Daventry District Council Surveillance Procedure

Version	Revision Date	Reviser	Description of Revision
1.0	April 2003	Mary Gallagher	Original
1.1	February 2008	Mary Gallagher	Update content
1.2	January 2012	Vikki Smith	Update format and content
1.3	January 2013	Vikki Smith	Update to include new rule regarding JP authorisation and 6 month sentencing
1.4	August 2014	Vikki Smith	Update name of Legal Advisor
1.5	February 2015	Vikki Smith	Include Section 8 on Social Media
1.6	November 2017	Vikki Smith	Change to SRO
1.7	November 2018	Vikki Smith	Removal of urgent authorisations, update social media section & use of drones

Prepared by Vikki Smith

W:\Legal\B306 Regulation of Investigatory Powers Act\File Notes\RIPA Policy & Procedure\DDC Surveillance Procedure - v 1.7.doc

DAVENTRY DISTRICT COUNCIL

COVERT SURVEILLANCE PROCEDURE (INCLUDING COVERT HUMAN INTELLIGENCE SOURCE [CHIS])

1. PURPOSE & INTRODUCTION

1.1 Daventry District Council is committed to working for the overall good of the people of the district and the wider public good, which will include carrying out appropriate investigations into allegations or concerns. Very occasionally, this will require us to gather information in respect of individuals who may be unaware of what we are doing (e.g. for suspected criminal offences) through covert surveillance. In doing so, we must draw a fair balance between the public interest and the rights of individuals.

1.2 In order to achieve that balance, the Council will take into account and comply with the Human Rights Act 1998 (HRA), the Regulation of Investigatory Powers Act 2000 (RIPA), the corresponding regulations and the Codes of Practice issued by the Home Office pursuant to RIPA. This Part of the Council's Procedure sets out the Council's approach to covert surveillance issues falling within the framework of RIPA in order to ensure consistency, balance and fairness.

1.3 The point of RIPA, to the extent that it applies to the Council, is to provide protection for the Council, individual officers and those subjected to or otherwise affected by the process. The terms of the protection are based on necessity, proportionality and the authorisation that is given in relation to a particular investigation. That said, even when RIPA is not invoked, persons conducting activities that might interfere with the right to respect for a persons private and family life will still need to rationalise and record their reasons for not seeking authorisation under RIPA.

1.4 The requirements set out in this Procedure are the minimum requirements that any officer seeking to use RIPA must comply with. If individual service areas wish to have additional procedures in place that is a matter for them but they must not be to the detriment of this Procedure, which ensures compliance with the legislation, and related Codes of Practice.

1.5 If in any doubt about the application or relevance of any part of this Procedure please seek advice from the Monitoring Officer (who is also the Senior Responsible Officer for the purposes of RIPA), the Legal Advisor, Gatekeeper or any of the Authorising Officers (detailed in Appendix I).

1.6 All persons considering the use of Directed Surveillance or a Covert Human Intelligence Source are required to have regard to this Procedure, the legislation and the relevant Codes of Practice.

1.7 It is important that the correct forms are used and so where a Home Office form is available that form must be used to ensure that it is the most up to date form. Links to the Home Office forms are in Appendix II. Home Office forms must not be stored locally or overtyped from previous applications. Either course of action may lead to avoidable errors.

1.8 The Council subscribes to the National Anti-Fraud Network (NAFN). The NAFN web site states that NAFN:

- provides an instant circulation service from one local authority to all local authorities with a view to obtaining further information and locating fraudulent activities

- offers local authorities access to services that they may not have, in order to assist with investigation work
- passes on information relating to fraud from external agencies to local authorities
- collates fraud intelligence from local authorities and external agencies
- provides regular bulletins containing intelligence on actual fraud cases
- maintains a national fraud database for access only by local authorities
- obtains intelligence to assist with serious fraud investigations by local authorities
- operates a Social Security Fraud Act 2001 Authorised Officer service to member authorities.

Having regard to service budgets and operational necessity, consideration may be given to using the services of NAFN for appropriate elements of this Procedure.

2. IMPORTANT DEFINITIONS

2.1 **'Private information'** means any information relating to a person in relation to which that person has or may have a reasonable expectation of privacy. This includes information relating to a person's private or family life and this should be considered to include an individual's private or personal relationship with others and family life should be construed as extending beyond the formal relationships created by marriage, including business and professional relationships. A person's private life may be affected by surveillance effected outside their home, business or other premises. A person's reasonable expectation as to privacy is a significant consideration albeit not necessarily a conclusive factor.

Private life considerations are likely to arise if several records are to be analysed together to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if the individual records do not. Where such conduct includes surveillance, a directed surveillance authorisation may be considered appropriate.

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites. See Section 8 below for further guidance about the use of the internet as a surveillance tool.

'**Non-private information**' may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, academic articles, conference proceedings, business reports,

and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public. Non-private data will also include the attributes of inanimate objects such as the class to which a cargo ship belongs.

2.2 **'Confidential information'** means information subject to legal privilege, confidential personal information, confidential journalistic information and information relating to the spiritual, physical or mental health of an individual (whether living or dead) who can be identified from it, such as consultations between a health professional and a patient or information from a patient's medical records. It also includes confidential discussions between Members of Parliament. If you think that you might want to use covert surveillance to obtain such information make sure that you seek advice first. Informal guidance from the Office of the Surveillance Commissioners suggests that the use of covert surveillance to seek to obtain such information should be considered very carefully with a great deal of caution and perhaps avoided if possible.

2.3 **'Covert Human Intelligence Source'** or **'(CHIS)'** means a person who establishes or maintains a personal or other relationship with a person for the purpose of covertly obtaining information or providing access to any information to another person or disclosing information obtained by the use of such a relationship or as a consequence of the existence of such a relationship. To be covert the relationship must be conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose of the relationship and the use or disclosure of such information is covert if and only if one of the parties to the relationship is unaware of the use or disclosure in question. You must remember that it is the personal or other relationship between the CHIS and the target which is relevant and not the Council and the CHIS, although of course the latter must be managed correctly by an appropriately trained person. It is important to note that the definition extends to CHIS activities designed to obtain any kind of information and not solely private information.
It is unlikely that Daventry District Council will ever use a CHIS.

2.4 **'Use of a CHIS'** means inducing, asking or assisting a person to engage in the conduct of a CHIS or to obtain information by means of the conduct of a CHIS.

2.5 **'Surveillance'** includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.

2.6 **'Directed Surveillance'** means surveillance which:

a) is covert but not intrusive surveillance; and

a) is undertaken for the purpose of a specific investigation or a specific operation; and

b) is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the

investigation or operation); and

c) is conducted otherwise than by way of an immediate response to events or circumstances the nature of which are such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance. If an immediate response is appropriate in such circumstances then the observation made would not constitute directed surveillance. This must not be abused.

