South Oxfordshire District Council

Listening Learning Leading

Vale of White Horse District Council

Regulation of Investigatory Powers Act 2000

POLICY AND PROCEDURES

July 2020

1. Introduction

1.1 Article 8 of the European Convention on Human Rights confers on every individual a "right to respect for his private and family life, his home and his correspondence". The convention provides there is to be no interference with this right unless it is in accordance with the law and it is necessary on specific grounds.

1.2 As the council has a number of functions to undertake which involve the enforcement of laws and regulations, officers will need to conduct investigations and where appropriate take legal proceedings. The council will not normally make use of covert surveillance and similar activities unless it is necessary for an investigation. The council will undertake its enforcement role having regard to the Human Rights Act 1998 and also the Equality Act 2010, which requires the council, in the exercise of its functions, to have due regard to the need to eliminate discrimination, harassment and victimisation.

1.3 Any covert surveillance conducted by the council can constitute an interference with the right protected by Article 8. Section 6 of the Human Rights Act 1998 provides that it is unlawful for a public body to interfere with those rights under the European Convention on Human Rights that are incorporated into the Act.

1.4 The Regulation of Investigatory Powers Act 2000 (RIPA) is the domestic law that regulates the way law enforcement agencies, and public bodies conduct surveillance for the purposes of law enforcement. The fundamental requirement of RIPA is that when the council considers undertaking directed surveillance or using a covert human intelligence source (CHIS) it must only do so if:

a) the activity has been authorised by an officer with appropriate powers, and

b) the relevant criteria are satisfied.

1.5 Some activities of council teams (eg in the field of environmental protection, health and safety, licensing, fraud investigation and Planning enforcement) may bring into play the provisions of RIPA.

1.6 Compliance with RIPA will ensure any interference is in accordance with domestic law. Compliance with RIPA assists to defend the council and its officers against complaints of interference with the right to respect for private and family life protected by Article 8 of the Convention. The council can thus show any interference is "in accordance with the law". Provided the activities undertaken are also necessary and proportionate there will be no contravention of human rights legislation.

1.7 All investigations or enforcement actions involving covert surveillance or the use of a CHIS must comply with the provisions of RIPA.

1.8 This policy applies to all staff and agents working for the council. A key purpose of the policy is to direct council enforcement officers and their managers on the procedures that should be followed where surveillance activities are contemplated, to ensure compliance with RIPA.

1.9 A central register of RIPA authorisations will be maintained by the council's Head of Legal and Democratic, who is the council's Senior Responsible Officer for the purpose of ensuring the integrity of the council's RIPA processes under the Act, and statutory guidance issued in pursuance of the Act. Day to day maintenance of the register and advice relating to RIPA issues is undertaken under the supervision of the Senior Responsible Officer by the council's Litigation and Planning Team Leader, in the role of RIPA Coordinating Officer.

1.10 This policy and procedures document and the council's use of covert surveillance as a tool in investigations shall be reviewed at least every two years and also when circumstances warrant it.

1.11 The council will from time to time issue further guidance and procedures to staff.

2. RIPA regulated activities

2.1 If an investigating officer identifies a contemplated surveillance activity as regulated by RIPA, a written authorisation in accordance with this guidance should be obtained, before the activity commences. If enforcement officers or their managers are in any doubt, they should seek the advice of the legal services team.

Activities covered by RIPA:

2.2 THE INTERCEPTION OF COMMUNICATIONS

This covers a situation where interception of the communication has not been authorised, or agreed by the sender and addressee of the communication. These guidance notes do not cover this activity, as the council is extremely unlikely to undertake this activity. The advice of the legal services team should always be sought should such an activity be contemplated.

2.3 THE USE OF COVERT HUMAN INTELLIGENCE SOURCES

The use of a covert human intelligence source (CHIS), and his or her conduct, would require authorisation under RIPA. In practice, it is unlikely that there will be any circumstances which would require the council to either use a CHIS or operate under cover in the manner of a CHIS, and advice should be sought from the RIPA Coordinating Officer or the Senior Responsible Officer before any authorisation is applied for or granted.

A CHIS is defined as the use or conduct of an individual who establishes or maintains a personal or other relationship with a person for the covert purpose of obtaining information. These provisions would cover the use of professional witnesses to obtain evidence or information, or officers operating 'under cover'. Great caution should be exercised in these circumstances and the authorising officer must be satisfied that the authorisation is necessary, that the conduct authorised is proportionate to what is sought to be achieved and that arrangements for the overall management and control of the individual are in force.

The provisions of RIPA relating to CHIS do not apply where a situation would not normally require a relationship to be established for the covert purpose of obtaining information. For example: where members of the public volunteer information to the council as part of their

normal civic duties; or where members of the public are asked to keep diaries of incidents in relation to, say, planning enforcement, anti-social behaviour or noise nuisance.

If a CHIS is used, both the use of the CHIS and his or her conduct require prior authorisation.

Where engaged, the Home Office Code of Practice on Covert Human Intelligence Sources (2018) requires public authorities to ensure that arrangements are in place for the proper oversight and management of CHIS, including appointing individual officers as defined in the Act for each CHIS. This is known as a 'handler' and the officer will have day to day responsibility for dealing with the CHIS on behalf of the authority concerned; directing the day to day activities of the CHIS; recording the information supplied by the CHIS; and monitoring the security and welfare of the CHIS.

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

In addition to a handler, a 'controller' will also be appointed. This officer will be responsible for the management and supervision of the handler and general oversight of the use of the CHIS.

In view of the rigorous nature and importance of these requirements it is essential that CHIS activity is not undertaken by or on behalf of the council except under the strict control and supervision of officers who have been properly and recently trained for the specific purpose.

2.4 DIRECTED SURVEILLANCE

As this activity is the most likely to be carried out, this policy addresses this activity in more detail. Where there is to be directed surveillance written authorisation must be obtained in accordance with the provisions of RIPA before the surveillance commences. Directed surveillance is defined as surveillance which is covert, but not intrusive and which is undertaken for the purposes of a specific investigation, and which is likely to result in obtaining private information about a person and which is carried out otherwise than as an immediate response to events where it would be impracticable to obtain prior authorisation. Therefore, investigating officers need to consider a number of key questions to determine whether a proposed activity falls within this definition of directed surveillance:

i) Is the proposed activity surveillance?

Surveillance is defined in wide terms as: any activity involving the monitoring, observing or listening to persons, their movements, their conversations or other activities or communications; the recording of anything monitored, observed or listened to in the course of surveillance; and the surveillance by or with the assistance of a surveillance device.

ii) Is the surveillance covert?

Surveillance is covert where it is carried out in a manner calculated to ensure that the subjects of the surveillance are unaware that it is, or may be taking place. It is therefore the intention of the officer carrying out the surveillance which is relevant to this issue of covertness.

iii) **Is the surveillance for the purposes of a specific investigation?**
General observation, not forming part of any investigation into suspected breaches of the law and not directed against any specific person or persons is not directed surveillance eg CCTV cameras in council car parks are readily visible and if they are used to monitor the general activities of what is happening within the car park, it falls outside the definition. If, however, the cameras are targeting a particular known individual, the usage will become a specific operation which will require authorisation.

iv) **Is the surveillance undertaken in such a manner that is *likely* to result in the obtaining of private information about a person?**
"Private information" is any information concerning a person's private or family life. Whether information is personal in nature is relevant when deciding whether information is private. The fact that observation of individuals occurs from the public highway will not prevent the discovery of private information. When officers consider this question they should give due weight to the probability of discovering such information, as authorisation is not required if there is only a slight possibility of discovering private information.

v) **Is the surveillance otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to obtain prior authorisation?**
If the surveillance is an immediate response to something happening during the course of an officer's work, it would not be reasonable to obtain prior authority. If this occurs, the officer must report the incident back to an authorising officer so a note can be made on the relevant department file and the central register.

vi) **Is the surveillance intrusive?**
The council is *not* authorised to carry out intrusive surveillance, but in any event it is extremely unlikely that the council would contemplate undertaking this activity. Surveillance is intrusive surveillance if it is carried out covertly in relation to anything taking place on residential premises or in a private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by a surveillance device.

3. Online covert activity/Use of social media

3.1. The growth of the internet, and the extent of the information that is now available online, presents new opportunities to view or gather information which may assist in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public that the council serves. It is important that the council is able to make full and lawful use of this information for its statutory purposes. Much of it can be accessed without the need 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, a RIPA authorisation may need to be considered. The following guidance taken from the latest (August 2018) Home Office Code of Practice may assist in identifying when such authorisations may be appropriate.

3.2. 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 considered. If a person acting on behalf of the council 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 2018 provide detail on where a CHIS authorisation may be available for online activity).

3.3. 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 the council may have 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 (required).

3.4. 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.

3.5. Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, 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.

3.6. Whether there may be interference with a person's private life includes a consideration of the nature of the council's activity in relation to that information. Simple reconnaissance of such sites (ie 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 there is systematic collection and recording of information about a particular person or group, a directed surveillance authorisation should be considered.

3.7. In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is

proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or group;
- Whether it is likely to result in obtaining private information about a person or group of people;
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include personal information and therefore constitute collateral intrusion into the privacy of these third parties.

4. Authorisations

4.1 No Authorising Officer shall grant an authorisation for the carrying out of directed surveillance or the use of a CHIS unless s/he believes:

(a) that an authorisation is necessary for the purpose of preventing or detecting crime, and in the case of directed surveillance that the offence in question carries a maximum sentence of at least six months imprisonment or relates to the sale of alcohol or tobacco to persons who are underage; and

(b) the authorised activity is proportionate to what is sought to be achieved by carrying it out.

4.2 The contemplated activity must be considered necessary in the particular circumstances of the case.

4.3 Proportionality is a key concept of RIPA. An authorisation should demonstrate how an authorising officer has reached the conclusion that the surveillance activity is proportionate to what it seeks to achieve, including an explanation of the reasons why the method, tactic or technique is not disproportionate (the proverbial 'sledgehammer to crack a nut'). Proportionality is not only about balancing the effectiveness of covert methods over overt methods but of explaining why the particular covert method, tactic or technique is the least intrusive. It is insufficient to make a simple assertion or to say that the 'seriousness' of the crime justifies any or every method available. It may be unacceptable to advance lack of resources or a potential cost saving as sufficient ground to use technological solutions which can be more intrusive than a human being. This critical judgment can only properly be reached once all other aspects of authorisation have been fully considered.

4.4 A potential model authorisation would make clear that the following elements of proportionality had been fully considered:

(a) balancing the size and scope of the operation against the gravity and extent of the perceived mischief,

(b) explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others,

(c) that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result, and

(d) providing evidence of other methods and why they were not implemented.

4.5 At the point in time immediately before the completion of the application for a RIPA authorisation and before it is presented to the Authorising Officer for his/her authorisation, the application should be delivered to the RIPA Coordinating Officer. This is to assist with the completion of the central record of authorisations and to provide for an additional element of 'quality control' over the content of the application. Assuming it is granted by the Authorising Officer, the completed authorisation should also be returned to the RIPA Coordinating Officer and again assessed for quality before arrangements are made for a Magistrates Court to consider its approval (see the judicial approval section below).

5. Judicial approval of RIPA authorisations

5.1 In addition to the pre-conditions and requirements for authorisations described above, no authorisation for directed surveillance or the use of a CHIS will take effect unless and until the relevant judicial authority (ie a Magistrate) has made an order approving the grant of the authorisation. It is therefore vital that any surveillance for which authorisation has been sought does not start until such time as it has been approved by a Magistrate.

5.2 It is necessary for the council to obtain judicial approval for all initial RIPA authorisations/applications and renewals. There is no requirement for a Magistrate to consider either cancellations or internal reviews.

5.3 The need for judicial approval from a Magistrate will require the RIPA Coordinating Officer or another lawyer under his supervision to contact the administration section at the local Magistrates Court to request a hearing for this stage of the authorisation. In advance of the hearing, the Authorising Officer should provide to the court the RIPA authorisation signed by him/her and a completed judicial application/order form, together with any other relevant supporting documents. The hearing to consider the application will be held in private, and the Magistrate will consider the documentation provided, and ask questions to clarify points or gain reassurance on any matters of interest or concern. Ordinarily, the person representing the council at this hearing will be the Authorising Officer, and this person should make sure that s/he takes to the hearing evidence of his/her own authorisation to grant authorisations and represent the council in court proceedings.

6. Authorising officers

6.1 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No 521 prescribes the Authorising Officer must be at least a director, head of service, service manager or equivalent.

6.2 Under the constitution's scheme of delegation, heads of service and the Chief Executive have delegated authority to issue RIPA authorisations, however further important provisions about Authorising Officers and about training are contained in section 7 below. For a service manager to become an Authorising Officer, a written authority must be produced by the relevant head of service.

6.3 The Authorising Officer should not be part of the surveillance team. S/he cannot grant a self-authorisation, and in the event that a head of service wishes to undertake the surveillance personally, or as part of the surveillance team, any authority should be issued by a different Authorising Officer.

6.4 Authorising Officers must be aware of the requirements of RIPA and how to properly consider requests for authority. Authorising Officers must demonstrate that these requests have been properly considered when they complete the authorisation form.

6.5 Where the surveillance is likely to lead to the obtaining of "confidential information" (as defined below), a RIPA authorisation can only be given by the Chief Executive (or in his absence, his deputy). For these purposes confidential information has the following specific meaning, namely:

(a) legally privileged information eg communications between a professional legal adviser and a client

(b) confidential personal information, which is information kept in confidence and relating to a person's physical or mental health or relating to spiritual counselling given to a person eg consultations between a health professional and a patient, information from a patient's medical records or conversations between an individual and a Minister of Religion

(c) confidential journalistic information, held for the purposes of journalism on the basis that it or its source would not be revealed.

6.6 It is difficult to envisage circumstances in which the council's investigative activities would either require, justify or otherwise result in the obtaining of confidential information and if any such information is obtained during surveillance, legal advice should be sought immediately.

6.7 The codes of practice referred to in paragraph 11.1 below provide further guidance relating to confidential material.

7. Training

7.1 The council will ensure that adequate training takes place for Authorising Officers and investigating officers. Such training may be arranged and provided through officers' own professional associations or through the use of outside agencies. Sharing training with other local authorities may also be appropriate. The council's legal services team can also assist with training and by giving guidance from time to time, either generally as legislation/guidance evolves or in specific cases. As it is especially important for Authorising Officers to be able to demonstrate an up to date knowledge of RIPA and best practice, the delegation to grant authorisations should generally be exercised only by those officers who have undertaken and kept up to date RIPA training. In order to assist this process, the Council's RIPA Coordinating Officer under the general supervision of the Senior Responsible Officer for RIPA will maintain, monitor and review a central record of RIPA training attended by officers of the council along with a list of those officers who have undertaken training necessary to enable them to assess and grant authorisations. It should further be noted that advice from the Investigatory Powers Commissioner's Office (IPCO) is that officers engaged in RIPA activity and/or management should receive training appropriate to their roles at approximately 18 month intervals.

8. Forms of authorisation

8.1 RIPA itself does not contain prescribed forms of authorisation. However, the adapted Home Office model forms below should be used. This will ensure a consistent approach is adopted across service teams and ensure all relevant issues are addressed during the decision-making process. Forms relating to directed surveillance are appended. If any proposed investigation involves the interception of communications or the use of a covert human intelligence source the advice of the legal services team should be sought. The appended forms comprise:

Appendix one	Application for the use of directed surveillance
Appendix two	Renewal of directed surveillance
Appendix three	Review of the use of directed surveillance
Appendix four	Cancellation of the use of directed surveillance

9. Duration of authorisation

9.1 A written authorisation for directed surveillance lapses, if not renewed, three months from the grant or last renewal (12 months in the case of a CHIS authorisation), and this period begins at the time of magistrates approval. However, officers should ensure authorisations only last for as long as is considered necessary and proportionate. Regular reviews of authorisations should be undertaken to assess the need for continued surveillance. The Authorising Officer will specify the frequency of reviews on the authorisation form.

9.2 Any time before the authorisation would cease to have effect, the Authorising Officer may renew, in writing, if s/he still considers it necessary.

9.3 Authorisations may be renewed more than once provided they continue to meet the criteria for authorisations. The renewal does not have to be authorised by the same authorising officer who granted the original authorisation.

9.4 The Authorising Officer who granted the authorisation or last renewed the authorisation must cancel it if satisfied the directed surveillance no longer meets the criteria upon which it was authorised.

10. Retention and security of forms and records

10.1 Decisions on requests for judicial approval, authorisations, requests for authorisation, renewals, and cancellations are confidential material. The documents and any information contained therein must not be disclosed to any person who has no legitimate need to have access to the document, or to the information that it contains. Authorising Officers must ensure that there are proper arrangements within their departments or services for the retention and security of such documents in accordance with the requirements of the Data Protection Act 1998 (or relevant successor legislation).

10.2 Such documents may need to be securely kept for a period (considered appropriate by the relevant head of service) following the completion of any surveillance, as they may have to be produced in court, or to the other party in court proceedings as part of legal disclosure requirements. Superfluous copies should not be made or kept.

10.3 The council's Head of Legal and Democratic holds the role of Senior Responsible Officer with general oversight of the council's conduct of RIPA processes and maintains a secure central register of all judicial approvals, authorisations, reviews, cancellations and renewals issued. Day to day management of the register and advice on RIPA issues is undertaken by the RIPA Coordinating Officer. All officers should ensure that original signed documents are given to the RIPA Coordinating Officer (or in his absence to another lawyer in the legal services team) upon issue in order to keep this register up to date. On receipt of a document to be included within the register, a date for review will be diarised.

10.4 The central register may be "weeded" of information that is more than seven years old, unless there are relevant outstanding court proceedings. All documentation that is no longer needed to be kept should be destroyed by shredding.

11. Codes of practice

11.1 The Home Office has published a Code of Practice on Covert Surveillance and Property Interference (August 2018) and a Code of Practice on Covert Human Intelligence Sources (August 2018) which provide further guidance on the use of these activities. These codes are available on the Home Office website and should be read by investigating officers and team leaders whose investigations may involve covert surveillance.

11.2 The codes of practice are admissible as evidence in criminal and civil proceedings. The council will normally follow the requirements of codes of practice issued by the Home Secretary unless there are exceptional circumstances justifying a departure from the recommended approach.

11.3 The IPCO also produces guidance from time to time on procedures and oversight arrangements for local councils on RIPA and its website offers a further valuable reference source.

Annex

Officers of the council with designated RIPA roles

Senior Responsible Officer

Margaret Reed, Head of Legal and Democratic
margaret.reed@southandvale.gov.uk

RIPA Coordinating Officer

Litigation and Planning Team Leader

Authorising Officers

Andrew Down, Acting Deputy Chief Executive – Partnerships
andrew.down@southandvale.gov.uk

Paul Howden, Revenues and Benefits Manager
paul.howden@southandvale.gov.uk

Appendix one

APPLICATION FOR THE USE OF DIRECTED SURVEILLANCE

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000

Authorisation Directed Surveillance

Public Authority *(including full address)*			
Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person other than the applicant)			

Unique Reference Number	

DETAILS OF APPLICATION
1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521. [1]
2. Describe the purpose of the specific operation or investigation.
3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.
4. The identities, where known, of those to be subject of the directed surveillance.
• Name: • Address: • DOB: • Other information as appropriate:
5. Explain the information that it is desired to obtain as a result of the directed surveillance.

[1] For local authorities: The exact position of the authorising officer should be given. For example, Head of Trading Standards.

Unique Reference Number	

6. Identify on which grounds the directed surveillance is <u>necessary</u> under Section 28(3) of RIPA. *Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (SI 2010 No.521).*
• In the interests of national security; • For the purpose of preventing or detecting crime or of preventing disorder; • In the interests of the economic well-being of the United Kingdom; • In the interests of public safety; • for the purpose of protecting public health; • for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
7. Explain <u>why</u> this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3].
8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.] **Describe precautions you will take to minimise collateral intrusion.**

Unique Reference Number	

9. Explain <u>why</u> this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means [Code paragraphs 3.4 to 3.7]?
10. Confidential information [Code paragraphs 4.1 to 4.31]. INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

Unique Reference Number	

11. Applicant's Details			
Name (print)		Tel No:	
Grade/Rank		Date	
Signature			

12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW– in this and the following box.]

I hereby authorise directed surveillance defined as follows: [*Why is the surveillance necessary, whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]*

13. Explain why you believe the directed surveillance is necessary [Code paragraph 3.3].

Explain why you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out [Code paragraphs 3.4 to 3.7].

Unique Reference Number	

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31.

Date of first review	

Programme for subsequent reviews of this authorisation: [Code paragraph 3.23]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.

Name (Print)		Grade / Rank		
Signature		Date and time		
Expiry date and time [e.g.: authorisation granted on 1 April 2005 - expires on 30 June 2005, 23.59]				

Unique Reference Number	

15. Urgent Authorisation [Code paragraph 5.9]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.				
16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer.				
Name (Print)		**Grade/ Rank**		
Signature		**Date and Time**		
Urgent authorisation Expiry date:		**Expiry time:**		
Remember the 72 hour rule for urgent authorities – check Code of Practice.	e.g. authorisation granted at 5pm on June 1st expires 4.59pm on 4th June			

Appendix two

RENEWAL OF DIRECTED SURVEILLANCE

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000

Renewal of a Directed Surveillance Authorisation

Public Authority *(including full address)*	

Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Renewal Number			

Details of renewal:

1. Renewal numbers and dates of any previous renewals.	
Renewal Number	**Date**

2. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.

Unique Reference Number	

3. Detail the reasons why it is necessary to continue with the directed surveillance.

4. Detail why the directed surveillance is still proportionate to what it seeks to achieve.

5. Indicate the content and value to the investigation or operation of the information so far obtained by the directed surveillance.

6. Give details of the results of the regular reviews of the investigation or operation.

7. Applicant's Details			
Name (Print)		Tel No	

Unique Reference Number	

Grade/Rank		Date	
Signature			

8. Authorising Officer's Comments. This box must be completed.

9. Authorising Officer's Statement.			
I, [insert name], hereby authorise the renewal of the directed surveillance operation as detailed above. The renewal of this authorisation will last for 3 months unless renewed in writing. This authorisation will be reviewed frequently to assess the need for the authorisation to continue.			
Name (Print)	.....	Grade / Rank	.....
Signature	.....	Date	.....
Renewal From:	Time:	Date:	

Date of first review.	
Date of subsequent reviews of this authorisation.	

Appendix three

REVIEW OF THE USE OF DIRECTED SURVEILLANCE

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000

Review of a Directed Surveillance authorisation

Public Authority *(Including address)*	

Applicant		Unit/Branch /Division	
Full Address			
Contact Details			
Operation Name		Operation Number* *Filing Ref	
Date of authorisation or last renewal		Expiry date of authorisation or last renewal	
		Review Number	

Details of review:

1. Review number and dates of any previous reviews.	
Review Number	**Date**

2. Summary of the investigation/operation to date, including what private information has been obtained and the value of the information so far obtained.

Unique Reference Number	

3. Detail the reasons why it is necessary to continue with the directed surveillance.

4. Explain how the proposed activity is still proportionate to what it seeks to achieve.

5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occuring.

6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.

7. Applicant's Details			
Name (Print)		Tel No	
Grade/Rank		Date	

Unique Reference Number	

Signature	

8. Review Officer's Comments, including whether or not the directed surveillance should continue.

9. Authorising Officer's Statement.
I, [insert name], hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal][it should be cancelled immediately].
Name (Print) ..... Grade / Rank -
Signature - - - - - - - - - - - - - - - - - Date -

10. Date of next review.	

Appendix four

CANCELLATION OF THE USE OF DIRECTED SURVEILLANCE

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000

Cancellation of a Directed Surveillance authorisation

Public Authority *(including full address)*	

Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:

Unique Reference Number	

2. Explain the value of surveillance in the operation:

3. Authorising officer's statement.			
I, [insert name], hereby authorise the cancellation of the directed surveillance investigation/operation as detailed above.			
Name (Print)	.....	**Grade**	_____
Signature	.....	**Date**	_____

4. Time and Date of when the authorising officer instructed the surveillance to cease.			
Date:		**Time:**	

5. Authorisation cancelled.	Date:	Time: