Report to Audit and Governance Committee

Date:	27 November 2023
Title:	**Annual RIPA and Communications Data Report**
Author and/or contact officer:	Nick Graham, Service Director – Legal and Democratic
Ward(s) affected:	All
Recommendations:	The Committee is asked:

1. **To note the contents of the Report**
2. **To agree the annual report is to be made on the first committee after January of each year.**

Reason for decision: Member oversight of the use of RIPA powers and policies are part of governance arrangements in relation to exercise of the Council's functions.

1. Executive summary

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA) governs the acquisition and disclosure of communications data and the use of covert surveillance by local authorities.

1.2 The Council can use powers under RIPA and IPA to support its core functions for the purpose of prevention and detection of crime where an offence may be punishable by a custodial sentence of 6 months or more or the offence is related to the underage sale of alcohol and/or tobacco (RIPA) or it relates to the prevention or detection of an offence punishable by a custodial sentence of 12 months or more, or in some cases where it relates to the prevention or detection of any crime or of preventing disorder (IPA).

1.3 RIPA powers cover covert surveillance which means monitoring or surveillance, and/or the recording, of an individual, either in person or using devices or the internet and includes the use of directed surveillance and also the use of covert human intelligence sources (CHIS).

1.4 IPA powers cover information about communications. It has been described as "the 'who', 'where', 'when', 'how' and 'with whom' of a communication but not what was written or said. It includes information such as the subscriber to a telephone service"

1.5 In order to use powers under RIPA or IPA there are procedures that the Council must follow to obtain the required authorisation.

1.6 The Home Office Covert Surveillance and Property Interference Revised Code of Practice (August 2018) recommends that elected members, whilst not involved in making decisions or specific authorisations should review the Council's use of the legislation and provide approval to its policies.

2. Background

Regulation of Investigatory Powers Act 2000

2.1 The Council can only use powers under RIPA to support its core functions for the purpose of prevention and detection of crime. RIPA procedures must be used where there is any covert surveillance in relation to an investigation of an offence punishable by a custodial sentence of 6 months or more or the offence is related to the underage sale of alcohol and/or tobacco.

2.2 Where used, RIPA powers are is usually undertaken by enforcement teams and Trading Standards.

2.3 Covert surveillance can include but is not limited to monitoring of social media, audio or visual recording of individuals either by CCTV or by officers, test purchases or other surveillance.

2.4 RIPA procedures require an internal approval by an Authorised Officer to ensure the proposed use of RIPA powers is 'necessary and proportionate'. A judicial approval is then required by the Magistrates Court before surveillance can be carried out. There are strict time limits for how long surveillance can continue, renewal of authorisations and requirements for record keeping.

2.5 The Council has a Covert Surveillance Policy and Procedure which governs the Council's use of RIPA and is reproduced at Appendix A.

2.6 The Council is required to have a Senior Responsible Officer to maintain oversight of RIPA arrangements, procedures and operations. Buckinghamshire Council's Senior Responsible Officer is the Service Director, Legal and Democratic Services.

Investigatory Powers Act 2016

2.7 The Council can only use IPA powers for the prevention or detection of an offence punishable by a custodial sentence of 12 months or more (serious crime). If however the data sought only relates to an entity such as a subscriber details the

powers can be used for the prevention or detection of any crime or of preventing disorder.

2.8 IPA powers are usually used by enforcement teams.

2.9 Procedures for obtaining communications data require internal notifications and all applications to be approved by the Office for Communications Data Authorisations (OCDA). The process is co-ordinated by the National Anti Fraud Network (nafn) on behalf of relevant public authorities with both OCDA and telecommunications providers.

2.10 As the authorisation process is co-ordinated by nafn there are specific portals and procedures which have to be followed. The Council therefore follows the nafn Workflow requirements.

2.11 The Council officer designated as the Approved Rank for supervision is Head of Legal Services (Non-Contentious).

Investigatory Powers Commissioner

2.12 The Investigatory Powers Commissioner has a statutory responsibility for reviewing the use of investigatory powers by public authorities throughout the United Kingdom.

