MENDIP DISTRICT COUNCIL

GOVERNANCE, ASSETS AND PUBLIC SPACES

CORPORATE POLICIES AND PROCEDURES ON THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

Author:	**Donna Nolan**
Document Name:	**RIPA Policy**
Document Number:	**~~V5~~ V6**
Effective Date:	**~~12 October 2015~~**
Date due for review:	**~~12 October 2016~~**
Responsible for review:	**Donna Nolan**
Version:	**~~V5~~ V6**

Version control

Number	Effective Date	Author / Reviewer	Comments (e.g. details of any policies being replaced)
V1	18.02.08		Superseded by this version
V2	09.07.12	Ann Higgins	Updates previous policy
V3		Ann Higgins	Updates previous policy
V4	24.02.14	Ann Higgins/Lesley Dolan	Updates previous policy
V5	29.09.15	Lesley Dolan	Updates previous policy
V6	29.03.16	Lesley Dolan	Updates previous policy

Dissemination

Name or Team	Method	Date	Version
Legal	Email	26.06.12	V6~~V5~~
CMT			~~V5~~V6
Cabinet	Report	~~12.10.15~~11.04.16	~~V5~~V6

Publication of current version

	Location	Date of Publication
	SharePoint	
	SharePoint	

Approvals for current version

Name	Date of Approval
Corporate Management Team	
Cabinet	~~12.10.15~~
Council	~~22.10.15~~

CONTENTS

APPENDICES

(A) FORMS

(B) OTHER APPENDICES

Home Office Codes of Practice *A: Covert Surveillance & B: Covert Human Intelligence Sources – can be accessed through direct link at 1.6 below.*

Under Article 8 of the European Convention on Human Rights, there shall be no interference by a public authority with the rights of an individual in respect of their private and family life except as in accordance with the law.

Under the Human Rights Act 1998 the Council is obliged not to act in any way which is incompatible with any convention right under the European Convention on Human Rights.

The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the carrying out of covert surveillance and the use of covert human intelligence sources.

1. INTRODUCTION

1.1 This document sets out the policies and procedures adopted by Mendip District Council ("the Council") in relation to the Regulation of Investigatory Powers Act 2000 ("RIPA"). RIPA regulates the Council's powers to use covert surveillance and covert human intelligence sources ("CHIS") in carrying out its functions. Under RIPA, the Council must have procedures in place that ensure surveillance is properly authorised, with full consideration given to the necessity and proportionality of the covert surveillance or CHIS in the context of individuals' rights under the Human Rights Act 1998 ("the HRA") and other relevant legislation. The policies and procedures set out in this document are based on the provisions of RIPA, the Home Office Codes of Practice on Covert Surveillance and Property Interference and Covert Human Intelligence Sources and guidance issued by the Office of the Surveillance Commissioner.

1.2 The HRA requires the Council and any organisations working on its behalf to respect the private life and family of citizens, their home and their correspondence. This is not an absolute right, but interference will only be justified if it is:-

a) in accordance with the law,
b) necessary, for one of the purposes defined in the HRA, and
c) proportionate to what is sought to be achieved.

1.3 The Council may need to make use of covert surveillance or CHIS in relation to planning enforcement, environmental health, fraud investigation, anti-social behaviour or in connection with other functions. However, covert surveillance will normally be a last resort in an investigation, and use of a CHIS by the Council is likely to be very rare. These activities will only be undertaken where there is no reasonable and less intrusive means of obtaining the information.

1.4 Any covert surveillance or use of a CHIS by or on behalf of the Council must be carried out in accordance with these policies and procedures, and must be authorised in advance by one of the AOs ("AOs") identified in Appendix 9 on the appropriate form (see Appendices 1-8). Both staff directly employed by the Council and external agencies working for the Council are subject to RIPA whilst they are working for the Council in a relevant investigatory capacity.

1.5 Compliance with the provisions of RIPA, the Home Office Codes of Practice and these policies and procedures should protect the Council, its officers and agencies working on its behalf against legal challenge.

Section 27 of RIPA states that: "conduct…shall be lawful for all purposes if an authorisation…confers an entitlement to engage in that conduct on the person whose conduct it is and his conduct is in accordance with the authorisation".

If correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman, and/or the Council

could be ordered to pay compensation. Such action would not, of course, promote the good reputation of the Council and would, undoubtedly, be the subject of adverse press and media interest. It is essential, therefore, that all involved with RIPA comply with this document and any further guidance that may be issued, from time to time, by the ~~Monitoring Officer~~Senior Responsible Officer.

1.6 In addition to setting out the procedures that must be followed, this document aims to provide guidance to officers about the circumstances in which they are permitted to embark on covert surveillance or use a CHIS. The forms set out in the Appendices contain relevant guidance notes; however, officers are encouraged to contact the ~~Monitoring Officer~~Senior Responsible Officer ~~–~~or the ~~Deputy Monitoring~~ RIPA Co-ordinating Officer for advice or assistance if required. Useful guidance can also be found via the web-sites of the Office of Surveillance Commissioners at Office of Surveillance Commissioners - Home and the Home Office RIPA web-site at Home Office | The new RIPA website.

1.7 Appropriate training will be arranged at regular intervals for all officers likely to make applications or authorise them. Corporate Managers should ensure that they and all relevant members of their staff undertake this training and that appropriate records are kept.

1.8 It is important to keep full records of all applications and authorisations relating to activities covered by RIPA, in accordance with the requirements of the relevant Codes of Practice and the procedures set out in this document.

2. THE SCOPE OF RIPA AND TYPES OF SURVEILLANCE

2.1 Officers should be aware of the scope and extent of activities covered by the provisions of RIPA. In many cases, investigations carried out by Council officers will not be subject to RIPA, as they involve overt rather than covert surveillance (see below).

2.1 RIPA **does**:

- require prior authorisation of directed covert 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.

2.3 RIPA **does not**:

- make unlawful conduct which is otherwise lawful.
- prejudice or dis-apply any existing powers available to the Council to obtain information by any means not involving conduct requiring authorisation under RIPA. For example, it does not affect the Council's current powers to obtain information via the DVLA or from the Land Registry as to the ownership of a property.

2.4 **'Surveillance'** includes

- monitoring, observing, listening to people, watching or following their movements, listening to their conversations and other such activities or communications.
- recording anything mentioned above in the course of authorised surveillance.
- surveillance by, or with the assistance of, appropriate surveillance device(s).

Surveillance can be overt or covert.

2.5 **Overt surveillance** will include most of the surveillance carried out by the Council - there will be nothing secretive, clandestine or hidden about it. For example, signposted CCTV

cameras normally amount to overt surveillance (but see 2.11 below). 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), and/or will be going about Council business openly (e.g. a car parks inspector walking through a Council car park).

2.6 Similarly, surveillance will be overt if the subject has been told it will happen. This will be the case where a noisemaker is warned that noise will be recorded if the noise continues; or where a licence for regulated entertainment is issued subject to conditions, and the licensee is told that officers may visit without notice or without identifying themselves to the owner/ licensee to check that the conditions are being met. Such warnings should be given to the person(s) concerned in writing and should state for how long the warning shall remain in place. The duration of a warning will be determined on a case by case basis after due consideration of all of the surrounding circumstances of the particular case.

2.7 Overt surveillance does not require any authorisation under RIPA. Neither does **low-level surveillance** consisting of general observations in the course of law enforcement (for example, where a planning officer drives past a site to check whether planning conditions are being complied with.) Repeated visits may amount to systematic, and therefore, directed surveillance and require authorisation: if in doubt, legal advice should be sought. The Office of Surveillance Commissioners guidance suggests that the use of equipment such as binoculars or cameras will be intrusive if it consistently provides information of the same quality as might be expected to be obtained from a device actually present on the premises or in the vehicle concerned. It is, therefore, the quality of the image obtained rather than the duration of the observation that is determinative as to whether or not an authorisation should be obtained.

2.8 **Covert surveillance** is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place.

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

2.9 **Directed surveillance** is surveillance which:-

- is covert; and
- is not intrusive surveillance (see definition below - **the Council is prohibited by law from carrying out any intrusive surveillance**);
- is not carried out in an immediate response to events which would otherwise make seeking authorization under RIPA unreasonable e.g. Spotting something suspicious 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).

Crime Threshold

Directed surveillance may only be used for criminal offences which meet the following criteria:
• The criminal offence is punishable by a maximum term of at least 6 months imprisonment, or
• Would constitute an offence under sections 146, 147, or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1993 (offences involving sale of tobacco and alcohol to underage children) regardless of length of prison term.

The Crime threshold only applies to Directed Surveillance, not to CHIS or Communications Data.

2.10 **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. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others that s/he comes into contact or associates with.

2.11 Similarly, although signposted town centre CCTV cameras do not normally require authorisation, this will be required if the camera is tasked for a specific purpose which involves prolonged surveillance on a particular person. (See Section 10 for guidance on the authorisation of directed surveillance undertaken by means of the Council's CCTV cameras.)

2.12 Other examples of directed surveillance include:

- officers following an individual over a period to establish whether s/he is working whilst claiming benefit
- test purchases where a hidden camera or other recording device is used

2.13 Surveillance that is unforeseen and undertaken as **an immediate response** to a situation normally falls outside the definition of directed surveillance and therefore authorisation is not required. However, if a specific investigation or operation is subsequently to follow, authorisation must be obtained in the usual way before it can commence. In no circumstance will any covert surveillance operation be given backdated authorisation after it has commenced.

2.14 For the avoidance of doubt, only those officers designated and certified to be 'AOs' for the purpose of RIPA can authorise 'Directed Surveillance' IF AND ONLY IF, the RIPA authorisation procedures detailed in this document are followed. If an AO has not been 'certified' for the purposes of RIPA, s/he CAN NOT carry out or approve/reject any action set out in this document.

Legal Privilege and Confidential Information

Particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Applications in which the surveillance is likely to result in the acquisition of confidential material will be approved only in exceptional and compelling circumstances. High regard must be had to the proportionality of such surveillance.

