BUCKINGHAMSHIRE COUNTY COUNCIL

www.buckscc.gov.uk

Covert Surveillance Policy and Procedure

REGULATION OF INVESTIGATORY POWERS ACT 2000 – PART 2

TABLE OF CONTENTS

1.	**COVERT SURVEILLANCE POLICY STATEMENT**	**3**
2.	**GENERAL BACKGROUND**	**5**
3.	**WHAT IS COVERT SURVEILLANCE?**	**8**
4.	**WHAT IS COVERT HUMAN INTELLIGENCE**	**10**
5.	**AUTHORISATION**	**12**
6.	**AUTHORISATION PROCEDURES**	**16**
7.	**APPENDIX A - SURVEILLANCE PERSONNEL LIST**	**20**
8.	**APPENDIX B - FLOWCHART OF APPLICATION PROCESS**	**21**
9.	**APPENDIX C – ADDITIONAL INFORMATION ON THE USE OF CHIS**	**23**
10.	**APPENDIX D - LIST OF FORMS IN USE FOR SURVEILLANCE DATA REQUESTS**	**25**

COVERT SURVEILLANCE POLICY STATEMENT

Introduction

1. Buckinghamshire County Council is committed to building a fair and safe community for all by ensuring the effectiveness of laws designed to protect individuals, businesses, the environment and public resources.

2. Buckinghamshire County Council recognises that most organisations and individuals appreciate the importance of these laws. The council will, therefore, use its best endeavours to help them meet their legal obligations without unnecessary expense and bureaucracy.

3. At the same time the Council has a legal responsibility to ensure that those who seek to flout the law are the subject of firm but fair enforcement action. Before taking such action, the council may need to undertake covert surveillance of individuals and/or premises. The purpose of this covert surveillance will be to obtain evidence of criminal offences and anti social behaviour.

Procedure

4. All covert surveillance shall be undertaken in accordance with the procedures set out in this policy.

5. Buckinghamshire County Council shall ensure that covert surveillance is only undertaken where it complies fully with all applicable laws, in particular the following:

    - Regulation of Investigatory Powers Act 2000
    - Human Rights Act 1998
    - Data Protection Act 1998
    - Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

6. The Council shall, in addition, have due regard to all official guidance and codes of practice particularly that issued by the Home Office, the Office of the Surveillance Commissioners (OSC) and the Information Commissioner.

7. In particular the following guiding principles shall form the basis of all covert surveillance activity undertaken by the Council:

    - All authorisations to carry our covert surveillance shall be granted by appropriately trained and designated authorising officers.

    - Covert surveillance shall only be undertaken where it is absolutely necessary to achieve the desired aims.

- Covert surveillance shall only be undertaken where it is proportionate to do so and in a manner that it is proportionate.

- Adequate regard shall be had to the rights and freedoms of those who are not the target of the covert surveillance

Training and Review

8. All council officers undertaking covert surveillance shall be appropriately trained to ensure that they understand their legal and moral obligations.

9. Regular audits shall be carried out to ensure that officers are complying with this policy.

10. This policy shall be reviewed at least once a year in the light of the latest legal developments and changes to official guidance and codes of practice.

11. The operation of this policy shall be overseen by the Council's Overview and Scrutiny Committee, which will receive reports on a quarterly basis.

Conclusions

12. All citizens will reap the benefits of this policy, through effective enforcement of criminal and regulatory legislation and the protection that it provides.

13. At the same time, adherence to this policy, when undertaking covert surveillance, will minimise intrusion into peoples' lives and will avoid any legal challenge to the council's activities or evidence.

GENERAL BACKGROUND

Legislation

1. The Regulation of Investigatory Powers Act 2000 (RIPA) provides the legislative framework within which covert surveillance operations must be conducted in order to ensure that investigatory powers are used lawfully and in accordance with human rights.