2.7 **'Intrusive Surveillance'** means covert surveillance carried out in relation to anything taking place on residential premises or in any private vehicle and that involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device. This kind of surveillance may take place by means either of a person or device located inside residential premises or a private vehicle of the person who is subject to the surveillance or by means of a device placed outside which consistently provides a product of equivalent quality and detail as a product which would be obtained from a device located inside. Surveillance within the ambit of the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010 (SI2010/461) is to be treated as intrusive surveillance.

Local authorities, including Daventry District Council, *cannot* undertake intrusive surveillance.

2.8 **'Private vehicle'** means any vehicle, including vessels, aircraft or hovercraft, which is used primarily for the private purposes of the person who owns it or of a person otherwise having the right to use it. This would include, for example, a company car owned by a leasing company and used for business and pleasure by the employee of the company.

2.9 **'Residential premises'** means so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation (specifically including hotel or prison accommodation that is so occupied or used). Common areas, such as hotel dining areas or communal stairways in blocks of flats, to which a person has access in connection with their use or occupation of accommodation are specifically excluded.

2.10 **'Collateral intrusion'** means intrusion into the lives of those not the subject of or otherwise directly connected with the surveillance by obtaining private information about them. Where it is proposed to conduct surveillance activity specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy of such individuals should not be considered as collateral intrusion but as intended intrusion. Any such surveillance should be very carefully considered against the necessity and proportionality criteria.

2.11 **'Authorising Officer'** means any of the holders of the posts listed in Appendix I to this Procedure. The Chief Executive may revise the list of Authorising Officers in writing from time to time.

2.12 **'Applicant'** means a person seeking authorisation in accordance with this

Procedure.

2.13 **'Covert surveillance'** means surveillance that is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware that it is or may be taking place.

2.14 **'Overt surveillance'** means surveillance that is carried out without being secretive or clandestine and which is therefore essentially open and something which the subject of the surveillance is aware of including where, for example, persons making noise are warned (preferably in writing) that if the noise continues the noise may be recorded for the purpose of the Council exercising its statutory powers or if the Council grants a licence subject to conditions saying that officers of the Council may visit without notice or without identifying themselves to check compliance with the conditions.

2.15 **'Codes of Practice'** means the Code of Practice – Covert Human Intelligence Sources and the Code of Practice – Covert Surveillance and Property Interference published by the Home Office and available on the Home Office website – *www.homeoffice.gov.uk*. The view has been taken that to ensure that the latest version available is considered it is appropriate to make reference to the Home Office web site rather than storing a copy locally for viewing which could lead to reliance upon an out of date version. Those needing to comply with the Codes of Practice may wish to store their own hard or electronic copies for ease of reference but they should ensure from time to time that they have the latest versions. The Codes of Practice are admissible as evidence in civil and criminal proceedings and so adherence to them is critical.

2.16 **'Handler'** means the person who will conduct all day-to-day contact between a CHIS and the Council and who also has responsibility for the security and welfare of the CHIS. A Handler must be appropriately trained before acting as such.

2.17 **'Controller'** means an officer of at least the same rank as the Handler who has a general overview of the CHIS. A Controller must be appropriately trained before acting as such.

2.18 **'Gatekeeper'** means the person who will maintain the central record of all Directed Surveillance or CHIS applications, reviews, renewals and cancellations and who will undertake checks of the paperwork to try to ensure any non-compliance with RIPA is identified.

2.19 **'Sensitive Document'** applies to any document which contains sensitive personal information where disclosure of this information would lead to considerable damage to an identifiable living individual. This also covers very sensitive commercial information.

3. GENERAL PRINCIPLES

3.1 If there is interference by the Council with the rights of an individual under the European Convention on Human Rights and there is no lawful authority for that interference any such interference is likely to be unlawful and actionable by virtue of section 6 HRA. In addition, any evidence obtained in the absence of a lawful authorisation may, at the discretion of the Court, be excluded.

3.2 A properly obtained and implemented authorisation under RIPA will provide the Council with lawful authority to interfere with the rights of the individual. It is not simply enough that an authorisation for surveillance is obtained. It must be properly obtained, implemented, reviewed and cancelled.

3.3 Failure to properly obtain and implement an authorisation under RIPA will make the surveillance unlawful and may expose the Council, and possibly the individuals concerned with the surveillance, to risk.

3.4 The Council can only grant an authorisation under RIPA for the use of directed surveillance where the local authority is investigating particular types of criminal offences. These are criminal offences that attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco. Examples of when covert surveillance might be necessary includes serious or seriel benefit fraud investigations, dangerous waste dumping or serious criminal damage. The Council cannot authorise the use of directed surviellance to investigate disorder that does not involve criminal offences or to investigate low-level offences, for example, littering, dog control and fly-posting.

3.5 The Council's properly obtained authorisation can only be given effect once a Justice of Peace (JP) has granted an order approving the authorisation.

3.6 Even if RIPA is not engaged, because the interference with the private and family life of the subject does not amount to surveillance covered by RIPA, it will still be necessary to record in writing why the decision has been made not to seek an authorisation under RIPA in order to demonstrate that the action taken has been rationalised and the necessity and proportionality of it against the rights of the subject have been properly considered.

3.7 Obtaining authorisation for surveillance effectively suspends a person's human rights and so it is essential that authorisations are justifiably applied for and granted and that as soon as an authorisation is no longer needed or the surveillance has ceased the authorisation is formally cancelled.

3.8 Even though the authorised periods for surveillance, unless renewed or cancelled, will lapse after three months from when granted, all authorisations must be formally cancelled at the earliest appropriate opportunity using the cancellation form identified in Appendix II.

3.9 The Council **cannot** carry out intrusive surveillance.

3.10 RIPA does not deal with the material or information obtained as a result of surveillance. The managing and handling of such material or information must be strictly in accordance with the General Data Protection Regulation and/or the Data Protection Act 2018 and the Criminal Procedure and Investigations Act, 1996. All material should be handled and managed properly and in accordance with these and any other statutory or other requirements that may apply from time to time. Failure to do so may render the material or information inadmissible as well as exposing the Council to risk.

3.11 All of the forms referred to in this procedure must be individually completed and

signed. The copying and pasting of stock phrases is not permitted. The authorisation has to be tailor-made to suit the specific risks and circumstances of the intended surveillance operation. The five Ws (Who, What, Where, When and Why) from the Authorising Officer should always be handwritten by the Authorising Officer to demonstrate that he or she has considered and addressed these points. If challenged and the five Ws are handwritten the 'someone else wrote it' argument can be quickly dismissed. The latest versions of the form should be used. The appropriate link to the form on the Home Office web site is set out in Appendix II to this Procedure. If locally stored versions of the forms are used, there is a risk of them being out of date and referring to the wrong statutory or Code of Practice provisions. The OSC has highlighted this as bad practice.

3.12 Some surveillance activity does not constitute intrusive or directed surveillance for the purposes of Part II of the 2000 Act and no directed or intrusive surveillance authorisation can properly be provided for such activity, albeit Daventry District Council cannot undertake the latter in any event. Such activity includes:

- covert surveillance by way of an immediate response to events;
- covert surveillance as part of general observation activities;
- covert surveillance not relating to specified grounds;
- overt use of CCTV and ANPR systems;
- certain other specific situations.

The use of ANPR systems does not on the whole raise issues at the moment as they are usually only directed at number plates but this will develop to the capture of plates and faces at which time there will be a need to ensure compliance with RIPA where necessary.

3.13 All records maintained under the Act must be kept secure and confidential. A central record of all authorisations, reviews, renewals, cancellations and refusals, whatever the type of surveillance, is held on behalf of the Monitoring Officer by the Gatekeeper. Copies of all such papers must be forwarded to that person at the earliest opportunity either by providing hard copies or scanning and providing electronic copies. If hard copies are being sent to the Gatekeeper an advisory e-mail should be sent when they are sent as a check in case they go missing. Documents should be sent in sealed envelopes and marked 'Strictly Private & Confidential' or delivered by hand. If being provided electronically, the original signed forms should be scanned into Adobe pdf format and the email flagged as 'Confidential'.

3.14 The Gatekeeper will raise with Authorising Officers and Applicants any errors in RIPA documentation that they are involved with in order that they can be corrected. Where appropriate, activity that has been authorised will need to be suspended until the error is rectified. That may necessitate the cancellation of the flawed activity and the submission of a new application for authorisation. All errors will be notified to the Senior Responsible Officer.

3.15 An error must be reported if it is a "relevant error". Under section 231(9) of the 2016 Act, a relevant error for the purpose of activity covered by the Code of Practice is any error by a public authority in complying with any requirements that are imposed on it by any enactment which are subject to review by a

Judicial Commissioner. This would include compliance by public authorities with Part II of the 2000 Act. Examples of relevant errors occurring would include circumstances where:

• Surveillance activity has taken place without lawful authority.

• There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of the Code of Practice.

When a relevant error has occurred, the Council must notify the Investigatory Powers Commissioner as soon as reasonably practicable, and no later than ten working days (or as agreed with the Commissioner) after it has been established by appropriate internal governance processes that a relevant error has occurred.

The necessity to report errors reflects changes introduced by the Investigatory Powers Act 2016. See section 8.6 of the Surveillance Code of Practice.

3.16 Save where expressly stated, the provisions of this procedure relate to both directed surveillance and the use of a CHIS.

3.17 Specific situations where authorisation is not available

The following specific activities constitute neither directed nor intrusive surveillance:

• the recording, whether overt or covert, of an interview with a member of the public where it is made clear that the interview is entirely voluntary and that the interviewer is a member of a public authority. In such circumstances, whether the recording equipment is overt or covert, the member of the public knows that they are being interviewed by a member of a public authority and that information gleaned through the interview has passed into the possession of the public authority in question

• *the covert recording of noise where the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm), or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear. In the latter circumstance the perpetrator would normally be regarded as having forfeited any claim to privacy. In either circumstance, an authorisation is unlikely to be available*

4. SCOPE OF PROCEDURE

4.1 This Part of the Council's Procedure applies to all officers of the Council wishing to gather information by way of:

- directed surveillance; or
- the use of Covert Human Intelligence Sources

For the purposes of convenience in this Procedure, these two areas will be

collectively referred to as 'Covert Surveillance'.

4.2 **It is critical to understand that the Council can only carry out directed surveillance where it is necessary to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment. The Council cannot use directed surveillance for any other purpose. (RIPA Order 2012 [SI 2012/1500]).**

In addition to internal authorisation, directed surveillance must be granted by a Justice of Peace (sections 37 and 38 of the Protection of Freedoms Act 2012).

4.3 Unless there is alternative legal authority, the Council's approach to Covert Surveillance is to comply with this Procedure, and therefore RIPA, and also to have regard to and comply with the Codes of Practice.

4.4 Under section 26(2)(c) of RIPA an immediate response to circumstances does not amount to directed surveillance. This must only be used when circumstances dictate and must not be abused by the improper avoidance of seeking authorisation when it is practicable to secure authorisation.

4.5 To carry out Covert Surveillance, authorisation must be obtained from an Authorising Officer. An authorisation must not and will not be granted unless the surveillance is:

- **NECESSARY** for the purpose of preventing or detecting crime or of preventing disorder (and therefore not before an abatement or enforcement notice is served in nuisance or planning cases) and necessary in that particular case. Section 81(5) of RIPA provides that detecting crime shall be taken to include, inter alia, establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed. Disorder includes anti-social behaviour.

- **PROPORTIONATE** to what is sought to be achieved by carrying out the surveillance. Filling in this part of the authorisation request requires regard for the prompts set out in the request which relate to:

  - why the directed surveillance is proportionate to what it seeks to achieve
  - how intrusive it might be on the subject of surveillance or on others
  - why the intrusion is outweighed by the need for surveillance in operational terms or whether the evidence be obtained by any other means

- In addition, measures must be taken where practicable to avoid or minimise so far as practicable Collateral Intrusion or intended intrusion.

4.6 The Authorising Officer must be certain that the following elements of balancing proportionality have been properly considered:

  - Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence – is the proposed Covert Surveillance a "sledgehammer to crack a nut"? If it is it is probably not

proportionate. Could the intended Covert Surveillance be considered excessive or could it be less invasive?

- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others, whether collateral or intended
- 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 – if there are other practical ways of getting the information they should be explored
- Evidencing, as far as reasonably practicable, what other methods have been considered and why they were not implemented – is the proposed Covert Surveillance the only practical way of getting the information needed?

The Authorising Officer must also consider whether the surveillance is likely to add anything to the investigation or operation and whether the resulting intelligence or evidence will significantly benefit the enquiry or chance of prosecution.

The Authorising Officer is likely to be a key witness in any challenge to the use of the RIPA procedures and so ensuring the proper consideration of all relevant issues and the recording of that consideration is fundamentally important.

4.7 If the proposed actions do not fall within these definitions, or there is alternative legal authority for their use, then there is no requirement to follow this procedure. This means that either surveillance should not be carried out or there is no need for an authorisation. It is not to be assumed that surveillance can be carried out simply because this Procedure does not seem to apply. If in doubt get advice from the Monitoring Officer, Legal Advisor, Gatekeeper or any of the Authorising Officers.