If the Requesting Officer or AO considers that confidential information may be obtained as a result of surveillance, advice should be sought in advance of any authorisation ~~[INSERT].~~from the Senior Responsible Officer or the RIPA Co-ordinating Officer.

"Confidential Information" is defined for the purposes of RIPA as: -

- matters subject to legal privilege, for example, communications between legal advisers and their clients
- confidential personal information, for example. Information about someone's health or spiritual counselling or other assistance given or to be given to them or
- confidential journalistic material (this includes related communications), that is, material obtained or acquired

The fullest consideration must be given to any cases where the subject of the surveillance might reasonably expect a high degree of privacy.

Directed surveillance that is carried out of legal consultation on certain premises including prisons, police stations, courts and premises of a professional legal advisor will be treated as intrusive surveillance irrespective of whether legal privilege applies

2.15 **Intrusive Surveillance** occurs when surveillance:

- is covert;
- relates to 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 they were in the premises/vehicle.

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

3. COVERT HUMAN INTELLIGENCE SOURCES

3.1 The use of a covert human intelligence source (CHIS), and his or her conduct, also requires authorisation under RIPA. The Council is only likely to use a CHIS under very exceptional circumstances, and advice should be sought from the ~~Monitoring~~ Senior Responsible Officer or the ~~Deputy Monitoring~~ RIPA Co-ordinating Officer before any authorisation is applied for or granted.

3.2 A CHIS is defined as someone who establishes or maintains a personal or other relationship for the purpose of

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

where the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of its purpose.

These provisions would cover the use of professional witnesses to obtain evidence or information, or officers operating “undercover”. Great caution should be exercised in these circumstances, and further advice sought.

3.3 The provisions of RIPA relating to CHIS do not apply:

- where members of the public volunteer information to the Council as part of their normal civic duties;
- where the public contact telephone numbers set up by the Council to receive information;
- where test purchases are carried out in the normal course of business (i.e. does not include developing a relationship with the relevant individuals and no covert recording is used);
- where members of the public are asked to keep diaries of incidents in relation to planning enforcement or anti-social behaviour;

as none of these situations normally require a relationship to be established for the covert purpose of obtaining information.

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

- **Conduct** of a CHIS = 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 = Actions inducing, asking, or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

Confidential Information

Where through the use or conduct of a CHIS it is likely that knowledge of legally privileged material or other confidential information will be acquired, the deployment of the CHIS must be authorised by the Head of Paid Service, who is the Chief Executive, or in his absence the person acting as the Chief Executive.

Where any Confidential Information or legally privileged material has been acquired and retained, the matter should be reported to the relevant Commissioner or Inspector during their next inspection and the material be made available to him if requested

3.5 Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 years of age).

Written parental consent must be obtained prior to authorization. The duration of any authorisation is a maximum of one month from the time of grant or renewal. The Authorising Officer must be the Chief Executive or in his absence the person acting as the Chief Executive.

Where consideration is being given to the use of a CHIS under the age of 18 the AO will need to be satisfied that the special provisions contained within the Regulation of Investigatory Powers (Juveniles) Order 2010.

On no account can a child under 16 years of age be authorised to give information against his or her parents or any person who has parental responsibility for them.

Similar safeguards also apply to the use of vulnerable individuals as sources. Where it is suspected that an individual may be vulnerable they should only be authorised to act as a CHIS in the most exceptional circumstances and the AO must be the Chief Executive. (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.)

Further advice must be sought from the ~~Monitoring~~ Senior Responsible Officer or the ~~Deputy Monitoring~~ RIPA Co-ordinating Officer before using juveniles or vulnerable individuals as sources, to ensure that all necessary legal requirements are complied with.

3.6 There are also specific legal rules which must be followed in relation to the management of sources. Details are given in the relevant Home Office Code of Practice, and further advice can be obtained from the ~~Monitoring~~ Senior Responsible Officer or the ~~Deputy Monitoring~~ RIPA Co-ordinating Officer.

Online Covert Surveillance

The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. Where the Council intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion.

Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought as set out elsewhere in this policy. Where an investigator may need to communicate covertly online, for example, contacting individuals using social media websites, a CHIS authorisation should be considered.

4. AUTHORISATION PROCEDURES

4.1 **Any directed surveillance or the use of a CHIS undertaken by or on behalf of the Council must be carried out in accordance with RIPA and must not commence until authorisation has been granted.**

Only those officers employed in the designated "Authorised Officer Posts" set out in Appendix 9 can authorise directed surveillance or the conduct or use of a CHIS. Officers holding the posts set out in Appendix 9 are referred to as "Authorised Officers" ("AOs") in this document and are "designated officers" within the terms of RIPA.

4.2 The procedure for making and granting authorisations is shown in the flow-chart in Appendix 10. Officers are advised to discuss the need to undertake directed surveillance or the use of a CHIS with their team manager before seeking an authorisation. All other reasonable and less intrusive options to gain the required information should be considered before an authorisation is applied for.

