South Somerset District Council

CORPORATE POLICY & PROCEDURES GUIDE

ON

THE REGULATION OF INVESTIGATORY POWERS ACT 2000

('RIPA')

Martin Woods
Director – Director of Place
The Council Offices
Brympton Way
Yeovil
Somerset
BA20 2HT

Tel: 01935 462071
e-mail: martin.woods@southsomerset.gov.uk

Revised version date: 3.11.20

CONTENTS PAGE

NB:
The Regulation of Investigatory Powers Act 2000 ('RIPA') refers to 'Designated Officers'. For ease of understanding and application, this Corporate Policy & Procedures Guide refers to 'Authorising Officers'. Such Officers can only act under RIPA if they have been duly certified by the Councils Director- Service Delivery (or his authorised deputy for such purposes). For the avoidance of doubt, all references to duly certified Authorising Officers in this Guide are the same as references to 'Designated Officers' under RIPA.

A. Introduction and Key Messages

1. This South Somerset District Council ('SSDC') *Corporate Policy & Procedures Guide on the Regulation of Investigatory Powers Act 2000 ('RIPA')* is based on the requirements of RIPA and the Home Office's Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources ('CHIS'). Further explanation of these terms is given below, but it can be said immediately that what we in SSDC are primarily concerned with is covert surveillance and not CHIS.

2. The authoritative position on RIPA is, of course, the Act itself (and the interpretation of the Act by the courts). Any officer who is unsure about any aspect of this Guide should contact, at the earliest possible opportunity, the Director of Service Delivery who is the Senior Responsible Officer (SRO) for RIPA, for advice and assistance. Appropriate training and instruction will be organised by the SRO for relevant Authorising Officers and other appropriate senior managers. Further information and guidance on RIPA can be found on the Home Office website and the website of the Investigatory Powers Commissioner's Officer (IPCO)

3. Once approved, copies of this Guide and the RIPA authorisation forms will be placed on the SSDC InSite intranet, a list of useful websites linking to legislation and guidance documents will also be placed on the intranet. The Guide minus the appendices will be put on the SSDC public website.

4. Since the introduction of the Protection of Freedoms Act 2012 the authorisation procedure must now undergo judicial scrutiny. Following an internal authorisation being made by an authorising officer judicial approval by a Justice of the peace at the Magistrates Court is necessary before the surveillance can take place.

5. The SRO will maintain (and check) the Corporate Register of all RIPA authorisations, reviews, renewals, cancellations and rejections as well as the judicial applications and approvals However, it is the responsibility of the relevant Authorising Officer to ensure that the SRO receives a copy of any completed RIPA form within 1 week of the date of authorisation, review, renewal, cancellation or rejection or judicial approval.

6. RIPA and this Guide are important for the effective and efficient operation of the Council's actions with regard to covert surveillance and the use of CHIS. This Guide will be reviewed every 6 months by the SRO to keep it up to date. Authorising Officers and other officers involved with RIPA are asked to bring any suggestions for the improvement of this Guide to the attention of the SRO at the earliest possible opportunity (in writing please). The Council wishes to ensure that RIPA procedures are continuously monitored and improved or updated as necessary.

7. In terms of monitoring e-mails and internet usage, it is important to recognise the interplay and overlaps with the Council's e-mail and internet policies and guidance, together with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Data Protection Act 1998 and its Codes of Practice. RIPA forms should be used where relevant and they will be only relevant where the criteria listed on the RIPA forms are fully met.

8. **If you are in any doubt about RIPA, this Guide or the related legislative provisions, please consult the SRO at the earliest possible opportunity.**

B. Council's Policy Statement

1. SSDC takes its statutory responsibilities seriously and it will at all times act in accordance with the law and take action that is both necessary and proportionate to the discharge of such statutory responsibilities. In that regard, the SRO is duly authorised by SSDC to keep this Guide up to date and 'user friendly'; and to amend, delete, add or substitute any provisions of this Guide as he deems necessary, whereupon such amendments, deletions, additions or substitutions shall stand as duly approved by SSDC. For administrative and operational effectiveness, the SRO is also authorised to add or substitute officers authorised for the purposes of RIPA (known as 'Authorising Officers') – see Appendix 1.

C. Authorising Officer Responsibilities

1. It is essential that Authorising Officers in those Services take personal responsibility for the effective and efficient operation of this policy Guide.

2. The SRO will ensure the authority have sufficient numbers of officers (after suitable training and instruction on RIPA and this policy Guide) duly certified to act as Authorising Officers.

3. The Authority will also ensure that all relevant members of staff likely to use RIPA are suitably trained as 'Applicants' for seeking RIPA authorisation, so as to avoid common mistakes appearing on RIPA forms. This can be done in conjunction with the SRO

4. Authorising Officers will need to ensure that relevant staff in their Service all follow the procedures set out in this Guide and do not undertake or carry out any type of surveillance without first obtaining the relevant RIPA authorisation.

5. Authorising Officers must also pay particular attention to Health and Safety issues that may arise from any proposed surveillance or CHIS activity. Under no circumstances should an Authorising Officer approve any RIPA form until s/he is satisfied that the health and safety of Council employees/agents has been suitably addressed and a risk assessment carried out. Risks should be minimised as far as possible. Health and safety considerations and risks should be proportionate to the surveillance or CHIS activity being proposed. If an Authorising Officer is in any doubt, s/he should obtain prior guidance on these issues from his/her Service Manager, the Council's Safety Adviser and/or the SRO.

