Policy & Guidance on Lawful Surveillance
Regulation of Investigatory Powers Act 2000

March 2018

Review and Amendment

Review Period: **Annual**

Responsible Officer: **Chief Legal Officer**

Date	Review or Amendment	Review Comments/ Summary of Amendment	Review/Amendment Made by
18/10/2017	Amendment	Various amendments made in response to OSC/IPCO Inspection Report	Simon Young
16/3/2018	Amendment	Various amendments in response to annual review	A Healy

Epsom & Ewell Borough Council
Town Hall
The Parade
Epsom, Surrey
KT18 5BY

Version 2.2
[March 2018 Final version]

CONTENTS

List of Appendices

A. INTRODUCTION

1. In September 2000, the Regulation of Investigatory Powers Act 2000 ("RIPA") came into force in England and Wales. The Act sets out in detail the type of surveillance work, and certain other investigatory work, the Council may lawfully undertake and the circumstances in which it may be undertaken. The Act provides a regulatory framework with which the Council must comply. In simple terms, the Act requires the Council to have procedures in place, which ensure that surveillance, and/or other regulated activities are: necessary, on specified grounds; proportionate to what is sought to be achieved; and are properly authorised.

2. The Council takes its statutory responsibilities seriously and will, at all times, act in accordance with the law and take necessary and proportionate action in these matters. The Council has various powers and duties in connection with the detection of crime, including environmental enforcement work, licensing and other regulatory work, and the detection of benefit fraud.

3. The Chief Legal Officer is duly authorised by the Council to keep this policy up to date and accurate and maintain a central record of authorisations for the purpose of RIPA. This policy should be read in conjunction with the codes of practice, which can be viewed at https://www.gov.uk/government/collections/ripa-codes

4. This version replaces version 2 of the Policy and Guidance documents approved in 2010. The current version of the policy and forms are those saved in O:\Common\SharedData\RIPA. If a hard copy has been printed, reference should first be made to the electronic copy of the policy, to check for any revisions. Forms should not be saved locally; the relevant form on the Home Office website should be used on each occasion. The forms are available at https://www.gov.uk/government/collections/ripa-forms--2. If the forms or website are unavailable for any reason, the forms in the above folder may be used instead.

5. **If you are in any doubt about RIPA or any related legislative provisions, please consult the Chief Legal Officer at the earliest possible opportunity.**

B. BACKGROUND

6. Article 8 of the European Convention on Human Right is enshrined in UK law by the Human Rights Act 1998. Article 8 requires the Council and any organisations working on its behalf to respect the private and family life of citizens. The European Convention made this a qualified right and not an absolute right and as such the Council may interfere in a citizens rights mentioned above if the interference is, a) in accordance with the law, b) necessary, and c) proportionate. RIPA was passed to ensure that law enforcement and other operations are consistent with the duties imposed upon public authorities by the Human Rights Act.

7. RIPA sets out a statutory mechanism for authorising certain regulated activities. It seeks to ensure that any interference with an individual's Article 8 rights is necessary and proportionate and there is a balance between the public interest and the human rights of individuals. Covert surveillance, and other regulated activities will only be undertaken where there is no reasonable and effective alternative means of achieving the desired objective. No activity shall be undertaken by the Council or its officers within the definition of intrusive surveillance.

8. Significant changes came into force pursuant to the Protection of Freedoms Act 2012, and amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010.

9. Investigatory activities are controlled by a system of authorisation, which requires a senior officer to consider the purpose for which action is to be undertaken and the arrangements for ensuring that it is undertaken in accordance with the requirements of Guidance issued by the Office of the Surveillance Commissioners. Authorisations can only be given effect once an order approving the authorisation or notice has been granted by a Justice of the Peace.

10. Any evidence gathered by activities subject to RIPA but not properly authorised may be ruled inadmissible in court, jeopardising the case and potentially rendering the Council liable to pay court costs. Such activities being undertaken without proper authorisation could also lead to a challenge and/or claim for compensation under the Human Rights Act.