2.13 As part of this oversight IPCO carry out regular inspections, usually every 3 years, to ensure compliance with surveillance powers. This will involve consideration of both the arrangements in place, governance and use of the powers. Feedback and recommendations for improvement will be made where considered appropriate.

2.14 As part of IPCO's inspections of nafn the Council's applications under IPA may be considered.

2.15 In addition IPCO require annual statistical data for RIPA each year. The Annual Report is published on the IPCO website at the following link https://www.ipco.org.uk/publications/annual-reports/

3. Matters to Consider

Exercise of Powers

3.1 Since the last report to the Committee relating to RIPA (27 September 2023) there have been no applications to use RIPA powers.

3.2 The Committee also requested statistics relating to IPA applications. Since January 2022, the Council has made 4 IPA applications. All related to mobile phone records.

3.3 It is suggested that future reports are now made at the first meeting of the committee after January each year as this will co-ordinate with the annual statistics return to IPCO.

Review of Procedures

3.4 As IPCO carried out a review in the summer and it is proposed that minor reviews of the RIPA Policy are brought to the annual report after January 2024. It is considered that apart from any typographical errors any update will relate to clarifications and further explanations only.

Training and awareness

Regular training for Authorising Officers and relevant applicant officers is required and is now due. Appropriate training is currently being identified so this can be delivered.

4. Other options considered

4.1 None.

5. Legal and financial implications

5.1 RIPA and IPA provides extensive powers for pubic authorities which are necessarily intrusive. It is an important part of the Council's governance arrangements that officers adhere to the Council's policies and the law when using these powers. An additional safeguard is regular inspection by IPCO.

6. Corporate implications

6.1 RIPA is only used as a last resort within the Council, but officers do need to be aware of these powers, and be appropriately trained in their use and authorisation. A training programme is in place to address this with relevant officers.

7. Local councillors & community boards consultation & views

7.1 Not applicable.

8. Communication, engagement & further consultation

8.1 Not applicable.

9. Next steps and review

9.1 A review of the Policy will be undertaken and a report will be brought back to the Committee on any recommended changes together with use of RIPA and IPA powers which have been used.

10. Background papers

10.1 None.

Appendix A
RIPA and IPA Report

BUCKINGHAMSHIRE COUNCIL

Covert Surveillance Policy and Procedure

REGULATION OF INVESTIGATORY POWERS ACT 2000 – PART 2

VERSION CONTROL

Version No	Reviewer	Key Changes	Date Amended
1	Joanna Swift	*Adoption*	1 April 2020
2	Maria Damigos	Minor updates	21 August 2023

TABLE OF CONTENTS

COVERT SURVEILLANCE POLICY STATEMENT

Introduction

1. Buckinghamshire 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 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 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 2018 and General Data Protection Regulation 2016/679
   - 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 Investigatory Powers Commissioner's Office (IPCO) 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 out covert surveillance shall be granted by appropriately trained and designated authorising officers.

10.2

- Authorisations for the use of directed surveillance, acquisition of communications data and the use of a CHIS under RIPA will need an order approving the grant or renewal of an authorisation or notice from a JP (a District Judge or lay magistrate) before they can take effect.

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

- Covert surveillance shall only be undertaken where it is proportionate to do so and in a manner that 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. The Senior Responsible Officer shall provide a report on the Council's use of RIPA to the Audit and Governance Committee on a regular basis as deemed appropriate. Annually, the report shall include a review of the effectiveness of this policy and any recommendation for changes to be made, including in the light of the latest legal developments and changes to official guidance and codes of practice.

Senior Responsible Officer

10. The Service Director Legal and Democratic Services is the designated Senior Responsible Officer who with the support of the RIPA Co-ordinator is responsible for the integrity of the process within Buckinghamshire Council and maintaining oversight and quality control in relation to RIPA functions and processes.