6. Authorising Officers must also ensure that RIPA forms (originals or copies) sent to the SRO (or any other relevant authority) are sent in sealed envelopes and marked 'Strictly Private & Confidential'.

D. General Information on RIPA

1. The Human Rights Act 1998 (which enacted much of the European Convention on Human Rights and Fundamental Freedoms 1950 into UK domestic law) requires SSDC (and agencies working on its behalf) to respect the private and family life of citizens, their home and their correspondence. See Article 8 of the European Convention.

2. However, the European Convention does not make this an absolute right, but a qualified right. Accordingly, in certain circumstances SSDC may interfere with the citizen's right mentioned above if such interference is:

   (a) in accordance with the law;

   (b) necessary; and

   (c) proportionate.

3. RIPA provides a statutory mechanism for authorising covert surveillance and the use of a 'covert human intelligence source' ('CHIS'), such as undercover agents. (SSDC will rarely use a CHIS and the advice of the SRO must be sought before any authorisation is sought for the use of a CHIS). RIPA seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, RIPA seeks to ensure that both the public interest and the human rights of individuals are suitably balanced. This balancing exercise has to be carried out every time that action is taken that may affect an Article 8 right, as it is part of the assessment of the proportionality of the proposed action.

4. Directly employed SSDC staff and external agencies working for SSDC are covered by RIPA during the time they are working for SSDC. Therefore, all external agencies used by SSDC must comply with RIPA. Work carried out by agencies on SSDC's behalf must be properly authorised by an SSDC RIPA designated Authorising Officer. Authorising Officers are those whose posts appear in Appendix 1 to this Guide (as may be added to or substituted by the SRO).

5. If the correct RIPA procedures are not followed, evidence could be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman, and the Council could be ordered to pay compensation. If this happened, the good reputation of the Council would be damaged and the matter would undoubtedly be the subject of adverse press and media comment. Therefore, it is essential that all SSDC staff and agents involved with RIPA regulated activities comply with the procedures set out in this Guide, and any further guidance that may be issued from time to time by the SRO.

6. A flowchart of the procedures to be followed appears at Appendix 2.

E. What RIPA Does and Does Not Do

1. **RIPA does**:

   - require prior authorisation of directed surveillance.
   - prohibit the Council from carrying out intrusive surveillance.
   - require authorisation of the conduct and use of a CHIS.
   - require safeguards for the conduct and use of a CHIS.

2. **RIPA does not**:

   - make unlawful conduct which is otherwise lawful.
   - prejudice or disallow any existing powers available to SSDC to obtain information by any means not involving conduct regulated by RIPA. For example, it does not affect SSDC's current powers to obtain information from the DVLA about the keeping of a vehicle or from the Land Registry about the ownership of a property.

3. If an Authorising Officer or any officer is in doubt about the above or any other aspect of RIPA, s/he should ask the Director of Service Delivery BEFORE any directed surveillance and/or CHIS is applied for, authorised, renewed, cancelled or rejected. As stated elsewhere, CHIS applications must in any case be subject to prior legal advice before they are submitted.

F. Types of Surveillance

1. 'Surveillance' includes

   - monitoring, observing, listening to people, watching or following their movements, listening to their conversations and similar activities.

   - recording anything mentioned above in the course of authorised surveillance.

   - surveillance by, or with the assistance of, appropriate surveillance devices.

   Surveillance can be overt or covert.

2. ***Overt Surveillance***

   Most of the surveillance carried out by the Council will be done overtly - there will be nothing secretive, clandestine or hidden about it. In many cases officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases carried out by Environmental Health for food hygiene or other purposes), or will be going about Council business openly (e.g. a car parks inspector walking through a Council car park).

3. Similarly, surveillance will be overt if the subject has been told it will happen. Examples could be where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues; or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or without identifying themselves to the owner/proprietor to check that the conditions are being met. Such a warning should be repeated if the surveillance is prolonged – say every 2 months.

4. ***Covert Surveillance***

   Covert Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place. (Section 26(9)(a) RIPA).

5. RIPA regulates two types of covert surveillance - **Directed Surveillance** and **Intrusive Surveillance** (plus the use of **Covert Human Intelligence Sources (CHIS)**).

6. ***Directed Surveillance***

   Directed Surveillance is surveillance that:

   - is covert; and

   - is not intrusive surveillance (see definition below - the Council must not carry out any intrusive surveillance);

   - is not carried out as an immediate response to events that would otherwise make seeking authorisation under the Act unreasonable (e.g. spotting something suspicious without prior knowledge and continuing to observe it); and

- is undertaken for the purpose of a specific investigation or operation in a manner likely to obtain private information about an individual (whether or not that person is specifically targeted for purposes of an investigation). (Section 26(10) RIPA).

7. Private information in relation to a person includes any information relating to his private and family life, his home and his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance of a single person will undoubtedly result in the obtaining of private information about that person - and other persons who he contacts or with whom he associates.

8. Similarly, although overt town centre CCTV cameras do not normally require authorisation, an authorisation will be required if the camera is used for a specific purpose that involves prolonged surveillance of a particular person. The way a person runs their business may also reveal information about their private life and the private lives of others.

9. For the avoidance of doubt, only those officers designated and certified to be 'Authorising Officers' for the purpose of RIPA can authorise 'Directed Surveillance' - and only if the RIPA authorisation procedures set out in this Guide and effective from the operative date are followed. Authorising Officers not yet 'certified' for the purposes of RIPA cannot carry out any such procedures, including approving or rejecting RIPA authorisations. Further, notwithstanding anything to the contrary in the Council's 'Schedule of Functions Delegated to Officers' (i.e. the officer delegation scheme) as set out in the Council's Constitution, or in any other statutory provisions, RIPA Authorising Officers cannot delegate their power of authorisation to another officer unless that officer is also an Authorising Officer for RIPA purposes (and listed in Appendix 1), in which case the officer would be authorising in his/her own right. If in doubt, check with the SRO. Officers will bear personal responsibility for ensuring correct RIPA authorisation procedures.

10. ***Intrusive Surveillance***

This is when surveillance:

- is covert;

- relates to activities inside residential premises and private vehicles; and

- involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if it was in the premises or vehicle.

11. Intrusive surveillance can only be carried out by the police and certain other law enforcement agencies. Council officers must not carry out intrusive surveillance.

12. ***Examples of different types of Surveillance***

Type of Surveillance	**Examples**
Overt	- Police Officer or Countryside Ranger on patrol. - Signposted Town Centre CCTV cameras (in normal use). - Recording noise emitted from premises after the occupier has been warned that this will occur if the noise persists.
Covert but not requiring prior RIPA authorisation	- CCTV cameras providing general traffic, crime or public safety information. Most test purchases (where the officer behaves no differently from a normal member of the public).
Directed (must be RIPA authorised)	- Officers following someone over a period to establish whether they are working when claiming benefit, or genuinely on long term sick leave from employment. - Test purchases where the officer has a hidden camera or other recording device to record information, which might include information about the private life of a shop-owner, e.g. where they are suspected of running their business in an unlawful manner.
Intrusive (the Council cannot do this)	- Planting a listening or other device (bug) in a person's home or in their private vehicle.

G. Conduct and Use of a Covert Human Intelligence Source ('CHIS')

Who is a CHIS?

1. Someone who establishes or maintains a personal or other relationship for the covert purpose of covertly using or covertly disclosing information obtained by that relationship. In common parlance, an 'undercover' police officer or, indeed, council officer. The archetypal CHIS would be a police officer carrying out an undercover drugs investigation where the 'target' does not know the officer's true identity. It would be most unusual for a local authority to use a CHIS.

2. RIPA does not apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or where the public contact telephone numbers set up by the Council to receive information.

What must be authorised?

3. The Conduct or Use of a CHIS requires prior authorisation.

   - **Conduct of a CHIS means**: Establishing or maintaining a personal or other relationship with a person for the covert purpose of (or incidental to the covert purpose of) obtaining and passing on information.
   - **Use of a CHIS means**: Inducing, asking, or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

4. The Council can only use a CHIS if the RIPA procedures in this Guide are followed. As mentioned above, it will be most unusual for the Council to use a CHIS. **THE ADVICE OF THE SRO MUST BE SOUGHT BEFORE ANY AUTHORISATION IS SOUGHT FOR THE USE OF A CHIS.**

5. In accordance with The Home Office Code of Practice on Covert Human Intelligence Sources the Council will ensure that arrangements are in place for the proper oversight and management of CHIS. This will include in each case requiring a CHIS the appointment and designation of individual officers to take the role of 'handler' 'controller' and 'record keeper'

6. The 'handler' will be of a rank or position below that of an authorising officer and this person will also be the 'record keeper', they will be;

- 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 CHIS's security and welfare

7. The 'controller' of the case will be responsible for the management and supervision of the handler and general oversight of the use of the CHIS.

Juvenile Sources

5. Special safeguards apply to the use or conduct of juvenile sources (i.e. sources under 18 years of age). On no account can a child under 16 years of age be authorised to give information against his or her parents. **Only the Chief Executive and Head of Paid Services are authorised by the Council to use Juvenile Sources**, as there are other onerous requirements that apply.

Vulnerable Individuals

6. A Vulnerable Individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness, and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.

7. A Vulnerable Individual will only be authorised to act as a source in the most exceptional circumstances. **Only the Chief Executive and Head of Paid Services are authorised by the Council to use Vulnerable Individuals**, as there are other onerous requirements that apply.

Test Purchases

8. As mentioned above, carrying out test purchases will not require the purchaser to establish a relationship with the supplier for the covert purpose of obtaining information. Therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).

9. However, developing a relationship with a person working in the shop for the purpose of obtaining information about the seller and his/her business (e.g. the seller's suppliers who are supplying illegally imported products) will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance. A combined authorisation can be given for a CHIS and also for directed surveillance.

Anti-social behaviour activities (e.g. noise, violence, race etc.)

10. Persons who complain about anti-social behaviour (such as playing music too loudly) and who are asked to keep a diary of incidents will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information; therefore, it does not require authorisation.

11. Recording sound on private premises could constitute intrusive surveillance unless it is done overtly. It will be possible to record noise levels without it being intrusive surveillance if the noisemaker is given written warning that such recording or monitoring will occur. (Such a warning should be repeated at least every 2 months if the operation is on-going). Placing a stationary or mobile video camera outside a building to record anti-social behaviour on residential estates will require prior authorisation.

Social Networking and Internet Site

12. Rapidly increasing use of the Internet and social networking sites across communities and businesses has resulted in law enforcement having access to an array of investigative tools, Social network sites (and other 'open source' intelligence resources) contain a wealth of information, intelligence and evidence

about suspects, victims, witnesses, members of organised crime groups and other aspects of crime and anti-social activity.