4.3 Before submitting an application for authorisation, the Investigating Officer must firstly telephone the RIPA ~~Coordinator~~Co-ordinating Officer, in ~~Legal Services~~Law & Governance, who will issue a Unique Reference Number ("URN"). This should be in the form:

Year/Group/Team/Number of Application.

Any subsequent forms (e.g. renewals or cancellations) relating to the same investigation or operation should be identified by means of the same URN.

AO's should not authorise any application which does not feature an URN, unless they are being asked to verbally authorise an urgent application out of normal office hours.

4.4 The RIPA ~~Coordinator~~ Co-ordinating Officer will require the following information from the Investigating Officer when issuing a URN:

- Type of activity
- Identity of subjects (if known)
- Location of camera (if identity of subjects not known)
- Name of Investigating Officer and Team
- Ward where surveillance is likely to take place
- AO to whom the application will be submitted

When issuing the URN, the RIPA ~~Coordinator~~ Co-ordinating Officer will provide advice to the Investigating Officer in relation to the activity to be authorised including any issues of necessity, proportionality and collateral intrusion.

4.5 All applications for authorisation must be made on the appropriate form as set out in Appendices 1-8. Guidance on completing the forms is included in the Appendices, but in the event of any query, officers making or authorising applications should consult the ~~Monitoring~~ Senior Responsible Officer~~, the Deputy Monitoring Officer~~ or the RIPA ~~Coordinator~~ Co-ordinating Officer in ~~Legal Services~~Law & Governance.

The application for directed surveillance authorisation should describe any conduct to be authorised and the purpose of the investigation or operation. The application should also include:

- the reasons why the authorisation is necessary in the particular case and the grounds.
- The nature of the surveillance
- The identities, where known, of those to be the subject of the surveillance;
- A summary of the intelligence case
- An explanation of the information which it is desired to obtain as a result of the surveillance;
- The details of any potential collateral intrusion and why the intrusion is justified and measures that will be taken to avoid or minimise it;
- The details of any confidential information that is likely to be obtained as a consequence;
- The reasons why the surveillance is considered proportionate to what it seeks to achieve;
- The level of authority required for the surveillance; and
- Record of whether authorisation was given or refused, by whom and the time and date
- The URN

4.6 The application will then be made to an AO, other than an AO in the Group covering their service area. However, each of the AOs can authorise applications, renewals and cancellations, and undertake reviews, in relation to any investigation carried out, or proposed to be carried out, by officers from any other Group, if the relevant AO is unable to do so. **AOs may not sub-delegate their powers in relation to RIPA to other officers.**

4.7 AOs should not authorise directed surveillance or the use of a CHIS in respect of an investigation in which they are the Corporate Manager accountable.

4.8 In any case where it is likely that **confidential information** may be acquired by the use of a CHIS or it involves a juvenile or vulnerable person , **the only AO who may grant authorisation is the Head of Paid Service, who is the Chief Executive, or in his absence the person acting as the Chief Executive.**

4.9 When considering an application, AOs must:

(a) have regard to the contents of this document, the training provided on RIPA and any other guidance or advice given by the ~~Monitoring~~ Senior Responsible Officer or the ~~Deputy Monitoring~~ RIPA Co-ordinating Officer;

(b) satisfy his/herself that the RIPA authorisation will be:

(i) **in accordance with the law**;

(ii) **necessary** in the circumstances of the particular case for the purpose mentioned in Section 4.6 above; and
(iii) **proportionate** to what it seeks to achieve.

(c) In assessing whether or not the proposed surveillance is proportionate, the AO must consider:

- Is the proposed conduct and use necessary for the prevention of crime or the prevention of disorder.
- How will the activity bring a benefit to the investigation
- Is the size and scope of the proposed activity balanced against the gravity and extent of the perceived crime or offence;
- how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- Is the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented. (the least intrusive means of obtaining the necessary information should always be preferred);

(d) take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (called 'collateral intrusion'), and consider whether any measures should be taken to avoid or minimise collateral intrusion as far as possible (the degree of likely collateral intrusion will also be relevant to assessing whether the proposed surveillance is proportionate);

(e) consider any issues which may arise in relation to the health and safety of Council employees and agents, and ensure that a risk assessment has been undertaken if appropriate.

4.12 When authorising the conduct or use of a CHIS, the AO must also:

(a) Ensure that the following arrangements are in place at all times in relation to the use of a CHIS:

a. There will be an appropriate officer of the Council who has day-to-day responsibility for dealing with the CHIS, and for the security and welfare of the CHIS
b. There will be a second appropriate officer to monitor ~~of~~ the use made of the CHIS, and who will have responsibility for maintain a record of this use. These records must include information prescribed by the Regulation of Investigatory Powers (Source Records) Regulations 2000.

(b) be satisfied that appropriate arrangements are in place for the management and oversight 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 the required particulars of the CHIS and that these are not available except on a 'need to know' basis.

AOs should consult the ~~Monitoring~~ Senior Responsible Officer or the ~~Deputy Monitoring~~ RIPA Co-ordinating Officer before authorising the use of conduct of a CHIS to ensure that all legal requirements are complied with.

4.13 The AO must record a clear description of what authority is being granted for by reference to subjects, property or location and the type of surveillance permitted. This may not be the same as what is being requested.

4.14 If an application is authorised, the AO must set a date for its review, and ensure that it is reviewed on that date (see 6.2 below). An appropriate diary method should be created by the AO and the Investigating Officer in order to ensure all deadlines and review dates are identified.

Records must be kept in relation to all RIPA applications and authorisations in accordance with Section 7 below.

Magistrates' Court

After the authorisation form has been countersigned by the Authorising Officer the Council is required to obtain judicial approval for the authorisation or a renewal of an authorisation.

The AO should provide the original authorisation form, a copy for court and a partially completed judicial application form.

The AO must obtain advice from the ~~Democratic Services Legal~~ Law & Governance Team and ensure that the appropriate person compiles and submits the court application. Since the hearing is a legal proceeding the officer will need to be formally designated to appear, be sworn in and present evidence or provide information as required.

5. URGENT AUTHORISATIONS

5.1 ~~Urgent authorisations can no longer be authorised orally.~~ Approval for directed surveillance in an emergency must be obtained in written form and be signed off by a Magistrates Court.

If the application is sought out of hours then the AO or Investigating Officer will need to contact the out of hours HMCTS representative to seek approval from a Magistrate.

6. DURATION OF AUTHORISATIONS

6.1 Authorisations will have effect from the date and time of the granting of approval by the Magistrates Court. They are granted for a period of three months for directed surveillance and for a period of twelve months for the use or conduct of a CHIS. Authorisations should be either renewed or cancelled and should not be left or simply expire. **No further operations should be carried out after the expiry of the relevant authorisation unless it has been renewed.**

It will be the responsibility of the Investigating Officer to ensure that any directed surveillance or use of a CHIS is only undertaken under an appropriate and valid authorisation, and therefore, he/she should be mindful of the date when authorisations and renewals will cease to have effect. The ~~Monitoring~~ Senior Responsible Officer will perform an auditing role in this respect **but the primary responsibility rests with the AO.**

6.2 Authorisations should be reviewed at appropriate intervals, as set by the AO. Reviews should normally take place on a monthly basis unless the AO considers that they should take place more or less frequently (if so, the reasons should be recorded). If the surveillance provides access to confidential information or involves collateral intrusion, there will be a particular need to review the authorisation frequently. The results of reviews should be recorded on the appropriate form as set out in Appendices 2 and 6.

Cancellation

6.3 Authorisations must be cancelled as soon as they are no longer necessary. **Even if an authorisation has reached its time limit and has ceased to have effect, it does not lapse and must still be formally cancelled.**

The responsibility to ensure that authorisations are cancelled rests primarily with the Investigating Officer, who should submit Cancellation Form

However, if the AO who authorised any directed surveillance or the use or conduct of a CHIS (or any AO who has taken over their duties) is satisfied that it no longer meets the criteria upon which it was authorised, s/he must cancel it and record that fact in writing even in the absence of any request for cancellation.

~~6.4 An urgent oral authorisation (if not already ratified in a written authorisation) will cease to have effect after 72 hours, beginning with the time of authorisation.~~

Renewals

If, at any time before any other directed surveillance *authorisation* would cease to have effect, the *authorising officer* considers it necessary for the *authorisation* to continue for the purpose for which it was given, he or she may renew it in writing for a further period of three months.

6.5 Authorisations shall be renewed in writing. Applications for renewal An *application* for renewal should not be made until shortly before the *authorisation* period is drawing to an end but should be made on the appropriate form in good time (at least seven working days if possible) before the authorisation is due to expire. The AO must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred. Renewals of an authorisation may be granted more than once, provided the criteria for granting that authorisation are still met. However, if the reason for requiring the authorisation has changed from the purpose for which it was originally granted, then it should be cancelled and new authorisation sought.

6.6 The renewal will begin on the day when the authorisation would otherwise have expired. Renewed authorisations will normally be for a period of up to 3 months for covert directed surveillance, 12 months in the case of CHIS and 1 month in the case of juvenile CHIS.

All renewals will require an order of the Magistrates Court.

7. PROCEDURE FOR MONITORING RIPA AND OVERSIGHT

7.1 Senior Responsible Officer (SRO)

7.1.1 The Council's Monitoring Officer will be the designated ~~SRO~~ Senior Responsible Officer and shall be responsible for the following:-

- the integrity of the process in place within the Council to authorise Directed Surveillance;

- compliance with Part II of RIPA 2000 and any associated Codes of Practice;
- acting as liaison with the Commissioners and Inspectors and engaging with them as appropriate;
- overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner.

7.1.2 The ~~SRO~~ Senior Responsible Officer shall ensure that all AOs are provided with copies of current and updated Codes of Practice and OSC Guidance and Procedure Notes as they are released from time to time.

7.1.3 The ~~SRO~~ RIPA Co-ordinating Officer shall maintain a Central Record of Authorisations.

7.1.4 The ~~Deputy Monitoring Officer~~ RIPA Co-ordinating Officer will assist the ~~SRO~~ Senior Responsible Officer in undertaking the tasks as specified above.

7.2 Oversight Procedures

7.2.1 The SRO shall establish and maintain regular meetings not less than [twice] a year with the AOs to check and test processes and address any training requirements. These meetings shall form part of the Corporate Management Team business. The SRO shall arrange an oversight meeting as soon as practicable following an inspection to discuss issues and outcomes as appropriate.

7.2.2 The SRO shall record any issues arising out of authorisation applications, the statutory considerations, reviews and cancellations and shall review the quality of authorisations granted from time to time.

7.2.3 The SRO shall carry out analysis of such issues and shall decide appropriate feedback to the AO. Such information and conclusions shall also inform the reports to Cabinet required under paragraph 10.3 below.

7.3 ~~Member Review~~

~~The members of the Council's Cabinet shall review the use of RIPA 2000 and this policy at least once a year. In order to facilitate this, the SRO shall provide bi-annual reports to Cabinet meetings on how RIPA 2000 has been used in the previous six months and whether there are any concerns as to the policy.~~

7.3 RIPA – Co-ordinating Officer

The RIPA Co-ordinating Officer is nominated by the SRO to be responsible for day to day matters such as training and awareness, oversight of authorisations and keeping records, including a centrally retrievable record of authorisations.

7.4 Member Review

Formatted: Font: Bold

Formatted: Font: Bold

~~The members of the Council's Cabinet shall review the use of RIPA 2000 and this policy at least once a year. In order to facilitate this, the SRO shall provide bi-annual reports to Cabinet meetings on how RIPA 2000 has been used in the previous six months and whether there are any concerns as to the policy.~~

The SRO will provide an annual report to be taken to Scrutiny/Cabinet in May each year with an interim report to be taken annually in December. The reports will cover how RIPA

200 has been used in the previous 6 months and whether there aer any concerns as to the policy.

8. RECORD MANAGEMENT

8.1 The Council must keep a detailed record of all applications for authorisations, grants, refusals, renewals, reviews and cancellations. A central register of all authorisations will be maintained by the ~~Monitoring~~ RIPA Co-ordinating Officer containing the information required from time to time by the relevant Home Office Code of Practice, and records will be retained for a period of at least five years from the ending of each authorisation.

The ~~Monitoring~~ Senior Responsible Officer will monitor authorisations to ensure compliance with the relevant law and guidance, and with these policies and procedures. The Office of Surveillance Commissioners (OSC) can audit and review the Council's policies and procedures, and individual authorisations.

8.2 ~~Copies~~ The originals of all completed RIPA forms, including applications (whether granted or refused), authorisations, renewals, cancellations and reviews, must be forwarded by the AO to the ~~Monitoring~~ Senior Responsible Officer within five working days of the date of the relevant decision.

The originals of these forms should be forwarded within the same time period to the person responsible for the maintenance of the information specified in 8.3 below, with the other information and documentation specified being forwarded as it becomes available.

All documents should be sent in sealed envelopes marked “Confidential”.

8.3 The following information and documents must be maintained by the Corporate Manager of each Group (or by an officer designated by them and notified to the ~~Monitoring~~ Senior Responsible Officer as the RIPA co-ordinator for their Group) in relation to each operation or investigation where RIPA authorisation is requested by officers within their Group:

- the URN for the operation or investigation;
- ~~the originals~~ copies of all completed RIPA application forms indicating whether the application was granted or refused, together with any supplementary documentation, and a copy of any notification of approval given by the AO;
- ~~details of any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;~~
- a record of the period over which the surveillance has taken place;
- details of the frequency of reviews prescribed by the AO;
- a copy record of the result of each review of the authorisation;
- ~~the original~~ copies of any request for a renewal of an authorisation, together with any supporting documentation submitted when the renewal was requested, details as to whether the request was granted or refused, and the reasons for doing so;
- ~~the original~~ copies of any cancellation of an authorisation, including the reasons for cancellation;
- the date and time when any instruction was given by the AO, (including any instruction to cease directed surveillance or to cease using a CHIS) and a note of that instruction and
- the date and time when any other instruction was given by the AO
- a copy of the order approving or otherwise the grant or renewal of an authorisation from a Justice of the Peace (JP)

The following additional information should also be maintained by the relevant Corporate Manager or RIPA co-ordinator in relation to any CHIS:

- any risk assessment in relation to the source;
- the circumstances in which tasks were given to the source;
- the value of the source to the investigating authority;

8.4 By law, an AO must not grant authority for the use of a CHIS unless s/he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the CHIS. Certain particulars must be included in the records relating to each CHIS, and the records must be kept confidential. Further advice should be sought from the ~~Monitoring Officer~~ Senior Responsible Officer or the ~~Deputy Monitoring~~ RIPA Co-ordinating Officer on this point if authority is proposed to be granted for the use of a CHIS.

8.5 A 'Surveillance Log Book' should be completed by the investigating officer(s) to record all operational details of authorised covert surveillance or the use of a CHIS. Once completed, the Log Book should be passed to the Senior Responsible Officer and a copy retained by the Corporate Manager of the relevant Group or to their designated RIPA co-ordinator for safe keeping in a secure place. Each Group will also maintain a record of the issue and movement of all Surveillance Log Books.