11. The RIPA Co-ordinator will have day to day responsibility for RIPA management including the following:

- Maintaining the Central Record of Authorisations together with collating submitted RIPA documentation;
- Day to day oversight of the submitted documents and the RIPA process;
- Organising a training programme and ensuring that relevant officers are fully RIPA trained;
- Raising RIPA awareness within the Council; and
- Liaising with the administration team at the magistrates' court to arrange a hearing and provide the necessary supporting documents and judicial application to obtain approval from a Justice of the Peace.

12. The Senior Responsible Officer is responsible for engagement with the Commissioners and Inspectors when they conduct their inspections and where necessary, overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner.

Conclusions

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

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

GENERAL BACKGROUND

Legislation

15. 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.

16. This document takes into account guidance issued by the Home Office under s71 of the 2000 Act and pursuant to the following 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

17. This document takes into account the Protection of Freedoms Act 2012.

18. 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 and Property Interference Revised Code of Practice ("the DS Code")
- The Covert Human Intelligence Sources Revised Code of Practice ("the CHIS Code")

19. Applications for access to communications data shall be made via the National Anti-Fraud Network (NAFN).

Codes of Practice

20. The most recent versions of the DS Code and the CHIS Code were issued in August 2018. 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 their content. The Codes of practice are available at:

https://www.gov.uk/government/collections/ripa-codes

RIPA Forms

21. Copies of forms referred to in this document can currently be found at the following address:

10.3 https://www.gov.uk/government/collections/ripa-forms--2

22. The Home Office website is at https://www.gov.uk/government/organisations/home-office

Compliance with RIPA

23. 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 Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, their home and correspondence.

24. 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.

25. 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.

26. 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.

10.4

27. The use of investigatory powers in the UK is overseen by the Investigatory Powers Commissioner. Further information on the role of the Commissioner and the Investigatory Powers Commissioner's Office can be found at: https://www.ipco.org.uk

Obtaining Judicial Approval of Authorisations

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

29. The Protection of Freedoms Act 2012 amends RIPA, to require that where an Authorising Officer has granted an authorisation for the use of directed surveillance or for the use of a CHIS, judicial approval will be required. The Council will be required to make an application, without giving notice, to the Magistrates' Court. The Magistrates will give approval if at the date of the grant of authorisation or renewal of an existing authorisation if and only if, they are satisfied that:

- there were reasonable grounds for believing that obtaining the covert surveillance or use of a human covert intelligence source was reasonable and proportionate and that these grounds still remain.
- the "relevant conditions" were satisfied in relation to the authorisation.

30. Relevant conditions are that:

- the relevant person was designated as an Authorising Officer
- it was reasonable and proportionate to believe that using covert surveillance or a covert human intelligence source was necessary and that the relevant conditions have been complied with;
- the grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under section 25(3) of RIPA; and
- any other conditions provided for by an order made by the Secretary of State were satisfied.

10.5

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

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

10.6

33. The form to be used for seeking judicial approval from the Magistrates Court is attached at Appendix F.

WHAT IS COVERT SURVEILLANCE?

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

- monitoring, observing or listening or 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.

35. 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.

36. 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.

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

Directed Surveillance

38. "Directed Surveillance" is defined under s.26(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 surveillance.

39. This can include surveillance of Council employees. However, it should be noted that a public authority may only seek authorisation under RIPA when it is performing its 'core functions'. 'Core functions' are the specific public functions undertaken by a particular public authority, in contrast to its 'ordinary functions' which are those undertaken by *all* authorities. For example, the disciplining of an employee is not a core function, although related criminal investigations may be.

40. **"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 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.

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

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

10.7

43. There are two further situations which *may* constitute directed surveillance:

- 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 once either the sender or recipient has consented to the interception (and where there is no interception warrant).

Intrusive Surveillance

44. **Intrusive Surveillance** is defined under s.26(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.

45. It is **not** necessary to consider whether intrusive surveillance is likely to result in the obtaining of "private information"[1]. The categorisation of surveillance as "intrusive"

[1] Para 3.3

relates to the location of the surveillance activity rather than the nature of the information obtained.