2. This document takes into account the changes made to the RIPA regime by the Home Office, which came into force on 6th April 2010 by virtue of three new statutory instruments:

    - The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, SI 2010/521

    - The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Code of Practice) Order 2010, SI 2010/462

    - The Regulation of Investigatory Powers (Covert Surveillance and Property Interference: Code of Practice) Order 2010, SI 2010/463

3. Officers and investigators involved in covert surveillance operations must familiarise themselves with the provisions of :

    - Article 8 of the European Convention on Human Rights 1958
    - The Human Rights Act 1998
    - Part 2 of the Regulation of Investigatory Powers Act 2000
    - The Covert Surveillance Code of Practice ("the DS Code")
    - The Covert Human Intelligence Sources Code of Practice ("the CHIS Code")

Codes of Practice

4. The Code of Practice on Covert Surveillance and Property Interference" and the "Code of Practice on Covert Human Intelligence Sources" came into force on 6 April 2010. Whilst the Codes are not themselves law, they are citable in a court of law and any deviation from them may have to be justified. Council officers involved in surveillance activities should be familiar with its content. The Codes of Practice are available at:

    http://tna.europarchive.org/20100413151426/http:/security.homeoffice.gov.uk/ripa/making-an-app-under-RIPA/codes-of-prac/index.html

RIPA Forms

5. Copies of forms referred to in this document can currently be found at the following address:
    http://tna.europarchive.org/20100413151426/http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/indexcd98.html?d-7095067-p=1

6. The Home Office website is at http://www.homeoffice.gov.uk/

Compliance with RIPA

7. The Human Rights Act 1998 (which brought much of the European Convention on Human Rights and Fundamental Freedom 1950 into UK domestic law) requires the City Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, his home and his correspondence.

8. Covert surveillance may constitute an interference with the privacy of individuals who are subject to investigation and of members of the public who are present on a site which is subject to surveillance. Such an interference engages an individual's right to private life, family life, home and correspondence under Article 8(1) ECHR. However interference with that right can be justified where it is prescribed by law and proportionate to the pursuit of a legitimate aim. Part II of RIPA provides a statutory mechanism for authorising covert surveillance and the use of a 'covert human intelligence source'. It is intended to ensure that the proper balance is struck between the right to privacy and, in the local authority context, the legitimate aim of preventing or detecting crime and preventing disorder.

9. It is vital that the substantive requirements and the process set out in Part II of RIPA are adhered to. Provided these requirements are complied with, the Council and its officers should have a legal defence to any legal proceedings by virtue of s27, which states that conduct under Part II is lawful provided it is authorised; and is in accordance with that authorisation.

10. The information obtained by surveillance in accordance with Part II of RIPA will, provided lawfully obtained, be admissible in criminal, civil and tribunal proceedings. However failure to comply with Part II can also render information obtained by surveillance inadmissible. It is therefore vital that the requirements put in place under RIPA are observed to protect the interests of both the Council and the Officers involved.

WHAT IS COVERT SURVEILLANCE?

11. Under s48(2) Regulation of Investigatory Powers Act 2000 ("RIPA"), surveillance includes:

- 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; and
- surveillance by or with the assistance of a surveillance device.

12. Most of the Council's surveillance activities will be overt. Under s26(9)(a) of RIPA, surveillance is "covert" if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place.

13. Covert Surveillance can be an important tool in assisting the Council's officers to fulfil their duties in relation to the prevention and detection of crime or the prevention of disorder. This includes the prevention and detection of anti-social behaviour.

14. RIPA distinguishes between two categories of covert surveillance, namely, **Directed Surveillance** and **Intrusive Surveillance**.

Directed Surveillance

15. "Directed Surveillance" is defined under s26(2) as covert surveillance that is not intrusive surveillance and is undertaken:

- for the purposes of a specific investigation or operation;
- in such a manner as is likely to result in the obtaining of *private information* about a person (whether or not that person is a person subject to the investigation)
- 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 RIPA to be sought for the carrying out of the surveillance.

16. This can include surveillance of Council employees.

17. **"Private information"** about a person should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships. The covert surveillance of a person's activities in a public place may still result in the obtaining of private information where a person has a reasonable expectation of privacy; and where a record is being made by a public authority of that person's activities.

"Private information" includes personal data, such as names, telephone numbers and address details.

18. Regard must be had to the totality of any records held about a person, even where individual records do not constitute "private information".

19. There are two further situations which *may* constitute directed surveillance[1]:

- Where information is derived from surveillance devices which provide information about the location of a vehicle alone, and is coupled with other surveillance activity from which private information is obtained. However the use of vehicle surveillance devices in itself does not necessarily involve the provision of "private information".

- Where postal or telephone communications are intercepted and one either the sender or the recipient has consented to the interception (and where there is no interception warrant).

Intrusive Surveillance

20. **Intrusive Surveillance** is defined under s26(3) as covert surveillance that is:

- carried out in relation to anything taking place on any residential premises or in any private vehicle; and
- involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device on the premises or in the vehicle or is carried out by means of a surveillance device that, although not on the premises or in the vehicle, provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

21. It is **not** necessary to consider whether intrusive surveillance is likely to result in the obtaining of "private information"[2]. The categorisation of surveillance as "intrusive" relates to the location of the surveillance activity rather than the nature of the information obtained.

22. For the purposes of RIPA, residential premises include hotel rooms, hostel rooms and prisons but not common areas to which a person is allowed access in connection with occupation (for example a communal stairway, hotel reception area or dining room, or front garden or driveway which is readily visible to the public)[3].]

23. The definition of **"premises"** under RIPA is broad, and extends to any place whatsoever, including any vehicle or moveable structure, whether or not occupied as land.

1

2 Para 2.12
3 Para 2.13-2.16

24. Under the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010, directed surveillance shall be intrusive surveillance if carried out on the following premises:

- Any place where persons serving sentences, in custody or on remand may be detained
- Any place of detention pursuant to immigration powers
- Police stations
- Hospitals where high security psychiatric services are provided
- The place of business of any legal adviser
- Any place used for the business of a court, tribunal, inquest or inquiry.

25. The Council's officers **CANNOT AUTHORISE** intrusive surveillance under RIPA.

WHAT IS COVERT HUMAN INTELLIGENCE?

26. A covert human intelligence source ("**CHIS**") is a person who establishes or maintains a relationship with someone in order to covertly obtain information, to provide another person with access to information or to disclose information as a consequence of that relationship. Essentially, this covers the use of informants and undercover officers.

27. Whether a **"relationship"** has been established will depend on all the circumstances, including the duration of the contact and the nature of the covert activity.

Test Purchasers

28. For example, where a test purchaser makes a single purchase, the relationship is likely to be too limited to require a CHIS authorisation. On the other hand if the test purchaser has to become acquainted with the vendor in order for him to make a sale, a relationship will have been established and the test purchaser will be treated as a CHIS. If there is any doubt whether authorisation is required in relation to a particular operation then the Investigating Officer should seek authorisation.

The use of juveniles as a CHIS

29. If a person under the age of 18 is to be used as a source, authorisation must be obtained from either the Head of Paid Service or (in his absence) the person acting as the Head of Paid Service.

30. On no occasion should the use or conduct of a person under 16 be authorised to give information against his parents or any person who has parental responsibility for him.

31. The *Regulation of Investigatory Powers (Juvenile) Order 2000* SI 2793 applies to the use of juvenile sources. This requires that where a source is under 16, an appropriate adult must be present at all meetings between the source and the Council's officers. The Order also requires a detailed risk assessment to be undertaken where a source is under 18. The existence and magnitude of any physical or psychological risk must be identified and the Authorising Officer must be satisfied that the use of the source is justified in light of that risk and that the risk has been properly explained to and understood by the source.

32. Authorisations for the use of juvenile source cease after 1 month instead of 12 months.

33. The use of a juvenile e.g. to attempt to buy alcohol or tobacco from a shop suspected of selling to persons under age may not constitute the use of a juvenile as a CHIS for the reasons set out at paragraph 2 above.

Members of the public as informants

34. A member of the public who reports a matter e.g. about unlawful trading to an officer is not a CHIS: . If an Investigating Officer wishes to request that person to e.g. maintain a relationship with a trader and keep records of their dealings or to make further inquiries of a trader, authorisation will, however, be required.

Monitoring the use and welfare of CHIS

35. Section 29(5) of RIPA provides that an Authorising Officer may only authorise the use of a CHIS if satisfied that there is at all times a person with the responsibility for keeping a record of the use made of the source. The Regulation of Investigatory Powers (Source Records) Regulations 2000 SI 2000/2725 sets out the particulars that must be included in the records relating to each source.

36. At all times, an individual officer should be appointed to manage a particular source. Before authorising the use or conduct of a CHIS, the Council should carry out a risk assessment to determine the risk to the CHIS and the likely consequences, should the role of the CHIS become known. Any matters of concern should be considered by the authorising officer and a decision taken as to whether to continue.

37. The ongoing safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled.

38. Material produced as a result of the use of a CHIS must be retained only for so long as necessary. When reviewing the retention of records, the Council must consider its duty of care to the CHIS and the likelihood of future civil or criminal proceedings relating to the information supplied.

39. Appendix C provides further information about the monitoring and welfare of CHIS.

AUTHORISATION

The Role of the Authorising Officer

40. **Directed Surveillance** must be authorised by an **Authorising Officer**. The Council's Authorising Officers are set out in the Surveillance Personnel List at Appendix A. The Head of Legal Services will revise the Personnel List as and when necessary.

