POLICY AND GUIDANCE ON THE

REGULATION OF INVESTIGATORY POWERS ACT

2000

Introduction

1. The Regulation of Investigatory Powers Act 2000 ("RIPA") (as amended by the Protection of Freedoms Act 2012) regulates surveillance carried out by the Council in the conduct of its business. It relates to directed surveillance, the use of covert human intelligence sources ("CHIS") and the accessing of certain communications data through a single point of contact (SPOC). It provides a legal framework for authorising investigations in a manner consistent with obligations under the Human Rights Act 2000 ("HRA") where the investigation is for the purposes of preventing or detecting crime or for preventing disorder.

2. RIPA is wide ranging in its application and will impact all officers with an enforcement or investigatory capacity, including internal investigations. Failure to comply with RIPA may result in a claim for a breach of the HRA. This may result in evidence being deemed inadmissible in a prosecution or even a claim for compensation for an infringement of that person's human rights.

3. The Council is committed to implementing RIPA in a manner that is consistent with the spirit and letter of RIPA and the HRA. The Council is committed to conducting all relevant actions in a manner which strikes a balance between the rights of the individual and the legitimate interests of the public.

4. The Council's Service Manager - Corporate and Human Resources will act as the Senior Responsible Officer under the Act and shall maintain a central record of all applications for authorisation.

5. Following the Protections of Freedoms Act 2012, any authorisation or notice by the Council under RIPA for the use of particular covert techniques can only be given effect once an order approving the authorisation or notice has been granted by a Magistrates' Court. This judicial approval is in addition to the Council's current authorisation process.

6. Furthermore, the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligences Sources) Order 2010 has been amended to include a new article 7A which introduces a crime threshold that must now be applied to the authorisation of directed surveillance under RIPA. The Council will only be able to use directed surveillance to prevent or detect criminal offences that are punishable by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco.

Codes of Practice

7. Statutory Codes of Practice supplement RIPA. These deal respectively with covert surveillance, CHIS, interception of communications, communications data and electronic information. They are available on the following web link:

   http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-codes-of-practice/

8. The Council's policy recognises the important role these Codes of Practice play in the practical implementation of RIPA. The Council will have due regard to and follow the guidance in the relevant Codes of Practice in the conduct of its activities relating to RIPA. It is essential, therefore, that all relevant officers involved in RIPA are familiar with the content of these Codes of Practice. In particular due regard will need to be had to the revised code of practice on Covert Surveillance and Property Interference that came into force in April 2010.

9. Any Officer who is uncertain or unsure about any aspect of this Policy, the Act or the Codes of Practice should contact the Council's RIPA Co-Ordinator for advice and assistance.

Surveillance

10. Most of the surveillance carried out by the Council is not directed surveillance and will be done overtly. Overt surveillance is not subject to the authorisation requirements under RIPA. In many cases, officers will be behaving in the same way as a normal member of the public or will be going about council business openly. Similarly, surveillance will be overt if the subject has been told that it will happen.

Examples of overt surveillance and not directed surveillance:

a. Activity that is observed as part of normal duties.
b. CCTV cameras – unless they have been directed as the request of investigators, these are overt or incidental surveillance.
c. Targeting a 'Hot Spot' e.g. licensing officers standing on a street to monitor private hire cars plying for hire illegally where this is not part of a planned operation, or standing on a street that has a high incidence of dog fouling.
d. Test purchases for sale of alcohol to under 18s.

11. Covert surveillance is defined in section 26(9)(a) of RIPA as any surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. It may be either direct or intrusive surveillance.

12. Directed surveillance is defined in section 26(2) of RIPA as surveillance which is covert, but not intrusive, and undertaken:

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

13. Use of directed surveillance under RIPA can only be authorised to prevent or detect criminal offences that are either punishable by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco.

14. Authorisation for use of directed surveillance in more serious cases, as long as the other tests are met, can continue. But 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.

15. The Code of Practice for Covert Surveillance and Property Interference provides detailed guidance on whether covert surveillance activity is directed surveillance or intrusive, or whether an authorisation for either activity would not be deemed necessary. That detailed guidance is not repeated here and officers are therefore directed to the Code of Practice for that information.

Examples of directed surveillance

Officers wish to drive past a café for the purposes of obtaining a photograph of the exterior. Reconnaissance of this nature is not likely to require a directed surveillance authorisation as no private information about any person is likely to be obtained or recorded. If the officers chanced to see illegal activities taking place, these could be recorded and acted upon as an 'immediate response to events'.

If, however, the officers intended to carry out the exercise at a specific time of day, when they expected to see unlawful activity, this would not be reconnaissance but directed surveillance, and an authorisation should be considered.

