

APPENDIX A

Policy on Directed Surveillance and use of Covert Human Intelligence Sources

VERSION	Version 5
DATE AGREED	October 2014
NEXT REVIEW DATE	October 2015
AGREED BY	Executive
COVERAGE	This Policy applies to service areas within Bracknell Forest Council
AUTHOR(S)	Borough Solicitor and Assistant Solicitor - Information Management and Corporate Governance

AMMENDMENT SHEET

Amendment Number	Details	Amended By	Date
Version 1	Policy 31.8.04 updated 11.12.06		
Version 2	Updated	Alex Jack – Borough Solicitor Nicola Thurloway – Assistant Solicitor	March 2010
Version 3	Updated in accordance with Revised Code of Practice	Alex Jack – Borough Solicitor Nicola Thurloway – Assistant Solicitor	April 2011
Version 4	Updated to take into account recent law including Protection of Freedoms Act and various Statutory Instruments and Home Office guidance	Alex Jack- Borough Solicitor Nicola Thoday – Assistant Solicitor	November 2012
Version 5	Updated to take account of the Inspector's Report of the 13 March 2014	Alex Jack Borough Solicitor and Anthony Igbiniyesu – Senior Solicitor	

POLICY ON DIRECTED SURVEILLANCE AND USE OF COVERT HUMAN INTELLIGENCE SOURCES

1. INTRODUCTION

- 1.1 In some circumstances it may be necessary for Council employees in the course of their duties to make observations of persons in a covert manner (i.e. carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place) or to use covert human intelligence sources. By its very nature, that sort of action is potentially intrusive and could expose the Council to a legal challenge as a potential breach of Article 8 of the European Convention of Human Rights, which establishes a “right to respect for private and family life home and correspondence”, incorporated into English Law by the Human Rights Act 1998. Also, there is a risk that if covert surveillance and covert human intelligence sources are not conducted properly the evidence obtained may be held to be inadmissible in court on the basis that it is unfair to use it as it was gathered contrary to Article 8 – right to privacy and infringes the defendants right to a fair trial as guaranteed by Article 6 – right to fair trial.

2. OBJECTIVE

The objective of this policy is to ensure that all covert surveillance carried out by Council employees including any involving covert human intelligence sources is carried out in accordance with the law.

Indeed RIPA recognises the Council’s right to infringe an individual’s right to privacy where any covert surveillance can be shown to be both necessary and proportionate and where it has been authorised by an appropriately designated officer within the organisation. Thus it is important to note that the requirements of RIPA provide protection for both the Council and the individual officers involved and should not be viewed as a mere exercise in bureaucracy

When carrying out such surveillance or using such sources officers should also bear in mind the **Codes of Practice** on Covert Surveillance and the Code of Practice on Human Intelligence Sources issued by the Home Office.

3. **SCOPE AND DEFINITIONS**

- 3.1 This policy applies in all cases where “directed surveillance” is being planned or carried out and “covert human intelligence sources” are used or planned to be used.
- 3.2 Directed surveillance is defined as surveillance which is covert, but not “intrusive” and undertaken:
- for the purposes of a specific investigation or specific operation
 - in such a manner as is likely to result in the obtaining of private information about a person (whether or not the person is specifically identified for the purposes of the investigation or operation).
- 3.3 Directed surveillance does not include surveillance which is an immediate response to events or circumstances where it is not reasonably practicable to obtain an authorisation as set out in this Policy.
- 3.4 Directed surveillance does not include intrusive surveillance. Surveillance becomes intrusive if the covert surveillance is carried out in relation to anything taking place on any residential premises or in a private vehicle and involves the presence of an individual or surveillance device on the premises or in the vehicle. The Council does not have the power or ability to authorise intrusive surveillance.
- 3.4 To fall within the meaning “use of a covert human intelligence source” there must:-
- be a source, and
 - the use of that source must be covert

A person is a “source” if they establish or maintain a personal or other relationship with someone else for the covert purpose of:-

- using the relationship to obtain information or to provide access to any information to another person, or
- covertly disclosing information obtained by the use of or as a consequence of the existence of such a relationship

In everyday language a “source” is an informant or officer working undercover. The other party to the relationship with the source must be unaware of the use or disclosure of information obtained as a result of the relationship.

4. **NEED FOR AUTHORISATION AND JUDICIAL APPROVAL**

- 4.1 Whenever it is proposed to conduct directed surveillance or to use a covert human intelligence source an authorisation should be sought under Part II of the Regulation of Investigatory Powers Act 2000. The authorisation does not take effect until such time (if any) as the Magistrate has made an order approving it

5. **GENERAL RULES OF AUTHORISATIONS**

5.1 Necessity and Proportionality

An authorisation should not be granted unless the directed surveillance/use of covert human intelligence source is both necessary and proportionate.

In terms of **necessity**, the directed surveillance/use of covert human intelligence source must be considered to be necessary to the operation on the following ground:-

- for the purpose of preventing or detecting conduct which constitutes one or more criminal offences

AND

- the offence is punishable by a maximum term of at least 6 months of imprisonment

Or

- is an offence under ;

section 146 of the Licensing Act 2003 (sale of alcohol to children)

section 147 of the Licensing Act 2003 (allowing sale of alcohol to children);

section 7 of the Children and Young Persons Act 1933 (sale of tobacco to persons under eighteen)

Even if the proposed activity is considered to be necessary, the person considering the application for authorisation must consider whether the activities are also **proportionate**.

The following elements of **proportionality** should therefore be considered;

- Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- Evidencing, as far as reasonably practicable, what other methods have been considered and why they were not implemented.

The proposed activity will not be proportionate if:-

- the intrusiveness is excessive in relation to the value of the information to be obtained, or
- the information sought could be obtained by less intrusive means

Where an individual is suspected of claiming a false address in order to abuse a school admission system operated by the Council it is likely that a RIPA Authorisation is not necessary as

less intrusive and overt means could be explored to obtain the information required.

The Authorising Officer should consider the issue of proportionality with particular care in relation to relatively minor offences, instead, other less intrusive methods such as general overt observation of the location should be used. In rare instances where such offences are especially problematic or occurring with particular frequency and the problem cannot be resolved by overt measures, RIPA authorisations may be considered appropriate but care should be taken to ensure that the amount of private information obtained is kept to the minimum necessary".

5.2 Collateral Intrusion

“Collateral intrusion” means intrusion into the privacy of persons other than those who are the subject of the investigation. Measures should be taken to minimise both the risk of such intrusion and the extent of such intrusion. An application for authorisation should consider the risk of such intrusion and the Authorising Officer must take such risk into account in reaching a judgment as to whether or not the proposed directed surveillance/use of covert human intelligence source is proportionate. If the investigation unexpectedly interferes with the privacy of persons who are not covered by the authorisation, the Authorised Officer should be informed.

5.3 Management of Covert Human Intelligence Sources

An Authorising Officers should not grant an authorisation for use of a covert human intelligence source unless he/she is satisfied of the following:-

- (a) that at all times there will be an officer who will have day-to-day responsibility for dealing with the source on behalf of the Council and for the source’s security and welfare
- (b) that at all times there will be another officer (senior to the officer having responsibility under (a) above) who will have general oversight of the use made of the source

- (c) that at all times there will be an officer responsible for maintaining a record of the use made of the source, and
- (d) that records maintained by the Council that disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons

5.4 The safety and welfare of the source and foreseeable consequences to others should be taken into account in deciding whether or not to grant an authorisation. A risk assessment determining the risk to the source in acting as a source of information to the Council, and in particular identifying and assessing the risks should the identity of the source become known, should be carried out. The welfare and security of the source after the operation has ceased should be considered at the outset. The officer having responsibility under 5.3(a) above (i.e. the officer with day-to-day responsibility for the source) should report to the officer having general oversight any concerns about the personal circumstances of the source, insofar as they might affect.

- the validity of the risk assessment
- the conduct of the source, and
- the safety and welfare of the source

If appropriate such concerns should be reported to the Authorising Officer who will need to determine whether or not to allow the authorisation to continue.

6. WHO CAN GRANT AN AUTHORISATION?

- 6.1 Subject to 6.4 below, the law permits authorisations for directed surveillance and use of covert human intelligence sources to be granted by officers of at least Service Manager status.
- 6.2 A list of those Officers designated as Authorising Officers is shown as **Annex A** to this document. Once an application has

been granted by the Authorising Officer, the authorisation then requires judicial approval before it can take effect.

- 6.3 Authorising Officers should not normally authorise investigations in which they are directly involved.
- 6.4 In the following instances an authorisation may only be granted by the Chief Executive, and in his absence, by any of the authorising Directors for RIPA surveillance involving the:-
 - (a) use of a juvenile Covert Human Intelligence Source (CHIS).
 - (b) surveillance involving the potential acquisition of confidential information. Confidential information means information which is; legally privileged information, confidential personal information or confidential journalistic material.
- 6.5 An Authorising Officer will receive training and is not able to authorise before then. Thereafter, each Authorising Officer shall receive further training/refresher training on at least a biennial basis.
- 6.6 The Senior Responsible Officer for RIPA, as recommended in the revised Code of Practice, is the Director of Corporate Services

7. THE PROCESS OF OBTAINING AN AUTHORISATION

- 7.1 The Investigating Officer seeking an authorisation should apply through their own line management structure unless it is impracticable in the circumstances (e.g. because no Director or Assistant Director in the relevant department is available).
- 7.2 An application for authorisation for directed surveillance or use of covert human intelligence sources should be made in the appropriate standard form which is available via the Home Office website at

<http://www.homeoffice.gov.uk/counter-terrorisim/regulation-investigatory-powers/ripa-forms>

- 7.3 Both the Investigating Officer seeking the authorisation and the Authorising Officer shall have regard to any guidance notes issued by the Home Office and the Legal Section on the use of those forms.
- 7.4 The Authorising Officer shall return the completed Form to the Investigating Officer. The Investigating Officer will use the Judicial Application /Order form at Annex B of the Home Office Guidance, seek judicial approval via a Magistrate in order for the application to take effect.

<http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/local-authority-england-wales?view=Binary>

- 7.5 The authorisation does not take effect until such a time (if any) as the Magistrate has made an order approving it.
- 7.6 In each case, the role of the Magistrates is to ensure that the correct procedures have been followed and the relevant factors have been taken account of. If the Magistrate refuses to approve an authorisation, the authorisation is quashed.
- 7.7 A copy of the Form and record of the Magistrate's decision (on the Judicial Application/ Order Form at Annex B of the Home office Guidance) will be provided to the RIPA Monitoring Officer after the hearing for it to be added to the Central Record.
- 7.8 The Borough Solicitor has already designated (under section 223 of the Local Government Act 1972) certain Investigating Officers to present RIPA applications in the Magistrates Court.

8. DURATION OF AUTHORISATION

- 8.1 In the case of directed surveillance, written authorisations cease to have effect after three months (unless renewed). In the case of covert human intelligence sources an authorisation expires after one month if the source is a child and one year if the source is an adult.

9. REVIEW OF AUTHORISATION

- 9.1 Once granted an authorisation should be reviewed regularly to assess whether or not the investigation continues to be necessary and proportionate. The date of review is event driven, for example a test purchasing application should be reviewed after the date of the test purchase.

The Authorising Officer should specify how often a review should take place and use the appropriate form from the Home Office (see 7.3 above) to conduct a review (i.e. a review of the use of directed surveillance or reviewing the use of covert human intelligence source.) This information will be held on the Central Record.

10 RENEWAL OF AUTHORISATION.

- 10.1 Judicial approval is required if an authorisation is being renewed. An application for renewal of authorisation should not be made until shortly before the authorisation is due to expire. An authorisation may be renewed more than once for at least three months in the case of directed surveillance or, in the case of covert human intelligence source, one year.
- 10.2 An application for renewal should be made to the officer who granted the original authorisation unless there is very good reason not to do so (e.g. because the original authorising officer is on annual leave).

Applications for renewal should be made using the appropriate Home Office forms (i.e. renewal of directed surveillance or renewal of authorisation to use covert human intelligence source). Officers seeking an authorisation for renewal and Authorising Officers shall have regard to Code of Practice issued.

- 10.3 Once the application has been renewed by the Authorising Officer the completed Form will be provided to the Investigating Officer who will seek judicial approval (see 7.5-7.8) via Magistrate in order for the renewal to take effect. The renewal does not take effect until such time (if any) as the Magistrate has made an

order approving it. This information will be held on the Central Record.

11. CANCELLATION AND CEASING OF AUTHORISATIONS

- 11.1 The Authorising Officer who granted or last renewed the authorisation must cancel it if he/she believes that the investigation is no longer necessary or proportionate. If the original Authorising Officer is no longer available the duty falls upon the person who has taken on that role. All authorisations should be cancelled or renewed before they cease to have effect.
- 11.2 Although authorisations cease to have effect after the relevant time expires (see paragraph 8) an authorisation should be reviewed, renewed or cancelled before the expiration of the time limit.
- 11.3 As soon as a decision is taken to cease the operation an instruction must be given to those involved to stop the directed surveillance/using the covert human intelligence source. A form (see 7.2 above) recording the cancellation should be completed and forwarded to the RIPA Monitoring Officer for inclusion in the Central Record.

12 ROLE AND DUTIES OF RIPA MONITORING OFFICER

- 12.1 The Council's RIPA Monitoring Officer is the Senior Solicitor (Anthony Igbiniyesu) and has the following responsibilities:-
- Central responsibility for quality control of the RIPA process including providing comments/ advice for future applications
 - Training
 - Raising awareness of RIPA throughout the Council and
 - Management of records in accordance with paragraph 13 below.
 - Keeping the Central Record (a register of all authorisations) updated.
- 12.2 Any Authorising Officer seeking guidance in authorisations or any RIPA related matter should contact Anthony Igbiniyesu.

13. RECORDING AUTHORISATIONS/REVIEWS/RENEWALS/ CANCELLATIONS

13.1 There shall be a Central Record which shall be kept by the RIPA Monitoring Officer. The role of the Central Record is to keep a complete record of all authorisations and to monitor the quality of authorisations. There will also be a summary record maintained of all the completed forms.

13.2 A copy of the originals of forms authorising or cancelling directed surveillance or use of a covert human intelligence source should be sent by internal email to the RIPA Monitoring Officer. The RIPA Monitoring Officer shall retain all such forms for a period of not less than three years. A copy of such forms shall be retained by the relevant department for at least three years. The original forms shall be retained by the relevant department together with:-

- a record of the period over which the surveillance has taken place
- the date and time when any instruction was given by the Authorising Officer

Relevant departments must ensure that any data is processed in accordance with Data Protection legislation.

13.3 In the case of use of covert human intelligence sources, records should be maintained in such a way as to preserve the confidentiality of the source and the information provided by the source.

13.4 Records to be kept in relation to Covert Human Intelligence Sources

The following matters must be included in the records relating to each source;

- (a) the identity of the source;
- (b) the identity, where known, used by the source;

- (c) any relevant investigating authority other than the authority maintaining the records;
- (d) the means by which the source is referred to within each relevant investigating authority
- (e) any other significant information connected with the security and welfare of the source;
- (f) any confirmation made by the person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source
- (g) the date when, and the circumstances in which, the source was recruited;
- (h) the identities of the persons who, in relation to the source;
 - (i) has day to day responsibility for their security and welfare;
 - (ii) has oversight of the use made of the source
 - (iii) has responsibility for maintaining a record of the use made of the source
- (i) the periods during which those persons specified in (h) above have discharged those responsibilities;
- (j) the tasks given to the source and the demands made of him in relation to his activities as a source;
- (k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
- (l) the information obtained by each relevant investigating authority by the conduct or use of the source;

- (m) any dissemination by that authority of information obtained in that way; and
- (n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

14. CODES OF PRACTICE

14.1 Two Codes of Practice have been issued by the Secretary of State relating to Directed Surveillance and Covert Human Intelligence Sources (CHIS) respectively. These came into force on 6 April 2010. Copies of both Codes are available on the Home Office website www.homeoffice.gov.uk/ripa

15 TEST PURCHASING AUTHORISATIONS

15.1 When conducting covert test purchases operations at more than one establishment, a separate authorisation is not required for each premises although each must be identified at the outset and necessity, proportionality, and collateral intrusion addressed in relation to each of the premises.

16 CCTV

16.1 Because CCTV is usually overt (i.e. members of the public are made aware that a CCTV system is in operation) an authorisation is not normally required for the use of CCTV material. However, there may be occasions when a covert CCTV system is used for the purposes of a specific investigation or operation in which case an application for directed surveillance may be required. The advice of the RIPA Monitoring Officer should be sought in such circumstances.

16.2 In the event of a Police request for directed surveillance using CCTV cameras they will need to follow their own internal procedure for obtaining authorisation in the first instance. In such cases a copy of the relevant Police authorisation should be

obtained by the Officer receiving the request and forwarded to the RIPA Monitoring Officer to confirm its validity.

17 INTERNET /"CHAT ROOMS"/SOCIAL NETWORKS

Authorisations under RIPA are not ordinarily required for participating in open online chat or posting on a social networking website (in a business capacity). However when steps have been taken to, store, monitor or establish a relationship with a person authorisation should be sought. CHIS authorisation should be obtained if steps are to be taken to develop online relationship with other participants with the view to gathering information. The advice of the RIPA Monitoring Officer should be sought when access to a site is obtained via membership (such as face book) with a view to carrying out an investigation.

18 NON COMPLIANCE

18.1 Evidence gathered in breach of the procedures described in this document will not automatically be excluded by a Court. However the defendant may argue that reliance by the prosecution on evidence obtained in breach of Article 8 – right to privacy denies him his right to a fair trial as guaranteed by Article 6 and that the case should not proceed. In addition, the admissibility of evidence is a matter for the Courts discretion and they will decide whether the evidence is put forward in such a way that the proceedings are fair as a whole. Therefore RIPA should be complied with at all times.

18.2 Apart from the above, non-compliance with RIPA may still result in:-

- a claim against the Council for a breach of Article 6 and/or 8 of the European Convention of Human Rights
- a complaint to the Local Government Ombudsman
- referral to a RIPA Tribunal
- censure by the Office of Surveillance Commissioners

ANNEX A

RIPA Authorising Officers

- Chief Executive; Timothy Wheadon
- Director Children, Young people and Learning; Janette Karklins
- Director Environment, Culture and Communities; Vincent Paliczka
- Chief Officer Environment and Public protection; Steve Loudon
- Chief Officer Housing; Simon Hendey
- Head of Regulatory Services; Robert Sexton