41. An Authorising Officer may only authorise Directed Surveillance for the purpose of the prevention or detection of crime or the prevention of disorder. An Authorising Officer must further be satisfied:

    - that sufficient evidence exists and has been documented to warrant the use of the particular directed surveillance exercise requested
    - that the use of the particular directed surveillance exercise requested is both necessary and proportionate to the particular objective pursued.

42. **The use and conduct of CHIS** must also be authorised by an Authorising Officer. The Authorising Officer must be satisfied that the use or conduct of a CHIS is necessary in the circumstances of the case for one of the following reasons: for the purpose of preventing or detecting crime or of preventing disorder;

43. If one of the above grounds applies, the Authorising Officer must go on to consider whether the use or conduct of a CHIS is proportionate.

Proportionality

44. In considering whether a particular exercise would be proportionate the Authorising Officer must consider whether it is excessive in the overall circumstances of the case. The fact that an offence is serious is not sufficient to render intrusive actions proportionate. The Authorising Officer must consider the following elements:

    - The size and scope of the proposed surveillance activity, weighed against the gravity and extent of the suspected offence.
    - Whether the methods suggested will cause the least possible intrusion on the subject and others.
    - Whether the proposed activity is a legitimate and reasonable way of obtaining the necessary result.
    - Whether other methods have been considered and the reasons for their non-implementation

Additional Safeguards

Collateral intrusion

45. Before authorising applications for **directed surveillance or CHIS**, the authorising officer must take into account the risk of "collateral intrusion" i.e. the risk of obtaining private information about persons who are not subjects of the surveillance activity.

46. Measures should be taken, where practicable, to minimise unnecessary intrusion into the privacy of those who are not the intended subjects. However activities resulting in collateral intrusion may still be lawful if they are proportionate. Applications by investigating officers should therefore include an assessment of the risk of collateral intrusion and details of any measures to limit this.

47. Planned surveillance activity against individuals who are not direct suspects should be treated as intended, rather than collateral, intrusion.

Confidential and Legally Privileged Information

48. Particular care should be taken where an investigation involves confidential information. **Confidential information** consists of matters subject to legal privilege, confidential personal information or confidential journalistic material. Confidential personal information means information held in confidence relating to the physical or mental health or spiritual counselling of an individual. Confidential journalistic information means information held in confidence acquired or created for the purpose of journalism.

49. Public authorities may obtain knowledge of matters subject to legal privilege via CHIS in the following scenarios:

    - Where the authority has deliberately authorised the use or conduct of the CHIS to obtain knowledge of matters which are subject to legal privilege.
    - Where the CHIS obtains knowledge of matters subject to legal privilege through conduct which is incidental to his conduct as a CHIS.
    - Where a CHIS obtains knowledge of matters subject to legal privilege where his conduct is not incidental.

50. If the surveillance is likely to yield confidential information as defined above, authorisation must be sought from the Council's Head of the Paid Service (i.e. the Chief Executive) or, in his or her absence, the Acting Chief Executive.

Legal consultations

The Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010 states that directed surveillance carried out on premises which are, at any time during the surveillance, used for the purposes of "legal consultation", is to be treated as intrusive surveillance. "Legal consultation" is defined as:

- A consultation between a professional legal adviser and his client or any person representing his client or

- A consultation between a professional legal adviser or his client or any such representative and a medical practitioner made in connection with or in contemplation of legal proceedings or for the purpose of legal proceedings.

51. For further information about surveillance involving confidential or legally privileged information or legal consultation, officers should consult the Codes of Practice on Covert Surveillance and CHIS.

52. If there is any doubt as to whether information likely to be acquired would constitute confidential information, advice should be sought from Legal Services.

The use of agents and cooperation with other bodies

53. The Council can employ or recruit an agent e.g. an agent with more specialised equipment than the Council would have available to act on its behalf in conducting surveillance. The same authorisation procedures must be followed.

54. The Council might wish to involve personnel or equipment from one of the Borough or District Councils in the course of its investigations. If such a request is to be made, the County Council will have to follow the usual authorisation procedures and the usual procedures in relation to record-keeping and the handling of information and will share sight of the authorisation with any third party agent.

55. The Council should also be mindful of any similar surveillance taking place in other areas which could have an impact on its activities. Where an authorising officer considers that conflicts may arise, they should consult a senior police officer within the area.