11. The Council is committed to using the RIPA framework in accordance with the Guidance issued by the Office of the Surveillance Commissioners and the Codes of Practice issued by the Home Office.

Necessity

12. The Council must consider whether the information that it is thought necessary to obtain by the authorised conduct could reasonably be obtained by other overt means and why it is necessary to use covert methods in the investigation. Prior to considering the "necessity" of a particular regulated activity, it is important to consider the scope of a local authority's powers to engage in that activity. For example, there is now the crime threshold referred to in paragraph 21, which restricts the Council's ability to authorise directed surveillance.

Proportionality

13. The following should be borne in mind when assessing proportionality:

- The means should not be excessive compared to the gravity of the alleged offence
- The least intrusive covert methods should be chosen
- Collateral intrusion should be minimised
- Whether all other reasonable methods have been considered and discounted

C. SURVEILLANCE

14. Surveillance includes:

- Monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications.
- Recording any of the above in the course of authorised surveillance.
- Surveillance by or with the assistance of appropriate surveillance devices.

15. Surveillance can be overt or covert. Most surveillance carried out by the Council will be overt (open) and not hidden or secretive. Any surveillance that is undertaken where the subject is aware of it, for example, where a noisy resident has been warned that they are going to be recorded for noise, comes under the definition of overt surveillance. In many cases, officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about Council business openly.

16. Overt Surveillance does not require RIPA authorisation.

17. Covert surveillance enables public bodies to detect and prevent crime and obtain information about an individual's or organisation's activities.

18. The Home Office Code of Practice on Covert Surveillance and Property Interference states that surveillance will be covert where it is carried out in a manner calculated to ensure that the subject is unaware that it is or may be taking place.

19. RIPA regulates surveillance that is 'directed surveillance', and/or 'intrusive surveillance'. Surveillance is **"Directed surveillance"** if the following are all true:

- It is covert but not intrusive.
- It is carried out for the purposes of a specific investigation or operation
- It is likely to result in the obtaining of private information about a person

(information relating to his/her private and family life, home and correspondence and aspects of business and professional life)

- It is not conducted by way of an immediate response to events or circumstances where it would not be reasonably practicable to seek authorisation.

20. Examples of “directed surveillance” have in the past included, for example, the surveillance of individuals in respect of possible fly tipping, benefit fraud, anti-social behaviour, or planning contraventions. Since 1 November 2012, it has only been possible for directed surveillance to be authorised where the authority is investigating particular types of criminal offences. These are criminal offences, which attract a maximum custodial sentence of six months, or more, or criminal offences relating to the underage sale of alcohol or tobacco.

21. The key element of "directed surveillance" is the targeting of an individual with the likelihood of gaining private information.

22. **"Intrusive surveillance"** is defined 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.

23. Intrusive surveillance can only be carried out by the police and other law enforcement agencies. Council Officers must **not** carry out intrusive surveillance. If the surveillance may become, or if there is a risk of it becoming, intrusive the surveillance should stop and the officer should seek advice from the Chief Legal Officer. Officers need to give careful consideration to their chosen methods of surveillance and/or devices to be used to ensure that there is no unwitting intrusive surveillance.

24. **CCTV -** The provisions of RIPA or the Code of Practice do not cover the overt use of CCTV surveillance systems. Members of the public are aware that such systems are in use for their protection and to prevent crime. However, if CCTV is targeted at an individual, a RIPA situation could arise.

25. **Collateral Intrusion** – Authorising officers should take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation. Measures should be taken to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

D. CONDUCT AND USE OF A COVERT HUMAN INTELLIGENCE SOURCE

26. A Covert Human Intelligence Source (CHIS) is a person who establishes or maintains a personal or other relationship with another person for the covert purpose of:

- using such relationship to obtain information or to provide access to any information to another person, or
- covertly disclosing information obtained by the use of such a relationship or as a result of the existence of such a relationship,
- where the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of its purpose or (in the case of disclosure of information) it is disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the disclosure in question.