46. 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)[2].

47. 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.

48. 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

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

10.8

<u>Online covert surveillance</u>

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

'The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need

[2] Para 3.23 – 3.26

for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

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

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

Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to

communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

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

WHAT IS COVERT HUMAN INTELLIGENCE?

51. 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.

52. 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

53. 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

54. 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 her absence) the person acting as Head of Paid Service.

55. 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.

56. The *Regulation of Investigatory Powers (Juvenile) Order 2018 SI 715* 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.

57. Authorisations for the use of juvenile source cease after 4 months instead of 12 months.

58. 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 above.

Members of the public as informants

59. 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

60. There must at all times be arrangements in place for the proper oversight and management of CHIS, including appointing individual officers to act as 'controller' and 'handler' for each CHIS.

10.9

61. The 'handler' will have day to day responsibility for:
    - dealing with the CHIS on behalf of the Council;
    - directing the day to day activities of the CHIS;
    - recording the information supplied by the CHIS; and
    - monitoring the CHIS's security and welfare.

10.10

62. The handler of a CHIS will usually be of a rank or position below that of the Authorising Officer.

10.11

63. The 'controller' will normally be responsible for the management and supervision of the handler, and general oversight of the use of the CHIS.

64. 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.

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

66. 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.

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

AUTHORISATION

The Role of the Authorising Officer

68. **Directed Surveillance** must be authorised by an **Authorising Officer** prior to approval by the Magistrates Court. The Council's Authorising Officers are set out in the Surveillance Personnel List at Appendix A. The Service Director Legal and Democratic Services will revise the Personnel List as and when necessary.

69. An Authorising Officer may only authorise Directed Surveillance for the purpose of the prevention or detection of crime or the prevention of disorder (punishable by a

maximum term of at least 6 months' imprisonment). 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.

10.12

70. It is fundamentally important that the Authorising Officer is able to evidence that his consideration of the application is based upon the principles of necessity and proportionality. This must include why it is necessary to use covert surveillance in the investigation

71. **The use and conduct of CHIS** must also be authorised by an Authorising Officer, prior to approval by the Magistrates Court. 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;

72. 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

73. 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

74. 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.

75. 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.

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

Confidential and Legally Privileged Information

77. 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.

78. 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.

79. An authorisation or renewal for the use or conduct of a CHIS **intended** to obtain, provide access to or disclose knowledge of matters subject to legal privilege must follow an enhanced regime of prior notification and approval. Before an authorising officer grants or renews such an authorisation, they must give notice to and seek approval from a Judicial Commissioner. An application for authorisation or renewal must contain a statement that the purpose, or one of the purposes, of the authorisation is to obtain legally privileged information, and should only be sought in exceptional and compelling circumstances.

10.13

80. If a CHIS is **not intended** to acquire knowledge of matters subject to legal privilege, but it is likely that such knowledge will nevertheless be acquired, the application should contain an assessment of the degree of likelihood, how any material obtained will be treated, and how access to the material will be minimised.

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

Legal consultations

82. 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.

83. 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 Property Interference and Covert Human Intelligence Sources.

84. 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

85. 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.

86. 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

87. 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.

88. Applications for authorisation for Directed Surveillance must be made on the form **2010-09 DS Application**.

89. Applications for authorisation for CHIS must be made on the form **2010-09 CHIS Application**.

90. 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.

91. 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.

92. The current Authorising Officers are set out in the Surveillance Personnel List. The Service Director Legal and Democratic Services will revise the Personnel List as and when necessary.

93. 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.

94. Once the above authorisation process has been completed and a provisional authorisation granted, the Council must apply to the Magistrates Court for an Order approving the grant or renewal of an authorisation.

10.15

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

Duration and termination of authorisation

95. A written authorisation for **directed surveillance** will cease to have effect (unless renewed) at the end of a period of three months beginning on the day the Magistrates approval took effect.

96. 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 four months beginning on the day the Magistrates approval was given (or one month where the source is a juvenile).

97. 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 **2007-01 CHIS Cancellation**) and submit this to the Authorising Officer for signature.

98. 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 an authorisation is justified to continue as approved 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 2010-09 CHIS Review**.

99. 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 is subject again to Magistrates approval, and 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 or refusal. An application for renewal must be made using the form **2007-01 DS Renewal** or form **2007-1 CHIS Renewal.**

100. 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

101. 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.

10.16

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

103. Authorisations may be renewed more than once, provided they meet the criteria for authorisation.

104. During a review the authorising officer 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

105. Copies of all signed forms of authorisation, renewals and cancellations should be filed on the case file and the originals should be sent to the RIPA Co-ordinating Officer within 5 working days of such authorisation renewal or cancellation. Forms will be kept for 5 years following the end of an authorisation or relevant court proceedings.

106. The RIPA Co-ordinating Officer 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 operation
- the title of the investigation or operation including a brief description and the names of subjects if known

- details of attendances at Magistrates Court to include the date of attendances at court, the determining magistrate, the decision of the court and the time and date of that decision
- the dates of any reviews
- 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 or privileged information and whether any such information was obtained
- whether the authorisation was granted by an individual directly involved in the investigation
- the date the authorisation was cancelled
- Where any application is refused, the grounds for refusal as given by the Authorising Officer or determining magistrate.

10.17

107. The RIPA Co-ordinating Officer 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

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

109. 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.

110. 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 2018 and General Data Protection Regulation.

APPENDIX A

SURVEILLANCE PERSONNEL LIST

ROLE	NAME	JOB TITLE	DIRECTORATE
AUTHORISATION WHERE CONFIDENTIAL INFORMATION LIKELY TO BE ACQUIRED; USE OF JUVENILE CHIS; USE OF VULNERABLE CHIS	RACHAEL SHIMMIN	CHIEF EXECUTIVE	HEAD OF PAID SERVICE
SENIOR RESPONSIBLE OFFICER	NICK GRAHAM	SERVICE DIRECTOR LEGAL AND DEMOCRATIC SERVICES	DEPUTY CHIEF EXECUTIVE
RIPA CO-ORDINATING OFFICER	MARIA DAMIGOS	PRINCIPAL SOLICITOR	LEGAL AND DEMOCRATIC SERVICES
AUTHORISING OFFICER/DESIGNATED PERSON	CRAIG MCARDLE	CORPORATE DIRECTOR ADULTS, HEALTH AND HOUSING	ADULTS,HEALTH AND HOUSING
AUTHORISING OFFICER/DESIGNATED PERSON	RICHARD BARKER	CORPORATE DIRECTOR COMMUNITIES	COMMUNITIES

APPENDIX B

FLOWCHART 1: DIRECTED SURVEILLANCE

Requesting Officer ('The Applicant') must:

- Read the Council's Policy
- Determine that directed surveillance is required
- Assess whether authorisation will be in accordance with the law
- Assess whether authorisation is necessary under RIPA and whether it could be done overtly
- Consider whether surveillance will be proportionate
- If authorisation is approved – review or renew regularly with Authorising Officer

↓

If authorisation is necessary and proportionate, prepare and submit Form CD1 to Authorising Officer

↓

Authorising Officer must:

- Consider whether all options have been duly considered, including the Council's Policy
- Consider whether surveillance is in accordance with the law, necessary and proportionate
- Authorise only if an overt or less intrusive option is not practicable
- Set an appropriate review date (can be up to 3 months after the authorisation date) and conduct the review.
- If authorised, apply to the Magistrates' Court for approval