AUTHORISATION PROCEDURES

56. The authorisation procedures are intended to ensure that any interference with privacy is subject to rigorous scrutiny. However, they also provide an opportunity for further discussion and refinement of the methods to be used in a particular investigation.

57. Applications for authorisation for Directed Surveillance must be made on the form **2007-01 DS Application.**

58. Applications for authorisation for the use of CHIS must be made on the form **2007-1 CHIS Application**.

59. The written application must describe:
    - the reason why the authorisation is necessary in the particular case for the prevention or detection of crime or the prevention of disorder
    - the purpose of the surveillance
    - the nature of the surveillance
    - the identities, where known, of those to be subject to the surveillance
    - an explanation of the information which it is desired to obtain as a result of the surveillance
    - the nature and extent of any likely collateral intrusion and why it is justified
    - the nature and extent of any likely confidential information
    - the level of authorisation needed
    - the reason why the surveillance is considered proportionate to what it seeks to achieve
    - a subsequent record of whether authority was given or refused, by whom and on what date

60. The Authorising Officer must satisfy him or herself that the particular surveillance requested is proportionate to the particular aim pursued in the course of the investigation. It is ultimately for the Authorising Officer to decide whether or not the proposed surveillance is necessary and proportionate.

61. The current Authorising Officers are set out in the Surveillance Personnel List. The Head of Legal Services will revise the Personnel List as and when necessary.

62. If the application is granted, the Authorising Officer must record the reasons for authorisation. If the application is refused, the Authorising Officer must record the reasons for refusal.

Duration and termination of authorisation

63. A written authorisation for **directed surveillance** granted by an Authorising Officer will cease to have effect (unless renewed) at the end of a period of three months beginning on the day the authorisation took effect.

64. A written authorisation for the use of a **CHIS** granted by an Authorising Officer will cease to have effect (unless renewed) at the end of a period of twelve months beginning on the day the authorisation was given (or one month where the source is a juvenile).

65. Once the exercise for which authorisation has been granted has been carried out the Officer must complete a cancellation notice (**Form 2007-01 DS Cancellation** or **2007-1 CHIS Cancellation)** and submit this to the Authorising Officer for signature.

66. A written authorisation should be reviewed monthly to assess whether or not there is a need for surveillance to continue. The Authorising Officer must be satisfied that the continuation of the authorisation is justified. The Authorising Officer must record the reasons for concluding that a continuation of the authorisation is justified or, alternatively, must record the reasons for concluding that the authorisation should not be continued. The review should be conducted using the form **2007-01 DS Review** or **Form 2007-1 CHIS Review.**

67. At any time before an authorisation would cease to have effect, the Investigating Officer may apply to the Authorising Officer to renew the authorisation. The Authorising Officer must be satisfied that the renewal would be proportionate. The authorisation of directed surveillance may be renewed for a further 3 months, taking effect at the time or on the day on which the authorisation would otherwise have ceased to have effect. The Authorising Officer must record the reasons for renewal. An application for renewal must be made using the form **2007-01 DS Review** or Form **2007 – 1 CHIS Renewal.**

68. All applications for a written renewal should record:

    - whether this is the first renewal or every occasion on which the authorisation has been renewed previously
    - any significant changes since the original application or last renewal or last review, as appropriate.
    - the reasons why continued surveillance is necessary
    - the content and value to the investigation of information so far obtained by the surveillance
    - the results of regular reviews of the investigation

69. Reviews and renewal applications for the use of a **CHIS** should also include the use made of the source during the period authorised, the tasks given to the source and the information obtained from the source.

70. An application for renewal should not be made until shortly before the authorisation period is drawing to an end.

71. Authorisations may be renewed more than once, provided they meet the criteria for authorisation.
72. During a review the authorising authority may amend the authorisation or cancel it, if the criteria for its initial authorisation are no longer met. As soon as the decision is taken to discontinue surveillance, all those involved in the surveillance must be notified.

Record Keeping

73. Copies of all signed forms of authorisation, renewals and cancellations should be filed on the case file and the originals should be sent to Legal Services for filing on the RIPA Authorisation File by the RIPA Coordinator. Forms will be kept for 5 years following the ending of an authorisation or relevant court proceedings.

74. The RIPA Co-ordinator will maintain a database of applications containing the following information:
    - the type of authorisation
    - the date the authorisation was given
    - the name and rank of the authorising officer
    - the unique reference number of the investigation or officer
    - the title of the investigation or operation including a brief description and the names of subjects if known
    - the date of any renewals and the name and rank of the officer authorising renewal
    - whether the investigation was likely to result in obtaining confidential information and whether any such information was obtained
    - the date the authorisation was cancelled
    - Whether the authorisation was granted by an individual directly involved in the investigation

75. The RIPA Co-ordinator will further maintain copies of all applications (whether or not authorisation was given) with supplementary documentation; a record of the period over which surveillance has taken place; the frequency of reviews; the result of any reviews; copies of any renewals of authorisation; the date and time of any instructions given by the authorising officer.

Handling of material and use of material as evidence

76. Material produced as a result of directed surveillance may be used in criminal proceedings and must be retained only for so long as necessary.

77. All material obtained as a result of covert surveillance will be recorded and logged in the investigating Officer's notebook in accordance with the usual procedures for the logging of evidence.

78. Material obtained using covert surveillance should be disposed of in accordance with the *Criminal Procedures and Investigations Act 1996*. Public authorities must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use of directed or intrusive surveillance. Authorising officers must also ensure compliance with the requirements of the Data Protection Act 1998.

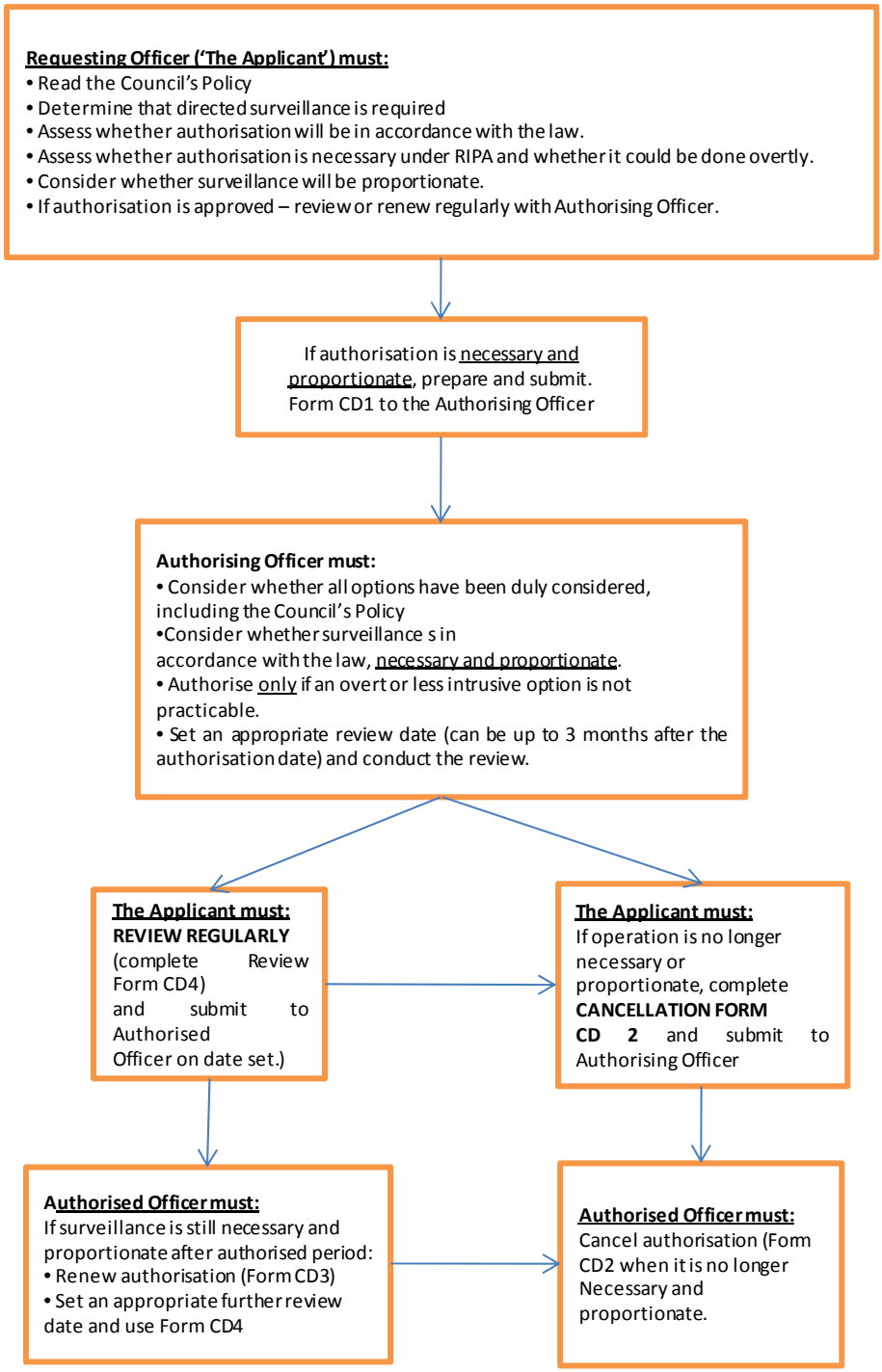
APPENDIX A

SURVEILLANCE PERSONNEL LIST

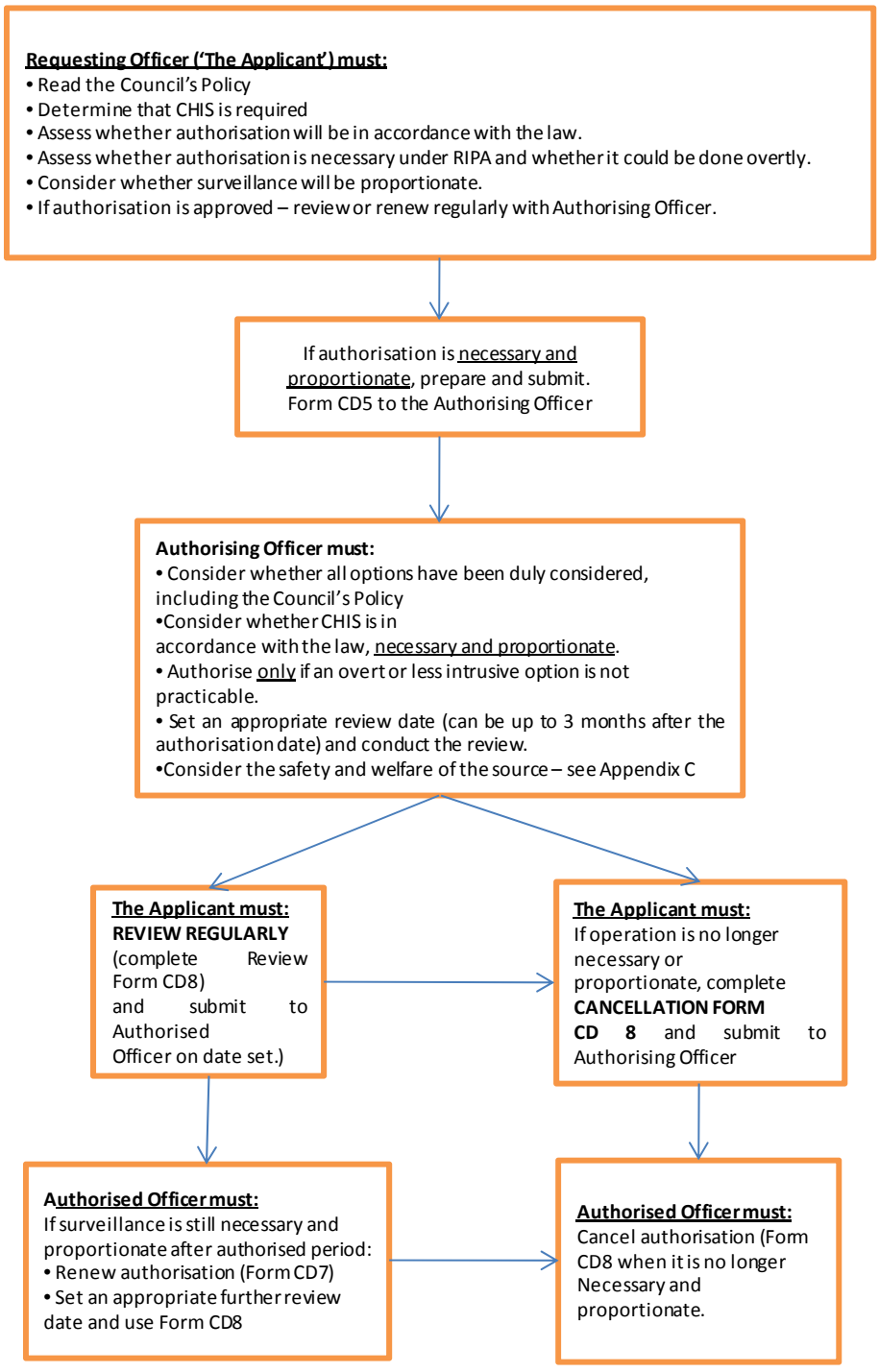
ROLE	NAME	JOB TITLE	DEPARTMENT
AUTHORISATION WHERE CONFIDENTIAL INFORMATION LIKELY TO BE ACQUIRED; USE OF JUVENILE CHIS	CHRIS WILLIAMS	CHIEF EXECUTIVE	HEAD OF PAID SERVICE
SENIOR RESPONSIBLE OFFICER	ANNE DAVIES	HEAD OF LEGAL AND DEMOCRATIC SERVICES	LEGAL & DEMOCRATIC SERVICES
AUTHORISING OFFICER	YVONNE GIBSON	GROUP SOLICITOR	LEGAL AND DEMOCRATIC SERVICES
AUTHORISING OFFICER	TERRY CARTER	ASSISTANT HEAD OF TRADING STANDARDS	TRADING STANDARDS
AUTHORISING OFFICER	AMANDA POOLE	ASSISTANT HEAD OF TRADING STANDARDS	TRADING STANDARDS
RIPA CO-ORDINATOR	HELEN FULLARTON	PA TO YVONNE GIBSON	LEGAL AND DEMOCRATIC SERVICES

APPENDIX B

FLOWCHART 1: DIRECTED SURVEILLANCE



FLOWCHART 2: CHIS



APPENDIX C

Additional Notes on CHIS (From Home Office Code of Practice On CHIS)

Management of sources

Tasking

Tasking is the assignment given to the source by the persons defined at sections 29(5)(a) and (b) of the 2000 Act, asking him to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant public authority. Authorisation for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

The person referred to in section 29(5)(a) of the 2000 Act will have day to day responsibility for: dealing with the source on behalf of the authority concerned; directing the day to day activities of the source; recording the information supplied by the source; and monitoring the source's security and welfare.

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 source.

In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example a source may be tasked with finding out purely factual information about the layout of commercial premises. Alternatively, a trading standards officer may be involved in the test purchase of items which have been labelled misleadingly or are unfit for consumption. In such cases, it is for the relevant public authority to determine where, and in what circumstances, such activity may require authorisation.

It is not the intention that authorisations be drawn so narrowly that a separate authorisation is required each time the source is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task. If this changes, then a new authorisation may need to be sought.

It is difficult to predict exactly what might occur each time a meeting with a source takes place, or the source meets the subject of an investigation. There may be occasions when unforeseen action or undertakings occur. When this happens, the occurrence must be recorded as soon as practicable after the event and, if the existing authorisation is insufficient it should either be updated and reauthorized (for minor amendments only) or it should cancelled and a new authorisation should be obtained before any further such action is carried out.

Similarly where it is intended to task a source in a new way or significantly greater way than previously identified, the persons defined at section 29(5)(a) or (b) of the 2000 Act must refer the proposed tasking to the authorising officer, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and the details of such referrals must be recorded.

Management responsibility

Public authorities should ensure that arrangements are in place for the proper oversight and management of sources, including appointing individual officers as defined in section 29(5)(a) and (b) of the 2000 Act for each source.

The person responsible for the day-to-day contact between the public authority and the source will usually be of a rank or position below that of the authorising officer.

In cases where the authorisation is for the use or conduct of a source whose activities benefit more than a single public authority, responsibilities for the management and oversight of that source may be taken up by one authority or can be split between the authorities.

Security and welfare

Any public authority deploying a source should take into account the safety and welfare of that source, when carrying out actions in relation to an authorisation or tasking, and to foreseeable consequences to others of that tasking. Before authorising the use or conduct of a source, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorisation, should also be considered at the outset.

The person defined at section 29(5)(a) of the 2000 Act is responsible for bringing to the attention of the person defined at section 29(5)(b) of the 2000 Act any concerns about the personal circumstances of the source, insofar as they might affect: the validity of the risk assessment, the conduct of the source, and the safety and welfare of the source.

Where deemed appropriate, concerns about such matters must be considered by the authorising officer, and a decision taken on whether or not to allow the authorisation to continue.

APPENDIX D

LIST OF FORMS IN USE FOR COVERT SURVEILLANCE

Form CD1: **Directed Surveillance** Application

Form CD2: **Directed Surveillance Cancellation**

Form CD3: **Directed Surveillance Renewal**

Form CD4: **Directed Surveillance Review**

Form CD5: **CHIS Application**

Form CD6: **CHIS Cancellation**

Form CD7: **CHIS Renewal**

Form CD8: **CHIS Review**