27. A CHIS may be an undercover officer or controlled informant. An informant can be considered to be “controlled” where a Council officer is directing the informant’s activities or enquiries.

28. **Other types of informants** – RIPA does not apply to members of the public who volunteer information as part of their civic duties, or members of staff who report information in accordance with their contract of employment, or under the Council's Whistleblowing Policy.

29. The Council is involved in many of the everyday functions of law enforcement. For example, Enforcement Officers might use an informer (CHIS) as part of their enforcement function. The Council's Internal Auditors might use an informer to see if there is an abuse of someone's official position, (e.g. stealing money).

30. The Council can only use a CHIS if RIPA procedures are followed. The conduct or use of a CHIS requires **prior authorisation.** All authorised officers should consult the Chief Legal Officer for further information regarding procedure prior to authorising a CHIS. It will be important for an authorising officer to follow the requirements of Section 29 of RIPA. So, for example, the authorising officers' needs to be satisfied that there will be a Handler for the CHIS – with day-to-day responsibility for the dealing with the CHIS, and for the CHIS' welfare and security; there also needs to be a separate Controller, with general oversight of the use made of the CHIS.

31. "Test Purchasing" usually involves a council officer or other volunteer, who attempts to buy a product or use a service, where the seller/provider is not authorised in the circumstances to sell the product or provide the service. Most usually, this is organised/undertaken by licensing officers. This will not normally require authorisation, as no relationship is established between the test purchaser and the "target" of the operation. However, this will be fact sensitive. It is recommended that a summary of the proposed operation is written down and a judgment taken and recorded as to whether authorisation is required. This should be sent to the Chief Legal Officer.

32. The Regulation of Investigatory Powers (Source Records) Regulations 2000 contain mandatory arrangements for using a CHIS. Adequate arrangements

must be in place to ensure that records are kept which relate to the source and that these records contain particulars of certain matters. The particulars are listed below:

- The identity of the source
- The identity, where known, used by the source
- Any relevant investigating authority other than the authority maintaining the records
- The means by which the source is referred to within each relevant investigating authority
- Any other significant information connected with the security and welfare of the source
- Any confirmation made by a person granting or renewing an authorisation that the information above has been considered and that any identified risks have been explained to and understood by the source
- The date when, and the circumstances in which, the source was recruited
- The identities of the persons who, in relation to the source, are discharging or have discharged the functions
- The periods during which those persons have discharged those responsibilities
- The tasks given to the source and the demands made of him in relation to his activities as a source
- All contacts or communications between the source and a person acting on behalf of any relevant investigating authority
- The information obtained by each relevant investigating authority by the conduct or use of the source
- Any dissemination by that authority of information obtained in that way, and
- In the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating

authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

E CONFIDENTIAL INFORMATION, VULNERABLE PERSONS AND JUVENILES

33. There are special safeguards which apply when either:

    a. Knowledge of confidential information is likely to be acquired;

    b. When a vulnerable individual is used as a source;

    c. When a juvenile, being a person under the age of 18, is used as a source.

34. In all three instances at a), b) and c) above only the Chief Executive or in her absence the person acting as Chief Executive can grant authorisation, save that in no circumstances can a juvenile under the age of 16 be authorised to give information that can be used against his or her parents.

35. Confidential information consists of matters subject to legal privilege, confidential personal information, communications between a Member of Parliament and another person or confidential journalistic material. This is further particularised in the revised Code of Practice.

36. A vulnerable person is a person in need of community care services because of illness, age, mental or other disability, or, is unable to take care of himself or herself, or is unable to protect himself or herself against significant exploitation or harm.

F. EXAMPLES OF DIFFERENT TYPES OF SURVEILLANCE

Type of surveillance	Examples
Overt Not requiring prior	• Police Officer or Wardens on patrol; • Signposted Town Centre CCTV cameras (in normal use);

Type of surveillance	Examples
authorisation	• Recording noise from outside the premises after the occupier has been warned that this will occur if the noise persists (in most cases).
Covert But not requiring prior authorisation	• CCTV cameras providing general traffic, crime or public safety information.
Directed **Must be RIPA authorised**	• Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit or on long-term sick leave. • Test purchasers where the officer has a hidden camera or other recording device to record information which might include information about the private life of a shop-owner, e.g. where s/he is suspected of running a business in an unlawful manner. • Can only be used for offences, which meet the crime threshold.
Intrusive Council Officers cannot do this	• Planting a listening or other device (bug) in a person's home or in their private vehicle.

G. ANTI-SOCIAL BEHAVIOUR (ASB) ACTIVITIES (e.g. noise, violence, etc.)

37. Persons who complain about ASB and are asked to keep a diary will not normally be Covert Human Intelligence Source and therefore do not require authorisation as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. decibel) will not normally capture private information and does not require authorisation. However, careful consideration should be given to how this is to be done in practice, as it is possible that conduct requiring authorisation might be undertaken.

38. Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it may be possible to record if the noisemaker is warned that this will occur if the level of noise continues. However, this will depend on how this is to be done,

including the technical capabilities of the equipment used. Placing a stationary or mobile video camera outside a building to record ASB on residential estates will require prior authorisation.

H. INTERCEPTION OF COMMUNICATIONS

39. Local authorities cannot generally intercept communications. Under Part I of RIPA, employers can intercept e-mails with employees consent. However, consent is not needed where the purpose is to detect and prevent crime OR unauthorised use of the e-mail or internet system. The employer must make "all reasonable efforts" to inform the employee that their e-mails may be intercepted. The Council cannot otherwise seek to intercept communications.

I. ACQUISITION OF COMMUNICATIONS DATA

40. Under Part I, Chapter II of RIPA, local authorities have powers in respect of the acquisition of communications data from telecommunications and postal companies. Communications data means any traffic or any information that is sent by telecommunications system or postal system, together with information about the use of the system by any person. For example, this could include the dates and times messages are sent or calls made, but not the content of the messages.

41. An authorised person can authorise another officer within the public authority to collect the data. The local authority is allowed to collect data communications itself, i.e. if a private telecommunications company is technically unable to collect the data, the local authority would be able to collect the communications data itself.

42. In order to compel a Communications Company to obtain and/or disclose communications data in their possession, a Notice must be issued (Appendix 2). The *only* grounds a local authority can compel this is for the purposes of "preventing or detecting crime or of preventing disorder".

43. In issuing a Notice, the authorising officer can authorise another person to

liaise with the Communications Company covered by the Notice.

44. Whilst RIPA allows local authorities in appropriate circumstances to acquire communications data, this is not something Epsom & Ewell Borough Council can directly do at present, as we have no appropriately trained and accredited officers.

J SOCIAL MEDIA AND WEBSITES

45. Although Social Media and other websites are easily accessible and a great deal of information may be published, if that information is going to be sought out and used as part of an investigation, consideration must be given to whether authorisation under RIPA should be obtained. A guidance note is included at Appendix 3.

46. Care must be taken to understand how the particular site/service works. Officers should not assume that one site or service provider will work in much the same way as any other. Individuals have a large measure of responsibility to set privacy settings to protect against unsolicited access to their private information on social media or the internet generally. Unprotected data may be considered published and no longer fully under the control of the originator. An author has a reasonable expectation of privacy, especially where access controls have been applied. Where privacy settings are available but have not been used, authorisation is not usually required to access and use that data in an investigation. Regard will of course need to be had to whether that information can be directly tied to a particular individual.

47. In certain circumstances, however, authorisation might be required. Following an individual's activities on social media could stray into covert surveillance. Any proposal to ask to become a "friend" or to otherwise connect with an individual could constitute use of a CHIS. One-off test purchasing over the internet where no ongoing relationship is established will not normally require a CHIS authorisation.

48. Social media could be a valuable source of information. Prior to undertaking research, legal advice must be sought, and the investigating officer should document their decision, if they conclude in light of that advice, that no authorisation is required. Records of activities should be kept, and officers should regularly review whether authorisation is required. If required, authorisations will be granted and administered in the normal way.

49. Officers must not create covert online identities, for the purposes of research or investigation without first seeking legal advice. This activity is generally to be discouraged. If such activities are, in exceptional circumstances, considered to be necessary, this will require the approval of the Chief Legal Officer and/or the Chief Executive, before any RIPA authorisation is considered by an authorising officer. The approved arrangements must include details of controls in place, including a register of such identities and details of which officers have access to those identities. A record must be kept of all activities using a covert identity.

K. NON-RIPA SURVEILLANCE

50. RIPA does not of itself grant powers to carry out surveillance; such powers are either available under specific legislation, or ancillary to other functions. RIPA provides a framework for ensuring that surveillance that is undertaken is authorised and supervised in a manner that ensures compliance with the Human Rights Act 1998. Equally, RIPA does not prevent surveillance from being carried out or require that it may only be carried out in accordance with RIPA.

51. There may, exceptionally, be times when it will be necessary to undertake covert surveillance or use a CHIS otherwise in accordance with RIPA. For example, there may be a serious internal investigation. If this might lead to criminal proceedings, then a RIPA authorisation may be appropriate, but if criminal proceedings are not contemplated, this might not be possible.

52. There may be serious cases of anti-social behaviour or nuisance for which the penalties would be below the threshold for a RIPA authorisation. Nonetheless, there may be good reasons why covert directed surveillance, or the use of a CHIS is necessary, in order effectively to deal with the matter, especially if it might be the only effective means of efficiently obtaining the information necessary in order for action to be taken.

53. In such circumstances it is recommended that the same procedures are followed, as if it were a RIPA authorisation – the forms should be clearly endorsed "NON-RIPA APPLICATION" on the top of each page. An application should be submitted for the consideration of an Authorising Officer in the usual way, who should consider it under the necessity and proportionality tests. The normal procedure of timescales, review and cancellations should also be followed.

54. The authorisation, review, renewal and cancellation of non-RIPA surveillance/CHIS activity must be notified to the Chief Legal Officer. Authorisations will not require Magistrates' Court approval and will take effect when authorised. Records will be kept alongside the RIPA central record.

L. PROCEDURES

55. The overall rules and procedures that need to be followed are set out below. A quick RIPA checklist is included at Appendix 4.

Authorisation

56. An authorisation under Part II of the Act will provide lawful authority for a public authority to carry out surveillance. Public authorities are strongly recommended to seek an authorisation where the surveillance is likely to interfere with a person's Article 8 right to privacy by obtaining private information about that person. There is a great likelihood of risk if you are carrying out observations around a person's home. The Chief Legal Officer who is the Monitoring Officer for RIPA is authorised by the Council to oversee

all RIPA use/processes within the Council and maintain the Central Record of Authorisations for the purpose of RIPA. The Monitoring Officer will receive and retain originals of all RIPA applications, authorisations, renewals, reviews and cancellations, and to maintain these in a central file. The list of authorised officers is attached as Appendix 1. If the Chief Operating Officer or Head of Service wishes to add, delete or substitute a post s/he must make a formal request to the Chief Legal Officer for consideration. The Monitoring Officer will oversee the RIPA process on behalf of the Council.

57. Private information is a broad term and can include aspects of private life such as gender identification, name, sexual orientation and sexual life. It can also cover interaction with others in the outside world (and not restricted to private premises), and may include activities of a professional or business nature (*Perry v United Kingdom*).

58. Ideally the Authorising Officer should not be responsible for authorising a CHIS in connection with their own activities, i.e. those operations or investigations in which they are directly involved or for which they have direct responsibility. If this is unavoidable, it should be highlighted in the central record.

59. All surveillance covered by the Act must be authorised using the corporate application forms, listed in Appendix 2. To ensure that the latest version of the relevant form is being used, officers must use a blank template on each occasion, and must not type over the top of a previously saved form.

60. Surveillance equipment will only be installed with the authorisation of the Council's authorised officers. If a resident is requested to keep a video diary as part of an evidence gathering exercise, this will be regarded as directed surveillance on behalf of the Council, and as such will require authorisation.

61. Directed surveillance or the conduct and use of CHIS can *only* be authorised by the Council on the ground of the prevention or detection of crime/disorder.

62. It is important that careful consideration be given to the issue of confidential information. It should be possible in most cases to ensure that it is not likely that confidential information will be acquired. In any case in which this is considered likely, advice should be sought prior to submission of an application to the Chief Executive for authorisation.

How is the application for authorisation made?

63. It should be made in writing, and it should specify:

- The details of the purpose for which the CHIS/surveillance will be used,
- The identities, where known, of those to be subject of the use or conduct of the CHIS/surveillance,
- Details of what the CHIS will be asked to do,
- An account of the investigation or operation,
- The ground on which the authorisation is sought (i.e. for the prevention or detection of crime/disorder),
- Why the use of CHIS/surveillance is considered to be proportionate to what it seeks to achieve.
- An explanation of the information which the Council desires to obtain as a result of the authorisation,
- Details of the level of authority required,
- The potential for collateral intrusion, that is to say, interference with the privacy of other persons other than the subjects of the investigation, and an assessment of the risk of such intrusion or interference,
- The likelihood of acquiring any confidential material and what that material might be,
- Where authorisation is sought urgently, reasons why the case is considered to be urgent.

64. In assessing an application form the Authorising Officer must:

- Be mindful of the corporate policy,
- Satisfy himself that**:**
    - The use of covert means is proportionate to the mischief being investigated and the degree of intrusion on the target and others;
    - the RIPA authorisation is in accordance with the law, and the proposed activity is necessary and proportionate, and
    - Whether other means show covert surveillance could be used,
- In assessing proportionality and necessity, consider whether other less intrusive means could be used to gather information,
- Consider the degree of intrusion for those likely to be affected, bearing in mind Article 8 of the Human Rights Act, including an assessment of the risk of any collateral intrusion,
- Set a date for reviewing the authorisation, Set the date on which the authorisation will expire
- Forward **the original** authorisation to the Chief Legal Officer within 5 working days of making the authorisation, keeping a copy on their own file.

65. When authorising the conduct or use of CHIS the Authorised Officer must adhere to the Regulation of Investigatory Powers (Source Records) Regulations 2000, and:

- Be satisfied that the appropriate arrangements are in place for the management of the CHIS. This should include a risk assessment for health and safety;
- Consider the diverse impact on community confidence that may result from the information obtained;
- Ensure that records are available on a need to know basis.

66. The authorisation must be reviewed within the time stated on the application form and cancelled as soon as it is no longer necessary. The duration of the authorisation for directed surveillance can last for a maximum of 3 months from the date of authorisation and 12 months for a CHIS. However, it is essential that the authorisations are reviewed or cancelled at the proper time. There must be evidence of cancellation on file.

67. Prior to any authorisation having effect, or being renewed, judicial approval must be sought. This will be done by the investigating officer in conjunction with the Council's legal team, who will advise on the completion of the judicial application/order form and liaise with the court service.

Training and Development

68. All officers certified to sign RIPA forms shall be given the appropriate training. If the Chief Legal Officer feels that an authorised officer has not had the appropriate training/guidance then he is authorised to retract the officer's authorisation until the training has been completed.

69. RIPA Monitoring Officer shall aim to keep a Central Record of all RIPA training undertaken (to include officer name, date, provider & course title, optional comments, and copy of course materials where appropriate and available)

70. Regular refresher training of key staff shall be programmed (every 2-3 years).

71. Anyone attending training shall be encouraged to share what they have learnt with colleagues.

72. Extra training /updating will be held on at least a biennial basis – to cover legislative changes/guidance/cases etc., and follow-up on the most recent OSC inspection report or good practice.

M. MAINTENANCE OF RECORDS AND OTHER MATTERS

73. The Chief Legal Officer is responsible for:

- The integrity of the process in place within the public authority for the management of CHIS;
- Compliance with Part II of the Act and the Codes;
- Oversight of the reporting of any errors to the Commissioner and identifying both the cause(s) of errors and the implementation of processes to minimise the repetition of errors;
- Engagement with the OSC inspectors when they conduct their inspections, where applicable; and
- Where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

74. The following documents must be forwarded to the Chief Legal Officer by the Authorising Officer and retained by the Chief Legal Officer where an authorisation has been granted:

- **The original** of the forms with any supporting documentation;
- A record for the period for which the surveillance has taken place;
- The frequency of reviews as prescribed by the Authorising Officer;
- A record of the result of each review of an authorisation;
- A record of any renewal of an authorisation, the reason why the person renewing an authorisation considered it necessary to do so, and the reasons, if any, for not renewing an authorisation;
- The date and time of any instruction by the Authorising Officer;
- A record including the date and time of any oral authorisation given by the Authorising Officer, and the reason why the case was considered urgent;
- Any risk assessment made in relation to a CHIS;
- The circumstances in which tasks were given to the CHIS;

- The value of the CHIS to the investigating authority;
- The reasons for cancelling an authorisation;
- The date and time when any instruction was given by the Authorising Officer to cease using a CHIS
- A copy of the judicial application form, and original of any order obtained from the Court.

75. The Council will retain records in the Central Register for a period of at least 3 years after the end of a period of authorisation.

Central Register of Authorisations

76. This will be maintained by the Chief Legal Officer. All completed forms must be sent to the Chief Legal Officer, marked “Private and Confidential”, within 5 working days for the purpose of maintaining the Central Register.

77. If you need any further advice on RIPA, please contact the Chief Legal Officer.

Who is responsible for overseeing compliance with RIPA?

78. The Chief Surveillance Commissioner and Surveillance Commission together with the Assistant Surveillance Commissioners have been appointed to provide independent oversight of the use of the powers contained in Part II of the Act. They will inspect the Council from time to time to ensure that the Council is complying with the Act. In addition, the 2000 Act establishes an independent tribunal. The tribunal has full powers to investigate and decide any case where a person complains about the conduct of the Council in exercising its powers that are covered by the Act.

Working with Other Organisations

79. Where another agency has been instructed by the Council to undertake any action under RIPA this must be done in accordance with this policy. The Chief Operating Officer or appropriate Head of Service requesting the work must ensure that the agency is made explicitly aware of what they are authorised to do.

Involvement of Councillors

80. This policy and the Council's use of RIPA will be reviewed on at least an annual basis by the Chief Legal Officer and by the Strategy and Resources Committee at least every four years. A report on the use of RIPA will be considered by the Audit Crime & Disorder and Scrutiny Committee at least annually. Councillors will not act as authorised officers.

Acknowledgement

In producing this policy the Council has considered the Guidance of the Office of Surveillance Commissioners, the Codes of Practice. Good practice from other local authorities was considered.

.

List of Appendices

APPENDIX 1 - LIST OF AUTHORISED OFFICERS

Chief Executive – Kathryn Beldon

Chief Operating Officer - Damian Roberts (also to act as the Chief Executive's Deputy when she is absent)

Chief Legal Officer [1]– Amardip Healy

Other Authorised Officers (subject to receiving the appropriate training):

Head of Housing & Community – Rod Brown

Grants and Licensing Team Leader – Rachel Jackson

Benefits Manager – Pete Wells

[1] Will not normally grant authorisations, due to role in overseeing use of RIPA.

APPENDIX 2 – RIPA FORMS

Please see paragraph 4 of the Policy

The forms are available at https://www.gov.uk/government/collections/ripa-forms--2

List of Forms

1. Application for Authorisation to Carry Out Directed Surveillance

2. Review of a Directed Surveillance Authorisation

3. Application for Renewal of a Directed Surveillance Authorisation

4. Cancellation of a Directed Surveillance Authorisation

5. Application for Authorisation of the Use or Conduct of a Covert Human Intelligence Source

6. Review of a Covert Human Intelligence Source (CHIS) Authorisation

7. Application for Renewal of a Covert Human Intelligence Source (CHIS) Authorisation

8. Cancellation of an Authorisation for the Use or Conduct of a Covert Human Intelligence Source (CHIS)

9. [Forms relating to the Acquisition of Communications Data have been removed from the list – please speak to the Chief Legal Officer for further information]

10. Application for judicial approval for authorisation to obtain communications data, to use a covert human intelligence source or to conduct directed surveillance.

APPENDIX 3 – GUIDANCE NOTE ON COVERT SURVEILLANCE OF SOCIAL NETWORKING SITES

The purpose of this guidance note is to provide clarity on the Council's position:

1. In using social media for the gathering of evidence:

    - officers must not 'friend' individuals on social networks
    - officers should not use their own private accounts to view the social networking accounts of other individuals
    - officers viewing an individual's profile on a social networking site should do so only once in order to obtain evidence to support or refute their investigation
    - further viewing of open profiles on social networking sites to gather evidence or to monitor an individual's status, must only take place once RIPA authorisation has been granted and approved by a Magistrate
    - officers should be aware that it may not be possible to verify the accuracy of information on social networking sites and, if such information is to be used as evidence, steps must be taken to ensure its validity.

2. It is not possible to provide a definitive list of social networking sites, so this should be taken to mean any site which involves individuals creating a profile which contains personal information and is viewable by others, whether accepted as 'friends' or otherwise. This might include sites such as 'Facebook' and 'Linked-In'.

3. As the definition of 'private information' under RIPA includes: 'any information relating to a person's private or family life and 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' Sites used to advertise goods and services should be included within the definition. Although there is likely to be a reduced expectation of privacy with this type of site, there

is still the possibility of obtaining private information that may be subsequently used in any enforcement proceedings.

4. If an allegation is received or, as part of an investigation into an individual, it is necessary to view their social networking site, officers may access the main page of the individual's profile once in order to take an initial view as to whether there is any substance to the allegation or matter being investigated.

5. The initial viewing must be reasonable – for example, it would not be reasonable to spend any significant amount of time searching through various pages of the individual's profile or to print out several pages just in case they may reveal something useful.

6. In some cases where, for example, a link to a site is provided by a complainant, it may be relevant for the receiving officer to view the link before passing it onto the investigating officer to also view. This would count as one viewing. However, it would not be reasonable for each officer in a team to view the site in turn so that they may each gather some information.

7. If there is a need to monitor an individual's social networking site, authorisation must be obtained.

8. If the offence being investigated falls under RIPA, a formal RIPA application must be completed, authorised by an Authorising Officers and then approved by a Magistrate.

APPENDIX 4 – QUICK RIPA CHECKLIST

When is RIPA Authorisation required? If the answer is 'Yes' to all of the following questions:

Questions to ask	Matters to consider
Is the proposed activity 'surveillance'?	involving 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 the proposed activity and/or a surveillance device will be used.
Is it 'covert'?	carried out in a manner calculated to ensure that the target(s) will be unaware of the activity
Is it 'directed'?	for the purposes of a specific investigation/operation.
Is it likely to result in obtaining private information about this person?	information about the target /targets' private or family life is likely to be obtained.
Is it a 'foreseen/planned response'?	something other than an immediate response to events. If the proposed activity has been planned in advance, it requires authorisation if all the answers to questions 1 to 4 above have also been 'Yes'.
Is it a "core function" of the Authority?	• matters which relate to functions the Authority is required to carry out under statute (such as investigating benefit fraud, planning or food hygiene enforcement, licensing). is for the purpose of preventing or detecting criminal offences that are

Questions to ask	Matters to consider
	either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco (the crime threshold)
does it meet Home Office requirements	If the answer is 'No' to any of the above questions, the proposed activity falls outside the scope of RIPA and this policy.