↙ ↘

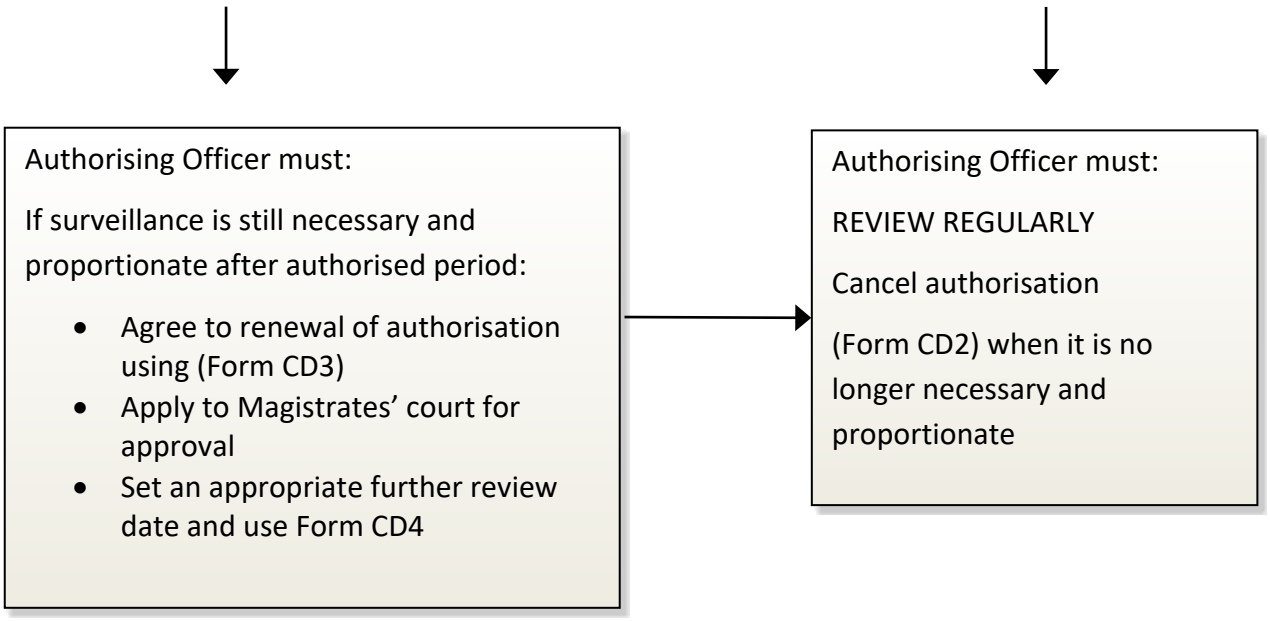
The Applicant must:

REVIEW REGULARLY

(Complete Review Form CD4) and submit to Authorising Officer on date set.

The Applicant must:

If operation is no longer necessary or proportionate, complete CANCELLATION FORM CD2 and submit to Authorising Officer


Authorising Officer must:
If surveillance is still necessary and proportionate after authorised period:
Agree to renewal of authorisation using (Form CD3)
Apply to Magistrates' court for approval
Set an appropriate further review date and use Form CD4
Authorising Officer must:
REVIEW REGULARLY
Cancel authorisation
(Form CD2) when it is no longer necessary and proportionate

FLOWCHART 2: CHIS

Requesting Officer ('The Applicant') must:

- Read the Council's Policy
- Determine that CHIS is required
- Assess whether authorisation will be in accordance with the law
- Assess whether authorisation is necessary under RIPA and whether it could be done overtly
- Consider whether surveillance will be proportionate
- If authorisation is approved – review or renew regularly with Authorising Officer

↓

If authorisation is necessary and proportionate, prepare and submit Form CD5 to the Authorising Officer

↓

Authorising Officer must:

- Consider whether all options have been duly considered, including the Council's Policy
- Consider whether CHIS is in accordance with the law, necessary and proportionate
- Authorise only if an overt or less intrusive option is not practicable
- Set an appropriate review date (can be up to 3 months after the authorisation date) and conduct the review.
- Consider the safety and welfare of the source – see Appendix C
- If authorised, apply to the Magistrates' Court for approval