9. MATERIAL OBTAINED DURING INVESTIGATIONS

9.1 Generally, all material (in whatever media) obtained or produced during the course of investigations subject to RIPA authorisations should be processed, stored and destroyed in accordance with the requirements of the Data Protection Act 1998, the Freedom of Information Act 2000, any other legal requirements, including those of confidentiality, and the Council's policies and procedures from time to time regarding document retention. The following paragraphs give guidance on some specific situations, but advice should be sought from the ~~Monitoring~~ Senior Responsible Officer, the ~~Deputy Monitoring~~ RIPA Co-ordinating Officer, or the Data Protection and Freedom of Information Officer where appropriate.

9.2 Where material is obtained during the course of an investigation which might be relevant to that investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should **not** be destroyed, but retained in accordance with legal disclosure requirements.

9.3 Where material is obtained, which is not related to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to suspect that it will be relevant to any future civil or criminal proceedings, it should be destroyed immediately.

9.4 Material obtained in the course of an investigation may be used in connection with investigations other than the one that the relevant authorisation was issued for. However, the use or disclosure of such material outside the Council, unless directed by any court order, should only be considered in exceptional circumstances, and in accordance with advice from the ~~Monitoring~~ Senior Responsible Officer or the ~~Deputy Monitoring~~ RIPA Co-ordinating Officer.

9.5 Where material obtained is of a confidential nature then the following additional precautions should be taken:

- Confidential material should not be retained or copied unless it is necessary for a specified purpose;
- Confidential material should only be disseminated in accordance with legal advice that it is necessary to do so for a specific purpose;

- Confidential material which is retained should be marked with a warning of its confidential nature. Safeguards should be put in place to ensure that such material does not come into the possession of any person where to do so might prejudice the outcome of any civil or criminal proceedings;

- Confidential material should be destroyed as soon possible after its use for the specified purpose.

9.7 Use of Social Media

The use of social networking sites by offenders to record their own unlawful activities makes these sites a prime source of evidence. The Council's "Facebook" Account is controlled by the SRO who would not permit access for these purposes and hence the Council is unlikely to engage in social media research, the "rule of thumb" guidance for officers researching open source material is that they will not need an authorisation unless they return to a site on repeated occasions when a directed surveillance authorisation would be required. Once the privacy controls are breached using a covert account, e.g. by becoming a "friend" on Facebook, there would be a minimum requirement for a directed surveillance authorisation; if any form of relationship is established with the account holder/operator, the likelihood is that CHIS relationship would be created requiring authorisation and the appointment of a Controller and a Handler. Records would have to be maintained and arisk assessment undertaken.

If there is any doubt as to whether material is of a confidential nature, advice should be sought from the ~~Monitoring~~ Senior Responsible Officer or the ~~Deputy Monitoring~~ RIPA C~~O~~o-ordinating Officer.

Formatted: Indent: Left: 2 cm, No bullets or numbering

Formatted: Indent: Left: 0 cm, Hanging: 1 cm

10. TELECOMMUNICATIONS DATA AND INTERCEPTION OF COMMUNICATIONS

10.1 Under the RIPA (Communications Data) Order 2003, the Council is permitted to acquire information defined as **communications data**. This includes subscriber details and service data, but not traffic data (as these terms are defined in the legislation). These powers are outside the scope of this guidance document, but officers who consider that they may need to exercise these powers in the course of any investigation, or who require further information, should contact the ~~Monitoring~~ Senior Responsible Officer or the ~~Deputy Monitoring~~ RIPA Co-ordinating Officer.

10.2 The recording of telephone calls between two parties when neither party is aware of the recording **cannot be undertaken**, except under a warrant granted under Part 1 of RIPA. Such warrants are only granted by the Secretary of State and it is not envisaged that such activity would fall within the remit of local authority Investigations. However, there may be situations where either the caller and receiver consent to the recording of the telephone conversation and, in such circumstances a Part 1 warrant may not be required. Such interception should be treated as directed surveillance.

10.3 Part 1 of RIPA does not, however, prevent a local authority in certain circumstances from lawfully intercepting its employees' e-mail or telephone communications, or monitoring their internet access, for the purposes of prevention or detection of crime, or the detection of unauthorised use of these systems. This is authorised under Part 1 of the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

10.4 The legislation referred to above is complex, and further advice should be sought from the ~~Monitoring~~ Senior Responsible Officer or the ~~Deputy Monitoring~~ RIPA Co-ordinating Officer before any investigations are undertaken involving the interception of communications.

11. CCTV AND DIRECTED SURVEILLANCE

11.1 The Council's CCTV system is operated in accordance with a separate Code of Practice. Section 9 of this Code of Practice covers the situation where the CCTV cameras are used for directed or targeted surveillance in such a way that the operation may require authorisation under RIPA ("a Special Procedure" as defined in the Code of Practice). It provides that if a Special Procedure is requested it will be formally considered against RIPA by the Council's CCTV Manager and the result of this assessment shall be noted on the appropriate form.

