The Council's Senior Responsible Officer is the Director of Strategy, Innovation and Resources.
- 8.2 The Codes of Practice also say elected members should review the Council's use of the 2000 Act and set the policy once a year. In addition to this, internal quarterly reports on the use of the 2000 Act should be considered to ensure that the consistency and compliance with Policy. These quarterly reports are submitted to the Cabinet Member for Customer and Locality Services. Consideration should also be given to appropriate liaison with the Local Magistrates Court with a view to reviewing consistency of approach and any training needs of the court clerks and magistrates.

9. SCRUTINY AND TRIBUNAL

- 9.1 To effectively "police" RIPA Commissioners have been appointed to regulate conduct carried out under the 2000 Act. The Chief Surveillance Commissioner will keep under review, among others, the exercise and performance by the persons on whom are conferred or imposed, the powers and duties under the Act. This includes authorising directed surveillance and the use of covert human intelligence sources.
- 9.2 A tribunal has been established to consider and determine complaints made under the 2000 Act. Complaints can be made by persons aggrieved by surveillance. The forum hears application on a judicial review basis. Claims should be brought within one year unless it is just and equitable to extend that.
- 9.3 The tribunal can order, among other things, the quashing or cancellation of any warrant or authorisation and can order destruction of any records or information obtained by using a warrant or authorisation, and records of information held by any public authority in relation to any person.

APPENDIX 1-PROCEDURE FOR APPLYING FOR AUTHORISATIONS

Applications

1. Except in urgent circumstances, applications for authorisation to carry out directed surveillance must be made in writing and should describe any conduct to be authorised and the purpose of the investigation or operation. The application should also include:-
 - The reasons why the authorisation is necessary in the particular case and on the relevant ground - this is for the purpose of preventing or detecting crime or of preventing disorder;
 - The reasons why the surveillance is considered proportionate to what it seeks to achieve;
 - The nature of the surveillance;
 - The identities where known, of those to be the subject of the surveillance;
 - An explanation of the information which it is desired to obtain as a result of the surveillance;
 - The details of any potential collateral intrusion and why the intrusion is justified;
 - The details of any confidential information that is likely to be obtained as a consequence of the surveillance;
 - The level of authority required (or recommended where that is different) for the surveillance; and
 - A subsequent record of whether authority was given or refused, by whom and the time and date

Urgent Cases

2. In urgent cases the authorisation should record (as may be):-
 - The reasons why the authorising officer or the officer entitled to act in urgent cases considered the case so urgent that an oral instead of a written authorisation was given; and/ or
 - The reasons why it was not reasonably practicable for the application to be considered by the authorising officer.
3. Where the authorisation is oral, the detail referred to above should be recorded in writing by the applicant as soon as reasonably practicable.

Renewals

4. Applications for renewal should record the above information together with details of:-
 - Whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
 - Any significant changes to the information previously provided;
 - The reason why it is necessary to continue with the directed surveillance;
 - The content and value to the investigation or operation of the information so far obtained by the surveillance;

- The result of regular reviews of the investigation or operation.

Covert Human Intelligence Source Records

5. The following information is included in records relating to each covert human intelligence source: -

- (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 all persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) or in any order made by the Secretary of State;
- (i) the periods during which those persons have discharged those responsibilities;
- (j) the tasks given to the source and the demands made of them in relation to their activities as a source;
- (k) all contacts or communication between the source and a person acting on behalf of any relevant investigating authority;
- (l) the information obtained by each relevant investigatory 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.

Covert Human Intelligence Source Applications

6. Applications for authorisation for the use or conduct of a source should be in writing and record the information laid down within the relevant code of practice. Applications for renewal of covert human intelligence sources 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 previously provided;
- the reasons why it is necessary to continue the use of the source;
- the use made of the source in the period since the grant, or, as the case may be, latest renewal of the authorisation;
- the tasks given to the source during that period and the information obtained from the conduct or use of the source;
- the result of regular reviews of the use of the source

Duration and Cancellation of Authorisations

7. For Direct surveillance the written authorisation will cease to have effect (unless renewed) at the end of a period of three months beginning with the day on which it took effect. Urgent Oral authorisations will, unless renewed cease to have effect after 72 hours beginning with the time when the grant or renewal was approved by the Magistrates Court.
8. In a case in which the authorisation is for the conduct of a covert human intelligence source, the authorisation shall cease to have effect after the period of 12 months beginning with the day on which the grant takes effect.
9. A person shall not renew an authorisation for a covert human intelligence source unless a review has been carried out as to the use made of the source, and tasks given during that period, and considered the same.
10. Authorisations should be cancelled if the criteria for the authorisation is no longer met. A separate authorisation is required for each investigation.
11. Reviews should be undertaken following any significant occurrence and the results of a review should be recorded on the central register of authorisations.

Magistrates Court

12. No authorisation or renewal relating to Directed Surveillance or CHIS can be acted upon unless approval is given by the Magistrates Court. An application for such approval will be made by a representative of Legal, Governance and Democracy Service accompanied by the Authorising Officer and the applicant.

APPENDIX 2

Standard forms to be used in connection with applications to authorise surveillance under the Regulation of Investigatory Powers Act 2000

The standard forms are also published on the Intranet.

- | | |
|---------------|---|
| 1 Form RIPA 1 | Authorisation Directed Surveillance |
| 2 Form RIPA 2 | Renewal of a Directed Surveillance authorisation |
| 3 Form RIPA 3 | Review of a Directed Surveillance authorisation |
| 5 Form RIPA 4 | Cancellation of a Directed Surveillance authorisation |
| 6 Form RIPA 5 | Application for authorisation of the conduct or use of a Covert Human Intelligence Source (CHIS) |
| 7 Form RIPA 6 | Application for renewal of a Covert Human Intelligence Source (CHIS) Authorisation |
| 8 Form RIPA 7 | Review of a Covert Human Intelligence Source (CHIS) Authorisation |
| 9 Form RIPA 8 | Cancellation of authorisation for the use or conduct of a Covert Human Intelligence Source (CHIS) |