↙ ↘

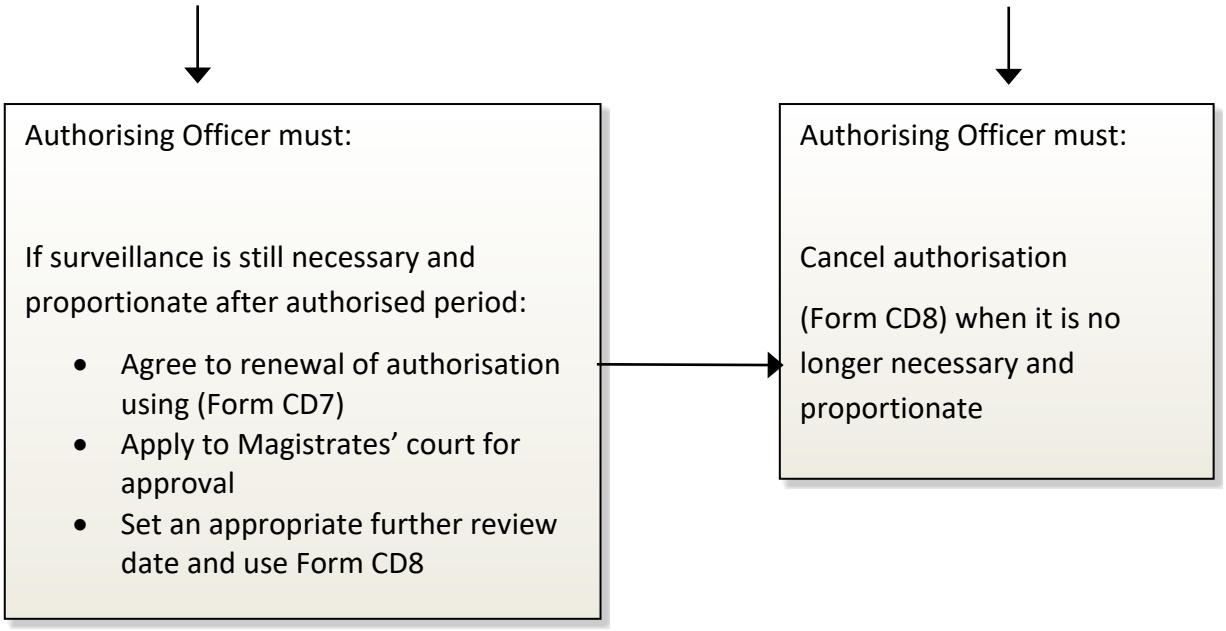
The Applicant must:

REVIEW REGULARLY

(Complete Review Form CD8) and submit to Authorising Officer on date set.

The Applicant must:

If operation is no longer necessary or proportionate, complete CANCELLATION FORM CD8 and submit to Authorising Officer


Authorising Officer must:
If surveillance is still necessary and proportionate after authorised period:
• Agree to renewal of authorisation using (Form CD7)
• Apply to Magistrates' court for approval
• Set an appropriate further review date and use Form CD8
Authorising Officer must:
Cancel authorisation
(Form CD8) when it is no longer necessary and proportionate

APPENDIX C

ADDITIONAL NOTES ON CHIS (FROM HOME OFFICE CODE OF PRACTICE)

Management of sources

Tasking

Tasking is the assignment given to the CHIS by the persons defined at sections 29(5)(a) and (b) of the 2000 Act, asking him to obtain, provide access to or disclose information. Authorisation for the use or conduct of a CHIS will be appropriate prior to any tasking where such tasking involves the CHIS establishing or maintaining a personal or other relationship for a covert purpose.

Authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task. If there is a step change in the nature of the task that significantly alters the entire deployment, then a new authorisation may need to be sought. If in doubt, advice should be sought from the Investigatory Powers Commissioner.

It is difficult to predict exactly what might occur each time a meeting with a CHIS takes place, or the CHIS 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 reviewed and updated (for minor amendments only) or it should be cancelled and a new authorisation should be obtained before any further such action is carried out.

Similarly, where it is intended to task a CHIS in a significantly greater or different 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 the existing authorisation is sufficient or needs to be replaced. This should be done in advance of any tasking and the details of such referrals must be recorded. Efforts should be made to minimise the number of authorisations per CHIS to the minimum necessary in order to avoid generating excessive paperwork.

Security and welfare

Any public authority deploying a CHIS should take into account the safety and welfare of that CHIS when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that tasking. Before authorising the use or conduct of a CHIS, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. This should consider the risks relating to the specific tasking and circumstances of each authorisation separately, and should be updated to reflect developments during the course of the deployment, as well as after the deployment if contact is maintained. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset and reviewed throughout the period of authorised activity by that CHIS. Consideration should also be given to the management of any requirement to disclose information which could risk revealing the existence or identity of a CHIS. For example this could be by means of disclosure to a court or tribunal, or any other circumstances where disclosure of information may be required, and strategies for minimising the risks to the CHIS or others should be put in place. Additional guidance about protecting the identity of the CHIS is provided at paragraphs 8.22 to 8.25 of the Home Office CHIS guidance.

The CHIS handler is responsible for bringing to the attention of the CHIS controller any concerns about the personal circumstances of the CHIS, insofar as they might affect:

- the validity of the risk assessment;
- the conduct of the CHIS; and
- the safety and welfare of the CHIS.

Where 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 D1: Directed Surveillance Application

Form D2: Directed Surveillance Cancellation

Form D3: Directed Surveillance Renewal

Form D4: Directed Surveillance Review

Form D5: CHIS Application

Form D6: CHIS Cancellation

Form D7: CHIS Renewal

Form D8: CHIS Review

APPENDIX E

GUIDANCE ON ACCESSING COMMUNICATIONS DATA

Any application for communications data (the who, when and where of a communication) must be completed on the CycComms data workflow system on the National Anti-fraud Network website at www.nafn.gov.uk. CycComms is an automated process which will enable you to apply for information, receive responses and manage your application. The National Anti-fraud Network SPoC, will act as a gatekeeper for your application, ensuring that it is practical and lawful and will engage with you to proactively provide advice, support and the most appropriate route which may require judicial approval. If it meets the legal threshold for obtaining communications data NAFN will post it on the website for approval by the appropriate Designated Person.

This procedure necessitates the applicant to be registered with the National Anti-fraud Network prior to making the application. For details on how to do this the applicant should visit www.nafn.gov.uk.

If rejected, by the Designated Person, NAFN will retain the application and inform the applicant in writing of the reason(s) for its rejection.

Comprehensive guidance on the application process is also available via the National Anti-fraud Network website at www.nafn.gov.uk.

APPENDIX F

APPLICATION FOR JUDICIAL APPROVAL FOR AUTHORISATION TO OBTAIN OR DISCLOSE COMMUNICATIONS DATA, TO USE A COVERT HUMAN INTELLIGENCE SOURCE OR TO CONDUCT DIRECTED SURVEILLANCE. REGULATION OF INVESTIGATORY POWERS ACT 2000 SECTIONS 23A, 23B, 32A, 32B.

Local authority: Buckinghamshire Council

Local authority
department:…….

Offence under investigation:……..

Address of premises or identity of subject:……
……
……

Covert technique requested: (tick one and specify details)

Directed Surveillance	
Communications Data	
Covert Human Intelligence Source	

Summary of details
……
……
……
……
……
……

……
……

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating
Officer:……

Authorising Officer/Designated
Person:……

Officer appearing before
JP:……..

Address of applicant
department……...
……
…….

Contact telephone number:……

Contact email address (optional)……

Local authority reference:……

Number of pages……..

Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Magistrates' court……

Having considered the application, I (tick one):

	am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied and I therefore approve the grant or renewal of the authorisation/notice.
	refuse to approve the grant or renewal of the authorisation/notice.
	refuse to approve the grant and quash the authorisation/notice.

Notes……
…….

……
……
……
……
……
……
……
……

Reasons……
……

……
……
……
……
……

Signed:……..

Date:……..

Time:……..

Full name:……..

Address of magistrates' court:……