13. Although social networking and internet sites are easily accessible, if they are going to be used during the course of an investigation, consideration must be given about whether RIPA authorisation should be obtained.

14. Care must be taken to understand how the social media site being used works. Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

15. Whilst it is the responsibility of an individual to set privacy settings to protect against unsolicited access to their private information on a social networking site, and even though the data may be deemed published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available; the author has a reasonable expectation of privacy if access controls are applied. Where privacy settings are available but not applied the data may be considered open source but you must be mindful that an individual is not expecting this source to be used to covertly monitor their actions and whereas an authorisation may not usually be required you must be careful of how you access this type of account and for what purpose. If you are scoping (this includes an initial look at someone through open source material) no authority would be required, however if from this you then identify the subject and a plan is made for the gathering of evidence and you access the same websites to monitor that person more than once or on a regular basis a RIPA authority must be considered. You must consider any collateral intrusion on third parties when accessing websites. You should keep details of the websites accessed, information obtained and your reasons for using the website and the information gained or for discounting it from your investigation. You must always record access to accounts as part of your investigation log.

16. If it is necessary and proportionate for the Council to covertly breach access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by the officer (ie the activity is more than mere reading of the site's content). This could occur if the officer covertly asks to become a 'friend' of someone on a social networking site.

17. CHIS authorisation is only required when using an internet trading organisation such as E-bay or Amazon Marketplace in circumstances when a covert relationship is likely to be formed. The use of disguised purchaser details in a simple, overt, electronic purchase does not require a CHIS authorisation, because no relationship is usually established at this stage. (Refer to G 5-7 above regarding the need to establish an officer for the roles of 'handler', 'controller' and 'record keeper' if a CHIS authorisation is required.)

18. See Appendix 5 – The Social Media and Networking Sites in Investigations Policy for more information

H. Authorisation Procedures

1. Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised and in strict accordance with the terms of the authorisation. Appendix 2 gives a flow chart of the authorisation process from application consideration to recording of information. Although this flow chart covers both Directed Surveillance and CHIS authorisations, remember that CHIS forms must not be completed without obtaining prior legal advice, as CHIS authorisations will be very unusual.

2. Once the Authorising officer has authorised the application, an application must be made on the correct form to the Magistrates Court for the Justice of the Peace to authorise.

Authorising Officers

3. Forms can only be signed by Authorising Officers holding a 'RIPA Authorising Officer Certificate' issued by the SRO (as shown at Appendix 3). Authorising Officer posts are listed in Appendix 1. Any Authorising Officer filling a post shown in Appendix 1 and holding such a Certificate can sign the forms.

4. Appendix 3 training will be kept up to date by the SRO and revised as necessary. If a Service Manager wishes to add, delete or substitute a post, s/he must refer such a request to the SRO for consideration. The SRO is authorised to add, delete or substitute posts listed in Appendix 1.

5. Remember that RIPA authorisation procedures are separate from powers delegated to officers under the Council's 'Schedule of Functions Delegated to Officers' (forming part of the SSDC Constitution). RIPA procedures are governed by this Guide. RIPA authorisations are for specific investigations only, and they must be renewed or cancelled once the specific surveillance is complete or about to expire. The authorisations do not lapse with time.

Training Records

6. Proper training in RIPA procedures will be given or approved by the SRO before Authorising Officers are issued with a RIPA Authorising Officer Certificate enabling them to sign RIPA forms. RIPA training already undertaken or to be undertaken will need to be verified and approved by the SRO. Instruction on RIPA procedures will be by means of a one-to-one meeting with the SRO (or his nominated representative). The issue of a RIPA Authorising Officer Certificate will be confirmation that the Authorising Officer has been properly trained in RIPA procedures. The SRO will keep a 'Central Register of Issued RIPA Authorising Officer Certificates' containing copies of Certificates issued to individual officers.

7. If the SRO considers at any time that an Authorising Officer has not fully complied with the requirements of this Guide, or is no longer properly trained in RIPA procedures or requires additional training, the SRO is duly authorised to revoke that Officer's RIPA Authorising Officer Certificate until such time as he is satisfied that the Certificate should be re-issued. SRO will need to be satisfied that the Officer concerned is a fit and proper person to be an Authorising Officer for RIPA purposes. RIPA forms cannot be signed by an officer who does not hold a RIPA Authorising Officer Certificate.

Application Forms

8. Only the current RIPA forms downloadable from the Home Office Security (Surveillance) website (and also available on the SSDC portal or from the SRO) must be used. Any other forms used after the operative date will be rejected by Authorising Officers and/or the SRO. Remember that CHIS forms must not be completed without obtaining prior legal advice, as CHIS authorisations will be very unusual. In respect of all forms, while we will do our best to ensure that the version on the intranet is the latest version, it is good practice to check the Home Office website (as above) to ensure that the SSDC version is the current version. Do not rely on the intranet/portal version being the latest version.