4.8 **Nothing in this Procedure permits the authorising or carrying out of Intrusive Surveillance.**

4.9 Surveillance is not directed surveillance if it is carried out by way of an immediate response to events or circumstances; the nature of which are such that they were unforeseen and it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance. If an immediate response is appropriate in such circumstances then the observation made would not constitute directed surveillance. This must not be abused. If an officer, for instance, leaves the offices with a view to observing conduct as an immediate response to a telephone tip off then that is not an immediate response to unforeseen circumstances as that is setting off with the intention of carrying out covert surveillance. Conversely, if an officer is out of the office carrying out duties and a completely unrelated and unforeseen set of circumstances arises then there is no need to obtain an authorisation before carrying out surveillance on that occasion. The circumstances, what was done and what evidence was obtained must be recorded in detail as soon as possible.

5. AUTHORISATIONS – DIRECTED SURVEILLANCE

5.1 Covert Surveillance within the scope of this Procedure needs to be properly authorised and recorded. An application for authorisation must be in writing

and authorised personally by an Authorising Officer.

5.2 Even though those who may be authorising officers for the purposes of RIPA are prescribed in regulations (and specifically SI2010/521), the Council has decided to limit those within the authority who may authorise applications to the persons in the posts detailed in Appendix I as 'Authorising Officers.' No other person may authorise applications. Authorising Officers are not restricted to authorising or refusing applications for applicants from their own service area. Following the internal authorisation process, applications for surveillance must be granted by a Justice of Peace (specifically under SI2012/1500). See section 6 of this procedure for the Judicial Approval process.

5.3 Applicants must complete and send to an Authorising Officer the standard application form available from the Home Office web site for which there is a link in Appendix II. Locally saved versions of the application should not be used or previous applications overtyped, since both run the risk of mistakes and unlawful authorisations.

Use the form with the name '**Directed Surveillance Application**'.

It is critically important that the extent of the covert surveillance is fully explained on the application form because the authorisation only permits the activities stated upon it. If a particular activity is not included within the authorisation form and then that activity is undertaken, it will not be authorised and the activity will, prima facie, be unlawful and any evidence gathered may be inadmissible.

5.4 A risk assessment will also need to be completed and this may initially be done by the Applicant but the Authorising Officer must consider the content of the form and amend and expand upon the information provided as appropriate to ensure, so far as possible, that risk and health and safety issues are properly assessed and that review periods are stated for the assessment of risk and health and safety and that triggers for such reviews are stated as may be dictated by events or other circumstances, as far as can be foreseen. A risk assessment form is available on Davnet under the Health and Safety section.

5.5 The Authorising Officer must fill in the appropriate details upon the relevant application form and the risk assessment (where appropriate) and approve and keep a copy of those documents. A copy of the forms must be forwarded to the central record as above.

5.6 One of the issues to be covered in the assessment of risk for an operation or investigation, using the risk assessment form, is whether to seek public interest immunity to allow for the exclusion of material which provides the location of an observation point, in order to protect the identity of owners and occupiers of the same. Watkins LJ in R. v. Johnson [1989] 1 All ER 121 at 128, Court of Appeal, gave a ruling for a trial judge assessing such an application. The minimum evidential requirements, from the ruling, are summarised below:

- The applicant in charge of the operation or investigation must be able to testify that beforehand he visited all observation places to be used and ascertained the attitude of the occupiers of premises, not only to the use to be made of them but also to the possible

disclosure thereafter of the use made and the facts which could lead to the identification of the premises thereafter and of the occupiers.

- The applicant may in addition inform the court of difficulties, if any, usually encountered in the particular locality of obtaining assistance from the public.
- A Service Manager or Head of Service must be able to testify that immediately prior to the trial he visited the places used for observation, the results of which it is proposed to give in evidence, and ascertained whether the occupiers are the same as when the observations took place and, whether they are or are not, what the attitude of those occupiers is to the possible disclosure of the use previously made of the premises and of facts which could lead at trial to identification of premises and occupiers. Such evidence will of course be given in the absence of the jury when the application to exclude the material evidence is made.

It is for this reason that it is likely that the completed risk assessment form will be a sensitive document for disclosure purposes. Further reference should be made to the Criminal Procedure and Investigations Act 1996 and to the Code of Practice issued pursuant to section 23(1) of that Act.

5.7 Authorising Officers have the responsibility for deciding whether to grant Covert Surveillance authorisations in accordance with this Procedure. Authorisation will only be given where the Authorised Officer believes that the Covert Surveillance is necessary and a proportionate response in all the circumstances and meets the statutory criteria set out in Section 28 of RIPA. Section 28 provides that a person shall not grant an authorisation for the carrying out of directed surveillance unless he/she believes it is necessary for the purpose of preventing or detecting crime or of preventing disorder, and that the authorised surveillance is proportionate to what is sought to be achieved by carrying it out. Due regard must be had to the appropriate Code of Practice.

5.8 In general, the Authorising Officer should not be directly involved in the investigation or operation in question. Should this be unavoidable for operational reasons this should be highlighted in the information passed to the central record of authorisations.

5.9 Authorisations will cease to have effect after three months unless renewed or cancelled. It is considered good practice to grant authorisations for the maximum permissible period with appropriate review periods. Cancellation can be at any time and so there is no detriment to anyone in granting authorisations for three months.

5.10 Authorisations for surveillance must be reviewed on a regular basis and formally cancelled when no longer needed. The review periods must be indicated in the authorisation.

6. JUDICIAL APPROVAL

6.1 In addition to internal authorisation local authorities who wish to use directed surveillance or CHIS need to obtain an order approving or renewing an

authorisation from a Justice of Peace (JP) (or District Judge or lay magistrate). The procedure for this is as follows:

6.2 Following approval from one of the Council's Authorising Officers the first stage of the process is for the Senior Responsible Officer and or Gatekeeper to contact Her Majesty's Courts and Tribunals Services (HMCTS) administration team at the magistrates' court to arrange a hearing.

6.3 Both the applicant and Authorising Officer should attend court to provide the JP with a copy of the original RIPA authorisation and the supporting documents setting out the case. This forms the basis of the application to the JP and should contain all information that is relied upon.

6.4 The original RIPA authorisation should be shown to the JP but will be retained by the Council so that it is available for inspection by the Commissioner's offices and in the event of legal challenge. The Court may take a copy.

6.5 In addition, the applicant and Authorising Officer will provide the JP with a partially completed Approval Order form (Appendix III).

6.6 The order section of this form will be completed by the JP and will be the official record of the JP's decision.

6.7 The Council needs to obtain judicial approval for all initial RIPA authorisations and renewals. The Council needs to retain a copy of the Approval Order form after the JP has signed it. There is no requirement for the JP to consider either cancellations or internal reviews. See Section 10 of this procedure for Reviews and Section 11 for Cancellations.