11.2 If the result of the assessment is that a RIPA authorisation is required, the Code of Practice provides that the Special Procedure must not be implemented unless the CCTV Manager confirms to operational staff that valid authorisation has been granted by a designated AO of the police or the Council.

12. AMENDMENTS TO THIS POLICY AND PROCEDURES

12. The ~~Monitoring~~ Senior Responsible Officer is duly authorised to keep this guidance document up to date, and to amend, delete, add or substitute any provisions as s/he deems necessary. For administrative and operational effectiveness, s/he is also authorised to amend the list of 'AO Posts" set out in Appendix 9, by adding, deleting or substituting any posts.

APPENDICES

APPENDICES 1-8 – FORMS

For the most up-to-date RIPA forms, see this link: [insert link to SharePoint]

[

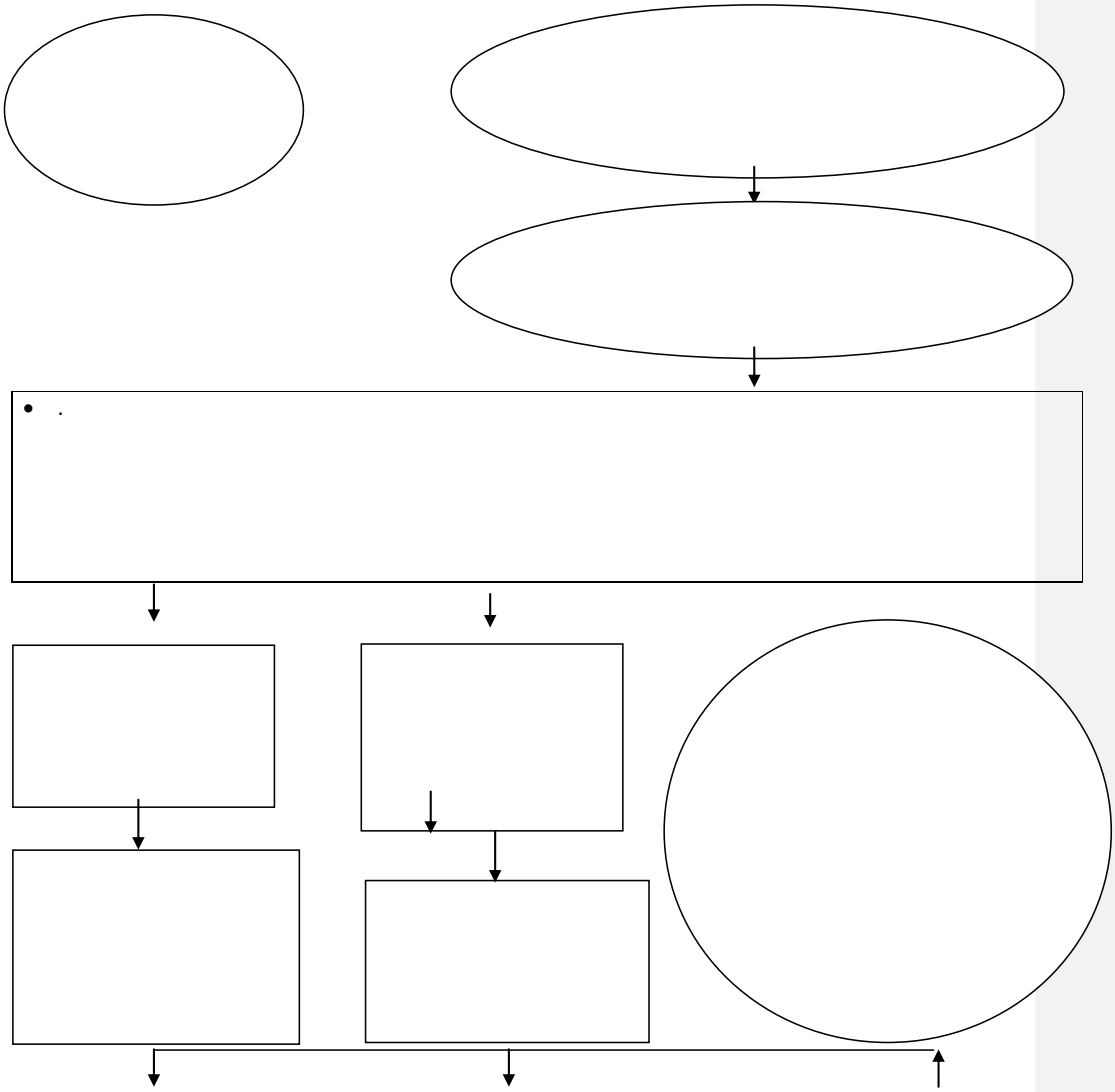
APPENDIX 9

Authorised Officer Posts (in accordance with SI. 521/2010)

Chief Executive
Corporate Managers

APPENDIX 10 - Need to amend to include Magistrates Process or include alternative form.

FLOW-CHART SHOWING AUTHORISATION PROCEDURES



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