9. **Types of Directed Surveillance Forms**

Application for Authorisation to Carry Out Directed Surveillance
Review of a Directed Surveillance Authorisation
Application for Renewal of a Directed Surveillance Authorisation
Cancellation of Directed Surveillance Authorisation

10. **Types of CHIS Forms – not to be used without obtaining prior legal advice**

Application for Authorisation of the Conduct or Use of a CHIS
Review of CHIS Authorisation
Application for Renewal of CHIS Authorisation
Cancellation of CHIS Authorisation

11. Any boxes not needed on the form(s) must be clearly marked as being 'NOT APPLICABLE', 'N/A' or a line put through the box. Great care must also be taken to ensure that accurate information is used and inserted in the correct boxes. Reasons for any refusal of an application must also be put on or stapled to the form and the form retained for future audits. Such refusal reasons must be signed and dated by the Authorising Officer.

Grounds for Authorisation

12. Directed Surveillance or the Conduct and Use of a CHIS can be authorised by the Council only on the following ground:

- For the prevention or detection of crime or preventing disorder

12A A further condition for authorisation of Directed Surveillance (but that does not apply to CHIS authorisations) is that the Crime being investigated can only be an offence punishable on summary conviction or indictment by a maximum term of at least 6 months imprisonment or is an offence under:

i) Section 146 of the Licensing Act 2003 (sale of alcohol to children)
ii) Section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children)
iii) Section 147A of the Licensing Act 2003 (persistently selling alcohol to children)
iv) Section 7 of the Children and Young Persons Act 1933 (sale of tobacco etc to persons under eighteen).

Assessing the Application Form

13. Before an Authorising Officer signs a form, s/he must:

(a) Have regard to this Corporate Policy & Procedures Guide, the training provided or approved by the SRO and any other guidance and advice issued by the SRO on such matters generally, or the authorisation sought specifically;

(b) Satisfy his/herself that the RIPA authorisation is:

(i) in accordance with the law;
(ii) necessary in the circumstances of the particular case on the ground mentioned in paragraph 10 above; and
(iii) proportionate to what it seeks to achieve;

(c) In assessing whether or not the proposed surveillance is proportionate the authorizing officer must be satisfied that the surveillance is proportionate to the mischief under investigation, that it is proportional to the degree of anticipated intrusion on the target and others and it is the only option after considering other appropriate means of gathering the information. The least intrusive method will be considered proportionate by the courts;

(d) Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (called 'Collateral Intrusion'). Measures must be taken wherever practicable to avoid or minimise collateral intrusion as far as possible, and this issue may be an aspect of determining proportionality;

(e) Set (and diarise) a date for review of the authorisation and review on that date;

(f) Allocate a Unique Reference Number (URN) for the application as follows:

Year / Service Code (*see Appendix 1*) / Number of Application

e.g. 2006/HRB/01

(g) Ensure that the RIPA Service Register is duly completed, and that a copy of the RIPA form is forwarded for inclusion in the SRO's Central Register within 1 week of the relevant authorisation, review, renewal, cancellation or rejection.

Additional Safeguards when Authorising a CHIS

14. When authorising the conduct or use of a CHIS, the Authorising Officer must also:

(a) be satisfied that the conduct and/or use of the CHIS is proportionate to what is sought to be achieved;

(b) be satisfied that appropriate arrangements are in place for the management and overseeing of the CHIS. These arrangements must address health and safety issues by the carrying out of a formal and recorded risk assessment;

(c) consider the likely degree of intrusion for all those potentially affected;

(d) consider any adverse impact on community confidence that may result from the use or conduct of the CHIS or the information obtained; and

(e) ensure that records contain particulars of the CHIS and that they are not available except on a 'need to know' basis.

Judicial Approval

15. The judicial approval process introduced by the Protection of Freedoms Act 2012 and effective from 1st November 2012 requires that once the form has been approved by the Authorising Officer, judicial approval of a Justice of the Peace at the Magistrates Court is necessary.

The JP will decide whether a local authority grant or renewal of an authorization or notice to use RIPA should be approved and it will not come into effect unless and until it is approved by a JP. Although it is possible for local authorities to request judicial approval for the use of more than one technique at the same time, in practice, as different considerations need to be applied to different techniques, this would be difficult to perform with the degree of clarity required. As a rule authorisations or notices should be submitted separately for each different technique.

Following the authorisation or renewal of an application the Authorising Officer must forward the authorisation and supporting documents to a Legal Officer, who will liaise with the investigation officer and assist in the making of an application to the Magistrates Court for judicial approval. The forms for this application will be kept by the SRO or are found on the Home Office website.

The Legal Officer assist in obtaining a court hearing date and time and will if necessary attend court along with the Authorising Officer or the Investigating Officer whoever is the most appropriate, to give evidence of the case and the technique required.

In emergency situations applications can be made to the Court outside usual office hours, Authorising Officers are advised to refer to Appendix 4. In such cases the investigating officer will need to provide two partially completed judicial application forms so that one can be retained by the JP. The Investigating Officer will have to provide a copy of the application form signed by the authorisation officer to the court on the next working day.

A copy of the signed Judicial Application form must be retained and sent to the SRO who will place it on the central register and enter it on the spreadsheet. There is not a requirement for the JP to consider either cancellations or internal reviews.

Duration of Authorisations

16. The authorised RIPA form must be reviewed at least at monthly intervals and cancelled once it is no longer needed. The authorisation to carry out/conduct the surveillance lasts for a maximum of 3 months from authorisation for Directed Surveillance, 12 months from authorisation for a CHIS and 1 month from authorisation for a Juvenile CHIS. However, whether or not the surveillance is carried out or conducted in the relevant period has no bearing on the

authorisation becoming spent. In other words, authorised RIPA forms do not expire. The authorised forms have to be reviewed and/or cancelled once they are no longer required.

17. Authorisations can be renewed in writing before the maximum period has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred. The SRO may review the case to ensure all procedures have been followed. Renewal's must be authorised by a JP, an application being made in the way described above.

I. Working With Or Through Other Agencies

1. When another agent or agency (such as a private investigator) has been instructed by or on behalf of the Council to undertake any action under RIPA, this Guide and the appropriate RIPA forms and Judicial approval mentioned must be used by the Council officers concerned (in accordance with the normal RIPA procedures) and the agency advised and kept informed of the various RIPA requirements. They must be made explicitly aware of what they are authorised to do by means of written instructions from the instructing officer, with a copy of the written instructions countersigned by the agency by way of acknowledgement of their instructions and returned to the instructing officer to be kept on the case file. If for reasons of urgency oral instructions are initially given, written confirmation must be sent (and acknowledged) within 4 working days. Officers should be satisfied that agencies are RIPA competent and RIPA trained before they are used, and a written record of that satisfaction (and the evidence for it) must be placed on the SSDC case file.

2. When some other agency (e.g. Police, Customs & Excise, Inland Revenue etc):

   (a) wishes to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures. Before any Council officer agrees to allow the Council's resources to be used for the other agency's purposes, s/he must obtain a copy of that agency's completed RIPA form for the Council's records (a copy of which must be passed to the SRO for the Central Register), or relevant extracts from the agencies RIPA form which are sufficient for the purposes of protecting the Council and the use of its resources;

   (b) wishes to use the Council's premises for their own RIPA authorised action, the Council officer concerned should normally co-operate with such a request, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. The request must be put in writing and any consent from the Council must also be in writing. Suitable insurance or other appropriate indemnities may need to be sought from the other agency to protect the Council's legal position (the Council's Insurance Officer and/or the SRO can advise on this issue). However, in such cases the Council's own RIPA forms should not be used as the Council is only 'assisting' and not being 'involved' in the RIPA activity of the external agency.

3. With regard to 2(a) above, if the Police or other agency wish to use Council resources for general surveillance (as opposed to specific RIPA authorised operations), an appropriate letter requesting the proposed use (and detailing the nature and extent of the use, duration, who will be undertaking the general surveillance, the purpose of it, and why it is not subject to RIPA) must be obtained from the Police or other agency before any Council resources are made available for the proposed use. The insurance/indemnity considerations mentioned above may still need to be addressed.

4. **If in doubt, please consult with the SRO at the earliest opportunity.**

J. Record Management

1. The Council must keep a detailed record of all authorisations, renewals, cancellations and rejections generated by Services and a Central Register of all authorisation forms will be maintained and monitored by the SRO.

2. ***Records maintained in the individual Service***

   The following documents must be retained by the relevant Service Manager or his/her designated RIPA Service Co-ordinator (such Co-ordinator to be appointed by the Service Manager and the name notified to the SRO) retention must be in accordance with the date retention policy. These will be retained in electronic file format.

   - Copies of any completed application form together with any supplementary documentation, plus notification of the approval given by the Authorising Officer;
   - A copy of the signed Judicial Approval;
   - a record of the period over which the surveillance has taken place;
   - the frequency of reviews prescribed by the Authorising Officer;
   - a record of the result of each review of the authorisation;
   - a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
   - a copy of any cancellation of an authorisation;
   - the date and time when any instruction was given by the Authorising Officer and a note of that instruction;
   - the Unique Reference Number for the authorisation (URN).

3. Each form will have a URN. The Service Manager or RIPA Service Co-ordinator will issue the relevant URN to applicants. The cross-referencing of each URN takes place within the forms for audit purposes. The relevant Service code to be followed is shown in Appendix 1. Rejected forms will also have URN's.

4. A 'Surveillance Log Book' will be completed by the investigating officer(s) to record all operational details of authorised covert surveillance. Once completed, the Log Book will be passed to the Service Manager or the designated RIPA Service Co-ordinator for safe keeping in a secure place. Each Service will also maintain a 'Surveillance Log Book Issue and Movement Register' for such Surveillance Log Books. The maintenance of the latter Register will be the responsibility of the Service Manager or the designated RIPA Service Co-ordinator. The SRO will prescribe the form of the latter Registers and Services must substantially follow that form.

Central Register maintained by the SRO

5. Authorising Officers must forward details of each issued RIPA form to the SRO for keeping on the Central Register within 1 week of the issue of the authorisation, review, renewal, cancellation or rejection. The SRO will monitor

forms, give appropriate guidance from time to time, and amend this Guide, as necessary.

6. The Council will retain records for a period of at least three years from the ending of the authorisation. The Service Manager or RIPA Service Co Ordinator will ensure that only one copy of the relevant documents of a RIPA authority and the evidence resulting from it is kept on file for the relevant case and the SRO will keep on copy on file in the central register until it requires destruction. The Investigatory Powers Commissioner's Office (IPCO) can audit and review the Council's policies and procedures, and individual authorisations.

K. Concluding Remarks of the SRO

1. Where there is an interference with a European Convention right such as the right to respect for private and family life guaranteed under Article 8 of Convention, and where there is no other source of lawful authority for the interference, or if it is held to be unnecessary and disproportionate in the particular circumstances, the consequences of not obtaining or not following the correct authorisation procedures set out in RIPA, RIPA Regulations and associated Codes of Practice may be that the action taken (and the evidence obtained) will be held by a court to be an infringement of a Convention right (possibly more than one) and thus unlawful behaviour under Section 6 of the Human Rights Act 1998. This could result in the Council losing a case and having costs (and possibly damages) awarded against it. Following this Guide should ensure that this does not happen.

2. It needs to be stressed that the concept of proportionality, i.e. proportional action, is very important under RIPA and under human rights. Action that is disproportionate in terms of the end to be achieved when judged against the Convention right infringed will be unlawful, even if a RIPA authorisation has been issued. Therefore, it is probably best to err on the side of caution when considering if covert surveillance is really required for an investigation. If the information can be obtained by other overt means, then it should be. Ask yourself the question: “Do I really need to do this, what will be the effect on others if I do it, and is there any other way to achieve the same ends?” Weigh it all in the balance. If possible, do a file note of your reasoning.

3. Authorising Officers must exercise their minds as to their RIPA obligations every time they are asked to sign a form. They must never sign or rubber stamp form(s) without thinking about both their personal responsibilities and the Council's responsibilities under RIPA, the Human Rights Act 1998 and the European Convention. Again, ask yourself the question: “Do I really need to do this, what will be the effect on others if I do it and is there any other way to achieve the same ends?” Weigh it all in the balance. If possible, do a file note of your reasoning.

Definition of Roles

(1) SRO – Senior Responsible Officer

Director Service Delivery, maintains central records of authorisations and collating the authorisations, reviews, renewals and cancellations they also have oversight of submitted RIPA documents. Is responsible for – integrity of the process, compliance with RIPA and its regulatory framework, engage with the Commissioners and Inspectors when they conduct an inspection, oversee the implementation of recommendations made by the IPCO to ensure authorising officers are of the appropriate standard

(2) RIPA Co-ordinating Officer

Specialist Legal, maintains Policy and Procedure, Organises training and raises awareness.

(3) RIPA Authorising Officer

Is certified to authorise applications before referral to the Magistrates Court.

(4) RIPA Services Co-ordinating Officer

Officer in relevant service who ensures relevant RIPA documents are retained and destroyed according to the Council's Policies.

(5) CHIS Controller

Officer appointed in relevant service on a case by case basis – responsible for the management and supervision of the handler and has oversight of the use of the CHIS

(6) CHIS Handler and Record Keeper

Officer appointed in relevant service on a case by case basis of rank below authorising officer to deal with day to day activities of the CHIS, recording information supplied and monitoring security and welfare of the CHIS

4. For further advice and assistance on RIPA, please contact the SRO. Contact details are provided at the front of this Guide.

APPENDIX 1

List of Authorising Officer Posts

Post	Service Identifier
Lead Specialist Legal	**LSM**
Director Commercial Services and Income Generation	**DCSIG**
Director of Strategy and Commissioning	**DSC**
Specialist Services Manager	**SSM**
Director Service Delivery	**DSD**

IMPORTANT NOTES

A. Even if a post is identified in the above list, the persons currently employed in such posts are not authorised to sign RIPA forms (including a renewal or cancellation) unless s/he has been certified by the SRO to do so by the issue of a RIPA Authorising Officer Certificate.

B. Only the Chief Executive and the head of Paid services are authorised to sign forms relating to Juvenile Sources and Vulnerable Individuals (see paragraph G of this Guide).

C. If a Service Manager wishes to add, delete or substitute a post, s/he must refer such request to the SRO for consideration.

D. If in doubt, ask the SRO BEFORE any directed surveillance and/or CHIS is authorised, renewed, rejected or cancelled.

APPENDIX 2

RIPA FLOW CHART

Requesting Officer ('The Applicant')must:

- Read the RIPA Corporate Policy & Procedures Guide and be aware of any other guidance issued by the SRO
- Determine that directed surveillance and/or a CHIS is required.
- Assess whether authorisation will be in accordance with the law. Assess whether authorisation is necessary under RIPA and whether the surveillance could be done overtly.
- Very importantly, consider whether surveillance will be proportionate.
- If authorisation is approved - review regularly

If a less intrusive option is available and practicable **use that option!**

If authorisation is necessary and proportionate, prepare and submit an approved form to the Authorisation Officer

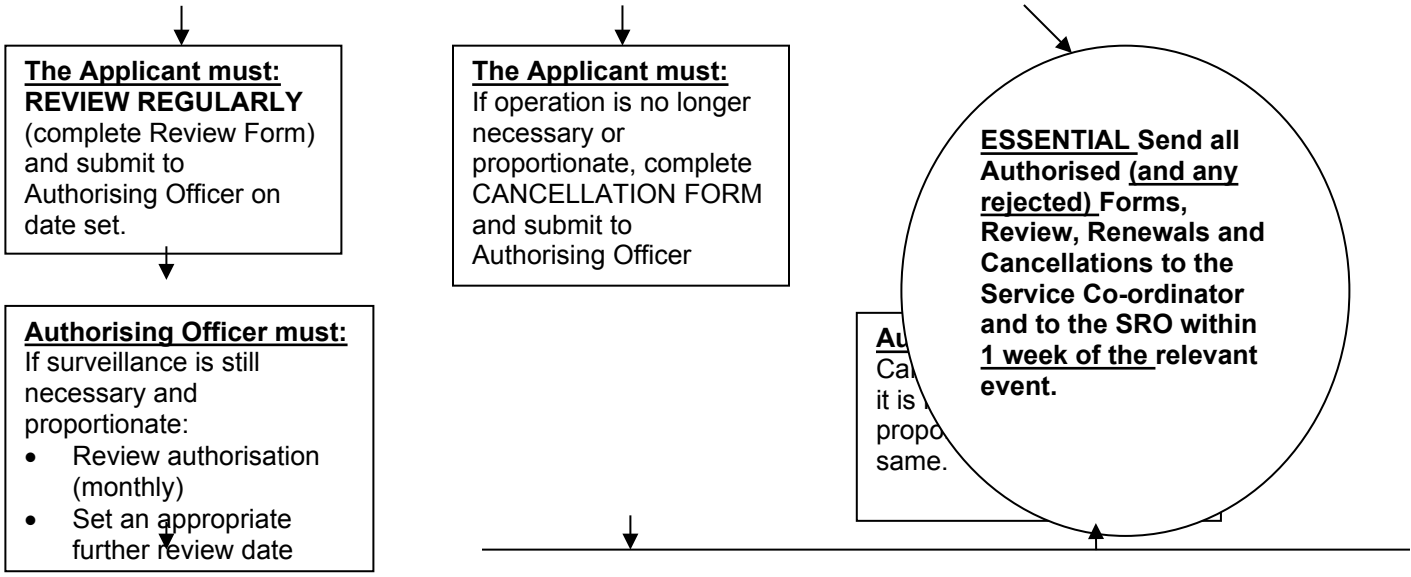
Authorising Officer must:

- Consider in detail whether all options have been duly considered, including the RIPA Corporate Policy & Procedures Guide and any other guidance issued by the SRO.
- Consider whether surveillance is considered by him/her to be necessary and proportionate.
- Authorise only if an overt or less intrusive option is not practicable.
- Set an appropriate review date (can be up to 3 months after Authorisation date) and conduct the review.

SRO to review the case to ensure procedures followed before seeking Judicial Approval

Judicial Approval

- Authorising officer refers to Legal Officer
- Court hearing – AO or applicant to attend (Legal Officer if necessary)
- Justice of the Peace consider all documents – authorise



NB: If in doubt, ask the SRO BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled, or rejected. Appropriate Managers will designate one of their staff to be a Service Co-ordinator for the purpose of RIPA and advise the SRO accordingly. CHIS forms are not to be used without prior legal advice.

APPENDIX 3

SOUTH SOMERSET DISTRICT COUNCIL

RIPA AUTHORISING OFFICER CERTIFICATE
No. [ ] / 20

I HEREBY CERTIFY that the Officer whose personal details are given below is an Authorising Officer for the purposes of authorising covert surveillance and the use and/or conduct of Covert Human Intelligence Sources ('CHIS') under the provisions of the Regulation of Investigatory Powers Act 2000.

It is further certified that this Officer has received training to perform such authorisation procedures.

Certificate issued to: [Full name of Officer]

Job Title:

Service:

Location:

Certificate date:

(signed) .....
Martin Woods
Senior Responsible Officer
Director Place
South Somerset District Council

(**PLEASE NOTE**: This certificate and the authorisation granted by it is personal to the officer named in it and cannot be transferred. Any change in personal details must be notified in writing to the SRO immediately. This certificate can be revoked at any time by the Director of Service Delivery by written revocation issued to the officer concerned. It is the named officer's personal responsibility to ensure full compliance with RIPA authorisation procedures and to ensure that s/he is fully trained in such procedures and that such training is kept up to date).

MAGISTRATES' COURTS IN AVON AND SOMERSET OTHER THAN BRISTOL

Procedure for dealing with Applications/Warrants out-of-hours

i.e. between: 5pm and 8.30 am Mondays – Thursdays
5pm on Friday and 8.30am Monday
Bank Holidays
(but please note the at the Magistrates Court sits at Bristol and Taunton on Saturdays and Bank Holidays at 10am and where possible applications should be made to the Court rather than using the Out of Hours procedures on these days)

PLEASE MAKE EVERY EFFORT TO RESTRICT APPLICATIONS TO THOSE OF EXTREME URGENCY. NON URGENT APPLICATIONS MAY NEED TO BE REFUSED.

APPLICATIONS BY OTHER AGENCIES

- **Agencies may only make contact with a Legal Adviser via the Avon and Somerset Constabulary Force Control Inspector Telephone 08454 567000**
- Force Control Inspector/his staff shall contact a Legal Adviser working in the area where the application is sough giving contact details of the agency to enable the Legal Adviser to contact the person requesting the warrant/making the application under the Children Act 1989. **Agency staff must not retain any contact details.**
- Where the officer is unable to contact a legal adviser in his/her area, he/she should make contact with a Legal Adviser in nearest proximity.
- The person making the application/requesting the warrant will give the Legal Adviser a summary of the nature of the application and its urgency.
- Legal Adviser then to make contact with a Magistrate who is able to hear the application.
- Arrangements to be agreed between the Legal Adviser and the agency regarding the venue and time the application to be heard.
- Agency staff may be required to collect the Legal Adviser from his/her home address and then go to the Magistrates home, returning the Legal Adviser thereafter. The Legal Adviser will have the discretion to make other arrangements where the need arises.
- Applications under the children Act 1989: The list of Legal Advisers states who can deal with these applications. (Only Legal Advisers with delegated powers are able to deal with applications for emergency process under Part IV of the Children Act, 1989). Please direct the application in the first instance to a Legal Adviser working in the area where order sought.