7. AUTHORISATIONS – COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

7.1 ***It is unlikely that Daventry District Council will ever use a CHIS. Anybody considering the use of a CHIS must in the first instance seek advice from the Senior Responsible Officer or his nominee and seek legal advice***. ***All CHIS applications require internal authorisation and judicial approval, see section 6 for the judicial approval process. The crime threshold of a maximum 6 months' imprisonment does not apply to CHIS.***

7.2 Covert Surveillance within the scope of this Procedure needs to be properly authorised and recorded. An application for authorisation must be in writing to and authorised personally by an Authorising Officer.

7.3 Even though those who may be authorising officers for the purposes of RIPA are prescribed in regulations (and specifically SI2010/521), the Council has decided to limit those within the authority who may authorise applications to the persons in the posts detailed in Appendix I. No other person may authorise applications even if they are in a post that is within the regulations. Authorising Officers are not restricted to authorising, or refusing, applications for applicants from their own service area.

7.4 If a CHIS is to be used as the means of Covert Surveillance, there must also be:

- a Handler of the source, of the required seniority as is required for authorisation, and with day to day responsibility for dealing with the CHIS and for the security and welfare of the CHIS;

- a Controller of at least the same rank as the Handler who has a general overview of the source. This person will usually be a person appointed by the Authorising Officer; and

- someone of at least the same rank who as the Handler and the Controller who shall maintain records of the use made of the source but this last function could be undertaken by the Controller.

These people must be appropriately trained otherwise they will be unable to perform the functions required of them.

7.5 The RIPA Source Records Regulations (SI2000/2725) specify the matters particulars of which must be included in the records relating to each CHIS. However, if you need it, make sure that you seek advice from the Monitoring Officer or Legal Advisor as to the current status of the regulations and any revised requirements there may be if you are intending to use a CHIS. The current record requirements are:

- 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 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;

- 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 mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);

- 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.

7.6 In the case of a juvenile or vulnerable adult CHIS, the Chief Executive is the only person permitted to grant an authorisation - save that in his absence the person deputising for him (but not the Monitoring Officer) may grant the authorisation.

7.7 An officer who wishes to use a CHIS must carry out a risk assessment to determine:

- the risk to the safety and welfare of the CHIS of any tasking; and

- the likely consequences should the role become known to the target, those involved in the target activity or any other person

The risk assessment must be updated immediately there are any changes to the risk identified or any information comes to light that indicates that a change to the identified risk might be likely.

7.8 Applicants must complete and send to an Authorising Officer the standard application form available from the Home Office web site for which there is a link in Appendix II. Do not use locally saved versions and do not overtype previous applications as both run the risk of mistakes and unlawful authorisations.

Use the form with the name '**CHIS Application**'.

It is critically important that the extent of the covert surveillance is fully explained on the authorising form because the authorisation only permits the activities stated upon it. If a particular activity is not included within the authorisation form and that activity is then undertaken, it will not be authorised and the activity will, prima facie, be unlawful.

It is very important to remember the CHIS record requirements arising from the Source Records Regulations referred to below.

7.9 If the use of a CHIS is necessary, proportionate and properly authorised, the Authorising Officer must demonstrate in his or her written comments, when authorising, their awareness of the Source Records Regulations and that due attention has been paid to them. The Authorising Officer should also ensure

that the necessary personal or other relationship between the CHIS and the target is properly understood and rationalised. Further, the special rules relating to the use of a juvenile or vulnerable person as a CHIS must be shown to have been considered and properly applied.

7.10 The Authorising Officer must consider the content of the risk assessment form and amend and expand upon the information provided as appropriate to ensure, so far as possible, that risk and health and safety issues are properly assessed and that review periods are stated for the assessment of risk and health and safety and that triggers for such reviews are stated as may be dictated by events or other circumstances as can be foreseen. A risk assessment form is available on the intranet although individual service areas may wish to devise their own risk assessment forms.

7.11 The Authorising Officer must fill in the appropriate details upon the relevant application form and the risk assessment and either approve or refuse the request for authorisation. The Authorising Officer shall keep a copy of those documents.

7.12 The consideration referred to above about whether to seek public interest immunity is equally valid here.

7.13 Authorising Officers have the responsibility for deciding whether to grant CHIS authorisations in accordance with this Procedure. Authorisation will only be given where the Authorised Officer believes that the proposed use of the CHIS is necessary and a proportionate response in all the circumstances and meets the statutory criteria set out in Section 29 of RIPA. Due regard must be had to the appropriate Code of Practice. There must be satisfactory arrangements for managing the source as required by Section 29(5) of RIPA.

7.14 It is very important that the full extent of the CHIS activities is fully explained on the authorising form, because the authorisation only permits the activities stated upon it.

7.15 The Authorising Officer will appoint an officer to act as the designated Handler for the CHIS. The Handler will make sure that appropriate records are kept of the activities of and interaction with the CHIS. Services may devise their own forms for these purposes.

7.16 Authorisations will cease to have effect after twelve months unless renewed or cancelled (one month for a juvenile source – see currently the Regulation of Investigatory Powers (Juveniles) Order SI2000/2793). Authorisations for surveillance should be given for the appropriate length of time but in any event not longer than the maximum duration.

7.17 Authorisations for surveillance must be reviewed on a regular basis and formally cancelled when no longer needed. The review periods must be indicated in the authorisation.

7.18 As one of the measures to be taken to protect the identity of the CHIS, consideration should be given to not holding the paperwork relating to the authorisation and use of the CHIS on the case file.

7.19 Each service area that wishes to use a CHIS shall appoint an administration officer who has had appropriate confidentiality training to maintain a register of every CHIS used in that service area to which access will be strictly limited according to the wishes of the Head of Service for the service area. These arrangements must comply with the source records regulations (SI2000/2725).

8. SOCIAL MEDIA

8.1 *S*ocial Media has a potential to become a CHIS issue. There has been a proliferation in the use of social media such as facebook, twitter and others, even E bay. A considered approach is required to establish whether or not any material obtained via these sites constitutes either Directed Surveillance or a CHIS.

8.2 Reviewing open source sites does not require authorisation unless the review is carried out with some regularity, usually when creating a profile, in which case a directed surveillance authorisation will be required. If it becomes necessary to breach the privacy controls and become, for example, a "friend" on the Facebook site, with the investigating officer utilising a false account concealing his/her identity as a Council officer for the purposes of gleaning intelligence, this is a covert operation intended to obtain private information and should be authorised, at a minimum, as Directed Surveillance. If the investigator engages in any form of relationship with the account operator then he/she becomes a CHIS, requiring authorisation as such and management by a Controller and Handler with a record being kept and a risk assessment created.

8.3 In the case of E bay, merely examining public feedback to gauge the level and type of sales listed would not constitute Directed Surveillance or CHIS, and neither would a one off test purchase. However, repeated visits to the site are likely to be undertaken covertly, and if used with other information obtained elsewhere, especially surveillance of any type, with a view to building up a profile of the subject, then the totality of the information obtained could be construed as 'private' with all the applicable RIPA ramifications. See the examples below.If in doubt, officers should seek legal opinion.