Similarly, if the officers wished to conduct a similar exercise several times, for example to establish a pattern of occupancy of the premises by any person, the accumulation of information is likely to result in the obtaining of private information about that person or persons and a directed surveillance authorisation should be considered.

16. Intrusive surveillance is defined in section 26(3) of RIPA as covert surveillance that:

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

17. Local Authorities are **NOT** authorised to conduct intrusive surveillance.

18. A device used to enhance your external view of a property is almost never intrusive surveillance. A device would only become intrusive where it provided a high quality of information from inside the private residential premises.

Examples are:

A. Officers intend to use an empty office to carry out surveillance on a person who lives opposite. As the office is on the 4th floor, they wish to use a long lens and binoculars so that they can correctly identify and then photograph their intended subject covertly. This is NOT intrusive surveillance as the devices do not provide high quality evidence from inside the subject's premises.

B. Officers intend using a surveillance van parked across the street from the subject's house. They could see and identify the subject without binoculars but have realised that, if they use a 500mm lens, as the subject has no net curtains or blinds, they should be able to see the document he is reading. This IS intrusive surveillance as the evidence gathered is of a high quality, from inside the premises and is as good as could be provided by an officer or a device being on the premises.

19. A CHIS is defined in section 26(8) of RIPA as a person who:

    a. establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling with paragraph (b) or (c);
    b. he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
    c. he covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

20. There is a separate revised code of practice for the use of human intelligence sources that came into effect in April 2010. Again officers are directed to that code of practice for detailed guidance and examples.

Examples of a CHIS may include:

a. Licensing officers, working with the police, covertly building a business relationship with a cab company which is believed to be using unlicensed drivers.
b. Whistleblowing, when you actively recruit an employee to gather information on another employee who is the subject of a criminal investigation.
c. Planning officers posing as customers to get information about the commercial activities at premises and developing a relationship with the workers beyond that of supplier and customer.

Communications Data

21. In addition to carrying out covert surveillance and the use of a CHIS, the Council may also access certain communications data under RIPA, provided this, like all other surveillance, is **for the purpose of preventing or detecting crime or of preventing disorder**.

22. Authorisations may be granted by a Designated Person, who shall seek the advice of the Council's SPOC (Single Point of Contact) authorised by the Home Office. The codes of practice shall be followed at all times. Council staff are **not** permitted to obtain telecommunications and internet use data other than as provided for by the Act.

23. Communications data is defined by section 21(4) of the Act and is divided into three categories. The first relates to 'traffic data', the second is 'service use information' and the third is 'subscriber information'. However, the Council may only acquire communications data falling within the second and third category and must not under any circumstances obtain traffic data. In essence the Council may acquire certain information held by communication service providers relating to their customers but NOT data that includes the content or attachment of any communication.

24. The Act provides two different ways of authorising access to communications data: through an authorisation under section 22(3) and by a notice under section 22(4). An authorisation would allow the Council to collect or retrieve the data itself. A notice is given to a postal or telecommunications operator which requires the operator to collect or retrieve the data and provide it to the Council. A designated person decides whether or not an authorisation should be granted or a notice given, and must believe that obtaining the data in question by the conduct authorised or required by the authorisation or notice is proportionate to what is sought to be achieved by so obtaining the data

25. Before any authorisation or notice is to take effect, an application MUST be made to the Magistrates' Court for an order approving the grant or renewal of the authorisation or notice.

Social Media

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

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

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

29. Officers should not use false personae (e.g. a false Facebook profile or Twitter handle) to disguise their online activities. False personae should not be used for a covert purpose without authorisation. Legal advice should always be sought for anything other than "open source" material.

Authorising Officer

30. Before application to the Magistrates' Court, all requests for authorisation of directed surveillance or a CHIS under RIPA must first be approved in advance by an Authorising Officer. An Authorising Officer is a person who has been delegated power to act in that capacity by the Council with regulatory responsibilities. A list of officers who have, to date, been authorised, is annexed to this policy and is subject to regular review and updating by the Senior Responsible Officer.

31. In order to be approved as an Authorising Officer, that person must have attended a relevant training course on the practical application of RIPA.

RIPA Co-Ordinator

32. The Council operates a gate keeper system for all authorisations. Prior to submitting an application for directed surveillance or a CHIS to an Authorising Officer, you MUST first submit your forms to the RIPA Co-Ordinator who will guide you through the procedure. Details of who is authorised to act as the RIPA Co-ordinator is set out in the Appendix to this policy.

33. The RIPA Co-Ordinator will act as a form of quality control and will advise you on any aspect of your proposed surveillance operation, including the way in which you must complete your application for directed surveillance or CHIS.

Authorisation Process – Stage 1: The Authorisation

34. All requests to conduct, renew, review or cancel a covert surveillance exercise, or use of a CHIS, must be made in advance in writing on the appropriate forms. Following advice from the RIPA Co-ordinator, all such requests must be submitted to an Authorising Officer of the Council. To ensure the latest forms are used, please download the relevant version from the Home Office website, via the following link: http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/

35. The power to grant, renew, review and cancel will be limited to Authorising Officers in order to ensure greater independence and consistency. Written authorisation for a directed covert surveillance operation will be valid for a maximum of three months and for a CHIS a maximum of 12 months, both from the date of the original authorisation or renewal.

36. Prior to submitting the forms, you are required to obtain a unique reference number for your application. This is generated through the central record of authorisations. Please contact the RIPA Co-ordinator to obtain the next unique number.

37. When completing the forms, a full and detailed description of the operation should be provided. This should specify any equipment to be used as well as maps or sketches to show observation points and target premises. Officers need to take particular care to ensure there are no ambiguities in the description of the operation.

38. RIPA first requires that the person granting an authorisation believe that the authorisation is necessary in the circumstances of the particular case for the statutory basis grounds for directed surveillance or a CHIS; namely that the proposed activity is necessary for the prevention and detection of crime or prevention of disorder whilst ensuring that it fulfils the crime threshold for directed surveillance. This

is the **ONLY** ground that a local authority can apply for and be granted authorisation under the Act.

39. The application should identify

    a. the specific offence being investigated
    b. the specific point to prove that the surveillance is intended to gather evidence about
    c. that the operation is capable of gathering that evidence; and
    d. that such evidence is likely to prove that part of the offence.

40. Then, if the directed surveillance or use of the CHIS is necessary, the person granting the authorisation must believe that the directed surveillance or use of a CHIS is proportionate to what is sought to be achieved by the conduct and / or use of that CHIS. This involves balancing the intrusiveness of the surveillance or use of the CHIS on the target and others who might be affected by it, against the need for the surveillance or CHIS to be used in operational terms. The use of surveillance or a CHIS 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. The use of surveillance or a CHIS should be carefully managed to meet the objective in question and sources must not be used in an arbitrary or unfair way.

41. Proportionality must be carefully explained, not merely assented. Similarly, merely describing parts of the operation itself is not germane to proportionality. A good explanation of proportionality should refer to three elements:

    (a) balance the extent of the problem against the size and scope of the operation, demonstrating that it is not a 'sledgehammer to crack a nut',
    (b) explain that intrusion is to be kept to a minimum
    (c) show that having considered all other practical courses there is no other way in which the necessary evidence can be obtained i.e. a cover operation is the last resort.

42. The Authorising Officer must state their reasons for believing that the authorisation, renewal or cancellation is necessary. If they do not consider authorisation, renewal or cancellation to be appropriate they must also state their reasons for this on the relevant form.

43. The Authorising Officer's statement should not be a mere rubber stamp. It should include a full account, in his own words, of what is being authorised (the five W's test of Who, What, Why, Where & When) and how and why the Authorising Officer is satisfied that the operation is necessary and proportionate. A bare assertion is insufficient.

44. The application MUST make it clear how the proposed intrusion is necessary and how an absence of this evidence would have a prejudicial effect on the outcome of the investigation.

45. The Authorising Officer should not be put off by repetition as if challenged in court, the Authorising Officer may be required to demonstrate his own thought process at the time and will be in a weak position if he has to rely upon the applicant's account by adoption.

Authorisation Process – Stage 2: Judicial Approval

Application:

46. Following authorisation or renewal of an authorisation by the authorising officer under Stage 1 above, a hearing with a Justice of the Peace (JP) should be arranged as soon as possible at the Magistrates' Court.

47. An application to the JP must include the following:
    a. a copy of the original RIPA authorisation or notice (the original RIPA authorisation should be shown to the JP at the hearing but must be retained by the Council for its records and any inspections by the Commissioners' offices);
    b. the supporting documents setting out the case and all documents relied upon;
    c. a partially completed judicial application/order form (see the form at appendix 3).
    d. The JP may have regard to additional information that is submitted during the hearing, but information fundamental to the case must be submitted in advance with the application.

48. The application/order form does require a brief summary of the circumstances of the case but this is supplementary to providing the copy of the original RIPA authorisation as well. The JP will complete the order section of the form and this will be the official record of the JP's decision. A copy of the form after it has been signed by the JP must be retained.

Hearing and Officer Attendance:

49. The hearing will be in private and heard by a single JP. The JP may have questions to clarify points or require additional reassurance on particular matters. It is therefore important that an appropriate officer should attend this hearing to provide oral evidence when required. This officer should be best able to answer the JP's questions on the policy and practice of conducting covert operations and detail of the case itself. Home Office guidance suggests that the case investigator will be able to fulfil this role and that legally trained personnel shall not be required to make the case to the JP albeit they can attend to assist the officer.

50. Any officer who presents the case to the JP must be formally designated under the Council's Standing Orders to do so as the investigating officer. This must be checked and in place before the hearing.

Decision

51. The JP will consider:
    a. whether they are satisfied that at the time the authorisation or notice was granted or renewed, there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate;
    b. whether there continues to be reasonable grounds;
    c. whether they are satisfied that the person who granted the authorisation or notice was an appropriate designated person within the Council and that the authorisation was made in accordance with RIPA and any other legal restrictions.

52. If more information is required by the JP or if there is an error on the application form, the application is likely to be refused. It is therefore vital to make sure the application is correct and all supporting documents are provided.

53. The JP may decide to:
    a. Approve the grant or renewal of an authorisation or notice. The RIPA authorisation will then take effect and the Council may proceed to use the technique in that particular case.
    b. Refuse to approve the grant or renewal. The RIPA authorisation will not take effect and the Council must not use the technique in that case. The original internal authorisation remains and the Council can try and re-apply for judicial approval depending on the circumstances of the refusal.
    c. Refuse to approve the grant or renewal and quash the authorisation or notice. This not only prohibits the use of the technique applied for by quashes the internal authorisation. The court must not exercise this power unless the Council has had at least two business days from the date of the refusal in which to make representations.

54. A JP's decision can be appealed, but only on a point of law by judicial review. Advice from Legal should be sought if such a concern arises.

Collateral Intrusion

55. Before authorising the use or conduct of a source, the authorising officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the operation or investigation (collateral intrusion). Measures should be

taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

56. An application for an authorisation should include an assessment of the risk of any collateral intrusion. The authorising officer should take this into account, when considering the proportionality of the use and conduct of a source.

Practical Considerations

57. The Council's requirements for covert surveillance will normally be carefully planned so that the necessary consultations regarding risk assessment, insurance and health and safety can be carried out and the required provisions put in place before surveillance commences.

58. In the event of covert surveillance needing to be carried out in an emergency, authorisation is still required and must be a written application for authorisation.

59. General observation forms part of the duties of many enforcement officers and is not usually regulated by RIPA. For example, community wardens or coastal officers may be on patrol to observe or prevent crime. Such observation 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.

60. Directed surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by its very nature, could not have been foreseen. For example, a community warden or coastal officer would not require an authorisation to conceal him or herself and observe a suspicious person that s/he came across in the course of a patrol. If later, however, a specific investigation or operation is to follow an unforeseen response, authorisation must be obtained in the usual way before it can commence. In no circumstance will any covert surveillance / use of a CHIS be given backdated authorisation after it has commenced.

61. Embarking upon covert surveillance or the use of a CHIS without authorisation or conducting surveillance outside the scope of the authorisation will not only mean that the protection afforded by RIPA is negated but may also result in disciplinary action being taken against the officer / officers involved.

62. Although, the provisions of RIPA do not normally cover the use of overt CCTV surveillance systems, since members of the public are aware that such systems are in use, there may be occasions when public authorities use overt CCTV systems for the purposes of a specific investigation or operation. In such cases, authorisation for directed surveillance will be necessary.

63. Material obtained through covert surveillance may be used as evidence in criminal proceedings. The proper authorisation of surveillance should ensure the admissibility of such evidence under the common law, section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998. Furthermore, the product of the surveillance described in this code is subject to the ordinary rules for retention and disclosure of material under the Criminal Procedure and Investigations Act 1996.

64. Whilst acknowledging that covert surveillance / use of a CHIS is a last resort, RIPA does afford potential protection against claims of unlawful action. Officers must seek the view of an Authorising Officer if they are in any doubt as to whether RIPA is likely to apply to their investigation or action.

65. Where the use of a CHIS is deployed, a "Controller" and a "Handler", who can be officers of the Council, should be designated to have day to day responsibility for dealing with the CHIS. This will include their security, safety and welfare and a Risk Assessment should be completed to cover this.

66. The only circumstances where authorisation may be given under this regime is where the investigation is for the purpose of preventing or detecting crime or for preventing disorder.

Special Circumstances

67. The use of vulnerable people / juveniles for a CHIS should only occur in exceptional circumstances and due regard must be had to the Code of Practice.

68. Likewise, if covert surveillance is likely to obtain communications subject to legal privilege, or involve confidential personal or journalistic information or material, the officer should refer to the Code of Practice. An authorisation will then only be merited in exceptional or compelling circumstances.

69. Where Special Circumstances apply officers must obtain authorisation for the action from the relevant Executive Director.

Partnership Working

70. If conducting a relevant RIPA investigation in partnership with, under the direct guidance or supervision of or under a request from another body, officers must first seek the approval of an Authorising Officer.

71. When another agency wishes to use the Council's resources, that agency must use its own RIPA procedures. Before any officer agrees

to permit the use of Council resources, they must obtain a copy of that agency's RIPA form for the record, and/or relevant extracts from the form.

Training

72. All officers with an enforcement or investigatory function will receive training on the provisions of RIPA.

Central Record of all authorisations

73. The Senior Responsible Officer will be responsible for maintaining a record of all authorisations, renewals, reviews and cancellations issued by the Council. The RIPA Co-Ordinator will keep an electronic copy of the register.

74. The Requesting Officer will also be responsible for forwarding a copy of each and every form completed for that purpose to the RIPA Co-Ordinator within one week of completing that form. The form should be sent in an envelope marked Private and Confidential and for the attention only of the RIPA Co-Ordinator. The RIPA Co-Ordinator will then maintain the Central Record of Authorisations.

75. These records will be retained for a period of at least three years from the ending of the authorisation and should contain the following information:
- the type of authorisation;
- the date the authorisation was given;
- name and rank/grade of the authorising officer;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- whether the urgency provisions were used, and if so why.
- if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer;
- whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
- the date the authorisation was cancelled.

76. The Senior Responsible Officer will act as Audit Manager who is responsible for monitoring authorisations and carrying out annual and random reviews of applications, authorisations, reviews, renewals and cancellations.

Conclusion

77. The Senior Management Team will review this policy annually with the support and assistance of the Senior Responsible Officer and the RIPA Co-Ordinator, and such other officers as the portfolio holder may require. In addition, the Senior Responsible Officer will provide a yearly report to the relevant portfolio holder on the use of the powers under the Act to ensure that the powers are being used consistently with the local authority's policy and that the policy remains fit for purpose.

78. All enquiries about this policy or the applicability of RIPA should be referred at first instance to the RIPA Co-Ordinator or such other person as they may designate.

79. For additional information / guidance please see the Home Office or Office of the Surveillance Commissioners websites.

APPENDIX 1

Current List of Authorising Officers/Designated Persons

Executive Director of Business Operations

Executive Director of Resources

Senior Responsible Officer

Service Manager - Corporate and Human Resources – John Collins

RIPA Co-Ordinator

Deputy Legal Services Manager – Andy Eaton
Rother & Wealden District Councils Shared Legal Service

Appendix 2

Guidance Notes

Authorisation will be required for a proposed activity if the answer is 'Yes' to all of questions 1 – 7 below.

If the answer is 'No' to any of them, the proposed activity will not be entitled to protection under RIPA and authorisation will not be granted so should not be the subject of an application request.

1. Is there a need for covert surveillance. Is it necessary and proportionate in accordance with the Act and the Code of Practice? The activity will not be proportionate if it is excessive in the circumstances or if the information could reasonably be obtained by other less intrusive means.
2. Is the proposed activity 'surveillance'? Will it comprise monitoring, observing or listening to persons, their movements, their conversations or their activities and/or recording anything monitored, observed or listened to in the course of the proposed activity?
3. Is it covert? Will the activity be carried out in a manner calculated to ensure that the target will be unaware that it is or may be taking place.
4. Is it directed? Will the activity be for the purpose of a specific operation or investigation?
5. Is it likely to result in the obtaining of private information about this person?
6. Is there a risk of obtaining private information about another person? (this is known as collateral intrusion). If so, has the necessary risk assessment been carried out and is the covert surveillance proportionate in the circumstances.
7. Is it a foreseen / planned response? Is it something other than an immediate response in circumstances where it is not reasonable to get an authorisation?

Other important matters:

a. Has a risk assessment been completed that identifies all relevant risks to staff in the conduct of the operation. This is particularly important where a CHIS is being deployed.
b. On completion of the authorisation, has the AO set a review date for re-consideration of the authorisation?
c. Has the authorisation been approved by a Magistrates' court?
d. On completion of the surveillance, the Applicant must complete the cancellation form.
e. Ensure that the most up to date forms are used by downloading copies from the Home Office website on the link provided in the policy.