Example 1: A simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence is unlikely to need an authorisation. However, if having found an individual's social media profile or identity it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.

Example 2: Initial examination of an individual's online profile to establish whether they are of relevance to an investigation is unlikely to need an authorisation. Visiting a website would not normally amount to surveillance, but if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. As set out in 8.4, the purpose of the visit may be relevant as to whether an authorisation should be sought.

Example 3: As set out at paragraph (section on situations where authorisation is not available) below, general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation does not require RIPA authorisation. This includes any monitoring that is intended to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. It may also include the discovery of previously unknown subjects of interest, but once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.

8.4 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 organisation;
- Whether it is likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 2.1 above);
- 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 private information and therefore constitute collateral intrusion into the privacy of these third parties.

9. AERIAL COVERT SURVEILLANCE

9.1 '**Aerial covert surveillance**' is the use of airborne crafts or devices, for example helicopters or unmanned aircraft (colloquially known as 'drones'). When surveillance is planned using drones, the same considerations should be made about necessity and proportionality to determine whether a directed surveillance authorisation is appropriate. In considering whether the surveillance should be regarded as covert, account should be taken of the reduced visibility of a craft or device at altitude.

10. REVIEWS

10.1 The Authorising Officer should determine how often the authorisation should be reviewed. This needs to be as frequently as necessary and practicable but in any event at periods not exceeding one month both from the initial authorisation and during the life of the authorisation.

10.2 The likelihood of obtaining confidential information (see section 15 below) or collateral private information relating to someone other than the subject must be borne in mind when setting the review period as proportionality will change the longer the activity continues.

10.3 It is the responsibility of each Applicant to inform the Authorising Officer in advance of the time for a review. An authorisation monitoring form should be completed and held by the Authorising Officer and updated by the Applicant to help diarise this process.

10.4 Records of reviews will be kept as required below.

Use the form with the name **'Directed Surveillance Review'** for the review of a directed surveillance authorisation.

Use the form with the name **'CHIS Review'** for the review of a CHIS authorisation.

11. RENEWALS

11.1 As with applications for authorisation for directed surveillance, it is critical to the lawfulness of the authorisation and the resultant surveillance, and hence the admissibility of evidence, that particular attention is given to proportionality. There is a legitimate line of attack against an authorisation, the surveillance based upon it and the evidence gathered if the previously authorised surveillance has failed to gather the evidence that was sought or the proportionality of the surveillance has otherwise diminished since authorisation. Applicants should proceed on the basis that with each application for renewal the burden of satisfying the proportionality requirement increases. It is simply not acceptable to recite what has previously been recorded as to proportionality as the circumstances will be different, surveillance having already been carried out for a period.

If an Applicant gets it wrong it will be the Applicant and the Authorising Officer that will be answerable to the Court.

11.2 Authorisations may be renewed for a further period of three months (twelve months for CHIS or one month for a juvenile CHIS) provided an Authorising Officer is satisfied they continue to meet the criteria. The relevant standard renewal application forms must be used except in cases of urgency.

Use the form with the name **'Directed Surveillance Renewal'** for the renewal of a directed surveillance authorisation.

Use the form with the name **'CHIS Renewal'** for the renewal of a CHIS authorisation.

It is critical that when making an application for a renewal due regard is given to paragraph 8.1 as to the need to pay particular attention to proportionality at each renewal and at reviews between renewals.

11.3 Authorisations can be renewed more than once but note above at paragraph 8.1 the need to pay particular attention to proportionality at each renewal and at reviews between renewals.

11.4 Records of renewals will be kept as required below.

11.5 It is the responsibility of each Applicant to inform the Authorising Officer in advance of the time for a renewal. A monitoring form should be completed and held by the Authorising Officer and updated by the Applicant to help diarise this process.

12. CANCELLATION

12.1 The Authorising Officer must cancel the authorisation if satisfied that the activity no longer meets the criteria upon which it was or could have been authorised or satisfactory arrangements for the use of the CHIS no longer exist. The standard cancellation forms must be used.

Use the form with the name **'Directed Surveillance Cancellation'** for the cancellation of a directed surveillance authorisation.

Use the form with the name **'CHIS Cancellation'** for the cancellation of a CHIS authorisation.

12.2 Authorisations must be formally cancelled upon completion of the operations to which they relate or where they are no longer needed.

12.3 Records of cancellation will be kept as required below.

13. JOINT WORKING WITH OTHER AGENCIES

13.1 It may from time to time be appropriate to mount joint surveillance operations with other agencies. The tasking or lead agency should authorise the operation under its own covert surveillance procedure. It is important to avoid duplication and to ensure that parallel surveillance does not prejudice an operation by another body.

13.2 An example is where a police officer of at least superintendent rank requests the use of CCTV staff and equipment to monitor specific areas at specific times. The police officer, on behalf of the police as the tasking agency, should authorise the operation under the covert surveillance procedure of the police. The appropriate paperwork, and particularly the authorisation, should be sent to the Council's CCTV supervisor for approval prior to the start of the operation. In an emergency or where this is impracticable, the completed form should be faxed to the operation centre, and the supervisor can check and query or approve the form and the use of the CCTV system retrospectively. The police authorisation may contain a request for directed and intrusive surveillance for the additional grounds not available to the Council, such as public safety. It may also request the surveillance of a hot spot, which is an area not normally

or regularly covered by the CCTV system, but where surveillance is not likely to elicit private or confidential information.

13.3 If a joint operation is to be undertaken the lead or authorising authority must provide the other participating authorities with a copy of the authorisation and any renewal, review and cancellation paperwork. If this does not happen the participating authorities who are not the lead authority will not know the details of what has been authorised or when the authorisation has come to an end. Officers of Daventry District Council will not be permitted to participate in any surveillance for which authorisation is required unless this requirement as to document sharing is complied with. Copies of all such documents will be provided to the central record. Any difficulties in compliance will be reported without delay to the Senior Responsible Officer or his nominee who will then be obliged to liaise with the lead or authorising authority to ensure compliance or prevent the joint operation from taking place.

14. RECORDS

14.1 A central register of all authorisations, reviews, renewals, cancellations and refusals under this Part of this Procedure will be held by the Information Officer on behalf of the Monitoring Officer as Senior Responsible Officer. This register must be updated whenever an authorisation is granted, reviewed, renewed, cancelled or refused. This will be achieved by the Authorising Officer forwarding a copy of the approved application, review, renewal, cancellation, or refusal to the Information Officer. There will be no exceptions to this. The corporate register will be retained for at least three years.

14.2 The Applicant will retain the original forms of authority, review, renewal, cancellation or refusal and in addition will hold:

- Any supplementary documentation given to or by the Authorising Officer
- Any separate notification of approval given by the Authorising Officer
- A record of the period over which surveillance has taken place
- The frequency of reviews decided by the Authorising Officer in the case
- A record of the result of each such review
- Any supporting documentation provided for a renewal of authorisation
- The date and time of any instruction given by the Authorising Officer
- Records of the use of a particular CHIS, any risk assessment in relation to the source, the value of the source, the circumstances in which tasks were given to the source and any other record required by regulation.
- A note of when and how documents have been submitted to the central register.

14.3 All records maintained under the Act must be kept secure and confidential and the measures set out in paragraph 3.11 followed when documents are being

sent to the central register.

14.4 The proper keeping of records, including the central record, is also important for quarterly and annual reporting that is required to Members on the amount and nature of the use of RIPA that has occurred and also to allow Members to effectively consider the confirmation or variation, as appropriate and if necessary, of this Procedure on a quarterly and annual basis as required by the Codes of Practice.

15. CONFIDENTIAL INFORMATION

15.1 Although RIPA does not provide any special protection for confidential information, particular care should be taken where confidential information might be obtained. Further guidance is available in the relevant Codes of Practice.

15.2 Where it is likely that confidential information will be acquired activity must be authorised by the Chief Executive - or in the absence of the Chief Executive the person deputising for him (but not the Monitoring Officer). In general, legal advice should be obtained prior to any activity that is likely to acquire confidential information.

15.3 If an investigation is going to seek information about lawyers, priests, doctors or journalists in relation to their professional activities advice must be sought from the Monitoring Officer or Legal Advisor as special rules apply. (Further information can be found in the 1997 Act and 2010 Order for legally privileged and confidential information.)

16. RECORD KEEPING AND DATA PROTECTION

16.1 All records referred to in this procedure will be retained for a period of 3 years from the ending of the authorisation or last renewal. These records will be kept in a secure file, with access limited to the appropriate officers.

16.2 The central register will be kept as referred to elsewhere in this Procedure and will contain the following information:

- the type of authorisation;
- the date the authorisation was given;
- the name and grade of the authorising officer;
- the unique reference number of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- the date of attendance at Magistrates' court, determining Magistrate, court decision and time/date of court decision
- if the authorisation has been renewed, when it was renewed and who authorised the renewal, including the name and grade of the authorising officer;
- whether the investigation or operation is likely to result in obtaining confidential or privileged information as defined in this code of practice;
- whether the authorisation was granted by an individual directly involved in the investigation; and
- the date the authorisation was cancelled

- and if refused, the details

16.3 In relation to CHIS authorisations, these records need only contain the name, code name, or unique identifying reference of the CHIS, the date the authorisation was granted, renewed or cancelled and an indication as to whether the activities were self-authorised.

16.4 As appropriate, the authority's data protection advisors will be consulted to ensure that material is handled, stored and disposed of in accordance with the requirements of the Data Protection Act 2018.

16.5 Records kept in relation to CHIS authorisations shall be maintained in such a way as to preserve confidentiality, prevent disclosure of the identity of the CHIS and prevent disclosure of the information provided by that CHIS.

17. GENERAL

17.1 This Procedure is a public document and will be available for public inspection at Lodge Road, Daventry, Northamptonshire, NN11 4FP and upon the Council's internet site. Copies of this Procedure will be available to officers on Davnet. The procedure will be reviewed and updated from time to time by the Monitoring Officer in consultation with appropriate colleagues.

17.2 Oversight of RIPA Covert Surveillance procedures is provided by the Investigatory Powers Commissioner's Office who may be contacted at PO Box 29105, London, SW1V 1ZU.

17.3 Complaints concerning the way in which the Council has operated this procedure may be made to the Monitoring Officer, Lodge Road, Daventry, Northamptonshire, NN11 4FP or through the complaints system available on the Council's internet site.

APPENDIX I

The Council has limited those within the authority who may authorise applications, as below. No other person may authorise applications. Authorising officers are not restricted to authorising, or refusing, applications for applicants from their own service area.

Authorising Officers

The following persons who are in posts designated by the relevant regulations and who are considered to have sufficiently up to date experience and training:

Tony Gillet – Executive Director (Resources)
Maria Taylor – Executive Director (Community)
Michael Pullan – Revenues and Benefits Manager
Ed Cooke – Environmental Health Manager (Environmental Improvement)
Paul Knight – Environmental Health Manager (Health Improvement)

Authorised Officers in relation to Confidential material

Ian Vincent - Chief Executive or Ed Cooke in the absence of the Chief Executive (not the Monitoring Officer)

Senior Responsible Officer

Simon Bovey - Monitoring Officer

Legal Advisor

District Law

Gatekeeper

Vikki Smith – Information Officer

APPENDIX II

The links below have been cut and pasted direct from the Home Office web site and although there are some apparent spelling mistakes the links are correct.

Directed Surveillance Forms

Directed Surveillance Application:

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/application-directed-surveillanc

Directed Surveillance Review:

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/review-directed-surveillance

Directed Surveillance Renewal:

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/renewal-directed-surveillance

Directed Surveillance Cancellation:

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/cancellation-directed-surveillan

Covert Human Intelligence Forms

CHIS Application:

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-application

CHIS Review:

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-review

CHIS Renewal:

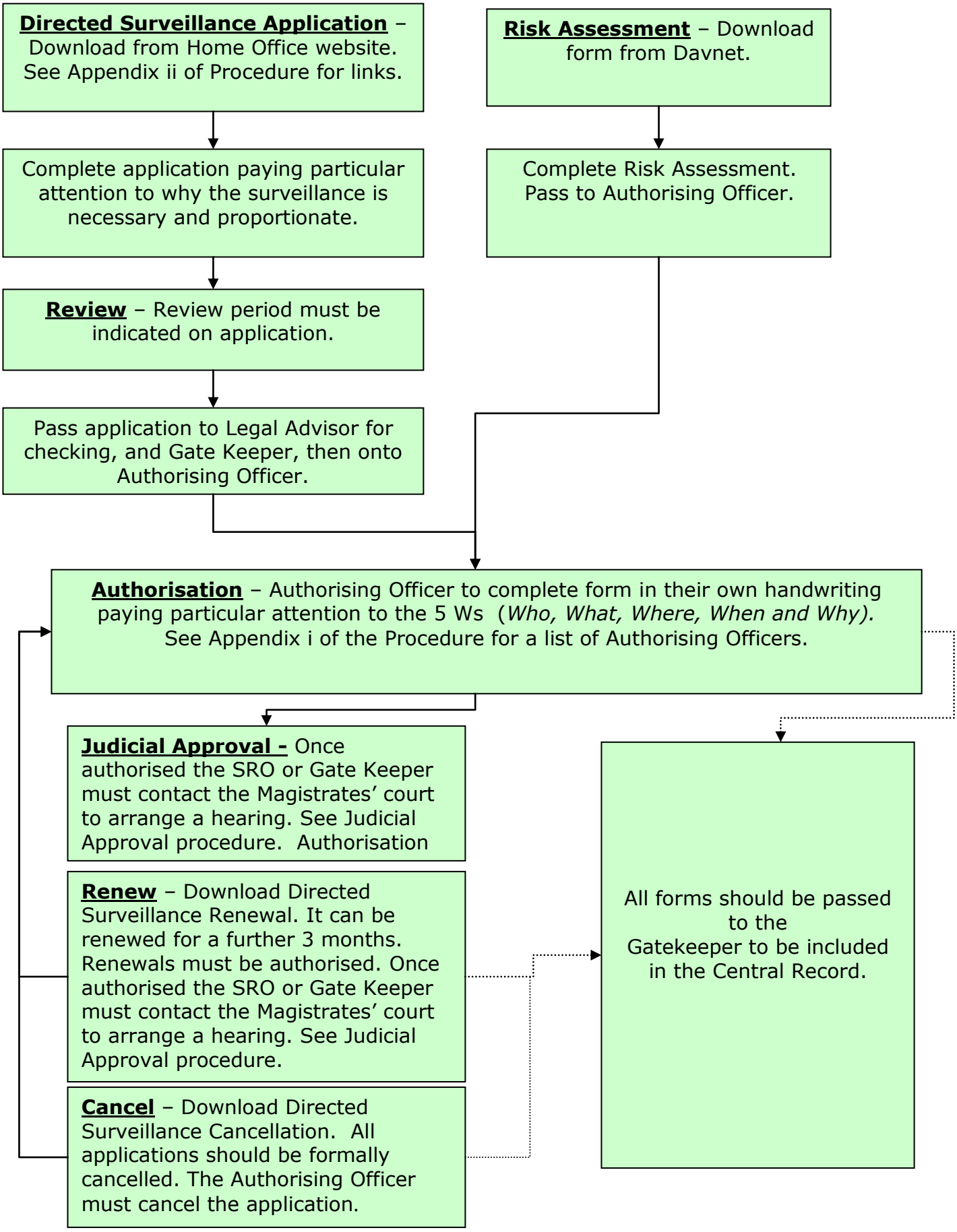
http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-renewal

CHIS Cancellation:

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-cancellation

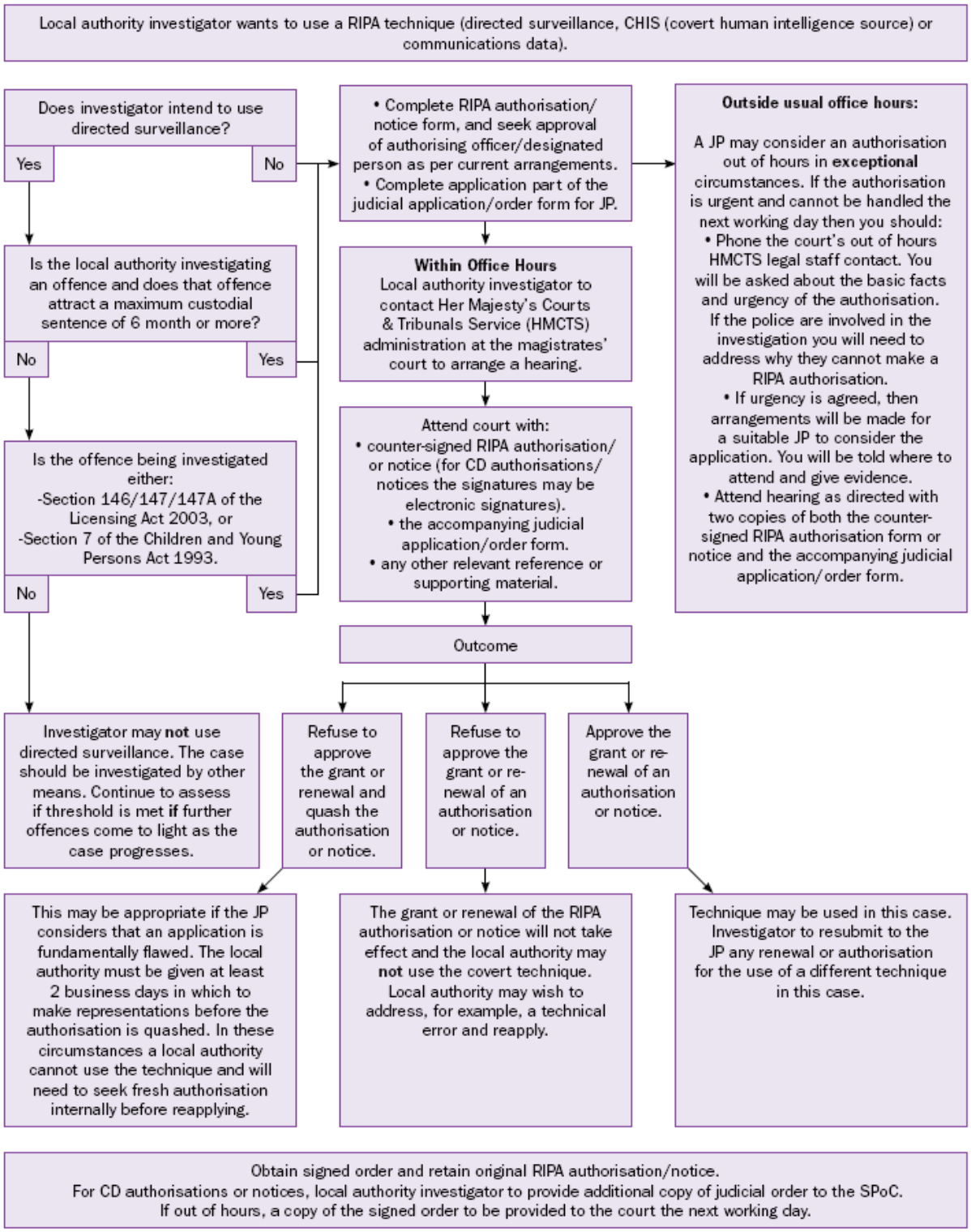
APPENDIX III

Procedure for Written Authorisations for Directed Surveillance:



APPRENDIX III - Procedure for Judicial Approval

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



APEPENDIX III – Approval Order form

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

Local authority:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of subject:.....

.....

.....

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

.....

.....

.....

.....

.....

.....

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

Investigating Officer:.....

Authorising Officer/Designated Person:.....

Officer(s) appearing before JP:.....

Address of applicant department:.....

.....

Contact telephone number:.....

Contact email address (optional):.....

Local authority reference:.....

Number of pages:.....

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

Magistrates' court:.....

Having considered the application, I (tick one):

☐ am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

.....

.....

.....

.....

.....

Reasons

.....

.....

.....

.....

.....

.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court: