Key Decision Required:	No	In the Forward Plan:	No

CABINET

12 DECEMBER 2014

REPORT OF PLANNING AND CORPORATE SERVICES PORTFOLIO HOLDER

A.6 REGULATION OF INVESTIGATORY POWERS – UPDATE

(Report prepared by Martyn Knappett, Lisa Hastings and Karen Neath)

(**PART 1 – KEY INFORMATION**)

PURPOSE OF THE REPORT

To agree an updated policy and procedure manual in relation the Regulation of Investigatory Powers and to agree related delegations to officers.

EXECUTIVE SUMMARY

The Regulation of Investigatory Powers Act (RIPA) came into force in 2000. It was enacted with a view to ensuring that investigative surveillance techniques by a public authority which intrude into an individual's human rights are undertaken in a sound and lawful manner. The Act gives the Council restricted powers to undertake directed surveillance (surveillance that is covert but not intrusive), the use of a covert human intelligence source and some limited powers to acquire some types of communications data.

The Protection of Freedoms Act 2012 brought in limitations regarding directed surveillance only being available over a certain criminal threshold and the requirement to obtain judicial approval through the Magistrate's Court before any surveillance can be undertaken.

The Covert Surveillance Policy and Procedure Manual ("The Policy") attached at Appendix 1 replaces in entirety the Council's previous RIPA guidance. The attached Policy updates and clarifies the process for authorisation, reflects all the latest guidance and legislation and includes comments from Sir David Clarke who recently undertook a review of the Council's arrangements on behalf of the Surveillance Commissioner.

The updated Policy also proposes revised officer appointments for the required roles of Senior Responsible Officer, RIPA Co-Ordinating Officer and seeks approval for delegated powers to appoint Authorising Officers. The policy specifies that no Authorising Officer should approve an application for surveillance unless they have had appropriate training. Training is currently being arranged and is anticipated to be delivered in January 2015. This report also seeks authority for the Legal Services Manager to appoint authorising applicants i.e. those members of staff that would appear in court to seek Judicial Approval for an application.

This Council has made limited use of RIPA in the past and no new applications have been made since 2012. However, it is important that the Council does have an up to date and robust policy for those occasions when the use of RIPA powers may be required and to raise awareness to officers undertaking enforcement action on the limited circumstances in which directed covert surveillance is permitted.

It is proposed to report back to Cabinet on the Policy in 12 months and to report RIPA activity through the performance management arrangements.

RECOMMENDATIONS
It is recommended that:- **a) The attached Policy and Procedure Manual be approved.** **b) The Corporate Director (Corporate Services) be appointed as the Senior Responsible Officer and the Legal Services Manager be appointed as the RIPA Co-Ordinating Officer.** **c) The Senior Responsible Officer and RIPA Co-Ordinating Officer be authorised to appoint Authorising Officers and Authorising Applicants.** **d) The Senior Responsible Officer be authorised to update the Policy for minor and legislative changes.** **e) The Constitution be amended to reflect the delegations within the Policy.** **f) That a further report be submitted to Cabinet in 12 Months.**

PART 2 – IMPLICATIONS OF THE DECISION

DELIVERING PRIORITIES
It is important that the Council has an up to date and robust RIPA policy to ensure that RIPA powers are used appropriately and effectively and the Council does not undertake directed surveillance without the appropriate authorisation.
FINANCE, OTHER RESOURCES AND RISK
Finance and other resources There is no cost involved with agreeing and implementing the RIPA policy. There will be a cost to engage an external trainer but this will be met from existing budgets. **Risk** There is a risk that, if RIPA approvals are sought from the Magistrate's Court without proper consideration or not in line with process, that these could be refused. This would be damaging to the Council's reputation. The attached Policy will mitigate this risk.
LEGAL
The relevant primary legislation is the Regulation of Investigatory Powers Act 2000 as amended and the Protection of Freedoms Act 2012
OTHER IMPLICATIONS
Consideration will be given to other implications as individual applications for use of RIPA powers are considered.

BACKGROUND PAPERS FOR THE DECISION
None

APPENDICES
Appendix 1 – Covert Surveillance Policy and Procedure Manual

Appendix 1

TENDRING DISTRICT COUNCIL

COVERT SURVEILLANCE POLICY AND PROCEDURE MANUAL

PURSUANT TO THE REGULATION OF INVESTIGATORY POWERS ACT 2000

This manual has been prepared to assist officers who undertake covert surveillance but is not intended to be an exhaustive guide

Martyn Knappett

Corporate Director (Corporate Services)
RIPA Senior Responsible Officer

GUIDANCE

1 PURPOSE

1.1 The Council's officers in the course of investigating frauds, regulatory criminal offences and in the interests of the safety and well being of the district may be required to undertake covert monitoring operations to gather evidence to present to a court. In doing so those officers must comply with the relevant legislation i.e., the Regulation of Investigatory Powers Act 2000 (RIPA) and the associated regulations and codes of practice. Evidence collected without complying with the statutory procedures may become inadmissible and prejudice the outcome of the investigation and may be the subject of a claim for damages under the Human Rights Act 1998.

2 SCOPE

2.1 This guidance applies to the planned deployment of directed covert surveillance or the use of Covert Human Intelligence Sources (CHIS) against specified individuals in such a manner as is likely to result in obtaining private information about the person. The following provisions relate therefore to the observation of specified individuals from a vehicle, foot surveillance, the setting up of covert observation positions, the use of equipment for the monitoring of specified individuals and the use of informants or undercover officers.

2.2 The Council's policy does not contemplate the monitoring of internet use, telephone use or portal use (communications data) other than in exceptional circumstances as this is unnecessary and disproportionate in most if not all local authority criminal investigations. Section 7 sets out the broad legislative framework around communications data, however, guidance regarding the acquisition of communications data is beyond the scope of this document and separate advice from the RIPA Senior Responsible Officer (SRO) or Co-ordinating Officer (RCO).

3 BACKGROUND

3.1 Part II of the Regulation of Investigatory Powers Act 2000 (RIPA) provides a mechanism for public authorities to undertake certain investigative techniques in compliance with the Human Rights Act 1998. In particular it allows lawful interference with Article 6 (right to a fair trial) and Article 8 (right to respect for private and family life) rights.

3.2 The Home Office has issued revised Codes of Practice to provide guidance to public authorities on the use of RIPA to authorise covert surveillance that is likely to result in the obtaining of private information. The revised Codes of Practice are titled "Covert Surveillance and Property Interference" and "Covert Human Intelligence Sources".

3.3 All Codes of Practice issued pursuant to section 71 of RIPA are admissible as evidence in criminal and civil proceedings. If any provision of the Codes appears to be relevant to a court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal established under RIPA, or to one of the Commissioners responsible for overseeing the powers conferred by RIPA, they must be taken into account.

3.4 This Manual sets out the procedures that must be followed when the Council undertakes authorised covert surveillance. It is intended to be a best practice guide. This Manual is not intended to replace the Home Office Codes.

3.5 Those officers that intend to apply for an authorisation under RIPA must familiarise themselves with the appropriate Code of Practice as well as this Manual. The Codes of Practice are available online through the following link:

https://www.gov.uk/government/collections/ripa-codes

3.6 The covert surveillance regulated by RIPA and covered by the above Codes of Practice is in three categories; intrusive surveillance, directed surveillance and covert human intelligence. The Act and Codes set up procedures for the authorisation of these activities.

3.7 The authorising officer should first satisfy themselves that the authorisation is necessary for the purpose of investigating crimes which carry a custodial sentence of 6 months or more (see paragraph 10.1 below) and that the surveillance is proportionate to what it seeks to achieve. Authorising and requesting officers (See Annex 1 and 2 for lists of named officers) should have regard to the Code of Practice "Covert Surveillance and Property Interference" , paragraphs 3.3 - 3.6. This states that obtaining an authorisation will only ensure that there is a justifiable interference with an individual's Article 8 Rights if it is necessary and proportionate for these activities to take place.

3.8 It first requires authorising officers to believe that the authorisation is necessary in the circumstances of the particular case which, for the purpose of investigating crimes, means those which carry a custodial sentence of 6 months or more (see paragraph 10.1) Authorising officers should ask themselves if the evidence could be obtained in any other way? Is the surveillance operation really necessary to what the requesting officer is seeking to achieve? Should there be a less intrusive means of obtaining the information, then the authorisation should not be granted. Judicial approval of the authorisation will also be required before the surveillance takes place which is set out further at paragraph 9.

3.9 If the activities are considered necessary, the authorising officer must then satisfy himself that they are proportionate to what is sought to be achieved by carrying them out. He should consider the four elements of proportionality:

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

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

iii) considering whether the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result, and

iv) evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

4 OVERT SURVEILLANCE

4.1 Most of the surveillance carried out by the Council will be done overtly. If observations are made as part of the normal duties of the person or officer involved, which may be termed "**general observations"** (e.g. a planning officer simply noticing something whilst travelling around), then this is not directed surveillance requiring authorisation under RIPA. He may consider that, as a result of his observations, surveillance action is required. If this surveillance is carried out covertly (i.e. without the person being observed knowing it is or may be taking place) then it is likely to be construed as directed surveillance and would first require authorisation under RIPA. If the person subject to surveillance is properly advised in advance that observations are to be carried out, then this is not surveillance that is being done covertly and will fall outside the definition of directed surveillance.

5 COVERT SURVEILLANCE

5.1 Covert surveillance means surveillance, which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. There are two categories of covert surveillance defined in RIPA: intrusive surveillance and directed surveillance.

Intrusive Surveillance

5.2 Covert surveillance is "intrusive surveillance" if it:-

- 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 or the 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 or vehicle. This is unlikely in the case of equipment such as a DAT recorder when used to assess noise nuisance but care must be taken in setting up of equipment and locating the microphone.

5.3 This form of surveillance can therefore only be carried out by the police and other law enforcement agencies. Council Officers **must not** carry out intrusive surveillance.

Directed Surveillance

5.4 Directed surveillance, as defined in RIPA Section 26, is surveillance which is covert, but not intrusive, and undertaken:

(a) For the purpose of a specific investigation or operation; and

(b) In such a manner as is likely to result in obtaining private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

(c) Otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this part to be sought for the carrying out of the surveillance.

6 COVERT HUMAN INTELLIGENCE SOURCES ("CHIS")

6.1 Surveillance by a CHIS will not be authorised by the Council other than in exceptional cases due to the adverse risk to the health and safety of officers and such use will usually only be authorised when working alongside the police.

6.2 If use of a CHIS is contemplated officers must familiarise themselves with the Code of Practice on Covert Human Intelligence Sources and advice should be sought from the SRO and RCO.

6.3 A CHIS is defined as a person who establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating anything that:

(a) Covertly uses such a relationship to obtain information or to provide access to any information to another person; or

(b) Covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

6.4 A relationship is used covertly if, and only if, it is conducted in a manner calculated to ensure that the person is unaware of its purpose. This relationship is established or maintained specifically to obtain or provide access covertly to information about private or family life of another person. It also covers those activities where the relationship itself can be construed as an infringement of a person's private or family life.

6.5 A member of the public making complaints or giving unsolicited information about individuals is outside the provisions of RIPA. However, someone might become a covert source as a result of a relationship with the case officer. For example when a member of the public is asked to monitor the occupation of a

premises. The normal sampling or undertaking of test purchases from shops does not come under the scope of the Act.

7 COMMUNICATIONS DATA

7.1 Under RIPA, Local Government only has power to request data under Section 21(4) (b) and (c) which are as follows:-

Section 21(4) (b) – any information which includes none of the contents of a communication (apart from any information falling within paragraph a)) and is about the use made by any person –

(i) of any postal service or telecommunications service ; or
(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunications system.

Section 21(4) (c) – any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service.

7.2 An Authorising Officer can only grant an authorisation to access data where they believe it is necessary for the purpose of preventing or detecting crime or preventing disorder.

7.3 Any Authorised Officer contemplating the use of this power should first seek separate advice from the SRO or RCO.

8 AUTHORISATIONS

8.1 An authorisation for directed surveillance or the use or conduct of a CHIS, may only be authorised by the council on the following ground:

- for the purpose of investigating crimes which carry a custodial sentence of 6 months or more or for offences relating to the sale of alcohol or tobacco to children and those under 18 (see paragraph 10.1)

The Authorising Officer must believe that:

(a) The action is necessary on the ground set out above; and

(b) The surveillance is proportionate to what it seeks to achieve.

The Authorising Officer will be responsible for considering all applications for covert surveillance and for granting or refusing authorisations as appropriate. The Authorising Officer will also be responsible for carrying out reviews and ensuring that authorisations are renewed or cancelled where necessary.

8.2 The minimum office, rank or position of an Authorising Officer has been designated by the Regulation of Investigatory Powers (Directed Surveillance and

Covert Human Intelligence Sources) Order 2010. For a local authority the Authorising Officer must be the Director, Head of Service, Service Manager or equivalent.

8.3 Wherever knowledge of confidential information, such as a doctor's report, is likely to be acquired through the directed surveillance, a higher level of authorisation is needed. In the Council, this would be the Head of Paid Service (the Chief Executive) or the Corporate Director (Corporate Services).

8.4 A list of those officers who have been nominated as Authorising Officers is given below at Annex 1.

8.5 It is also now recommended best practice that there should be a Senior Responsible Officer (SRO) in each public authority who is responsible for :

- The integrity of the processes in place to authorise directed surveillance
- Compliance with RIPA and with the Codes of Practice
- Engagement with the Commissioners and inspectors when they conduct their inspections, and
- Where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner.

8.6 As the SRO for a local authority has to be a member of the corporate leadership team, the Senior Responsible Officer for this Council will be the person named in Annex 1(b). He will also be responsible for ensuring that all authorising officers are of an appropriate standard in light of the recommendations or concerns raised in the inspection reports prepared by the Office of Surveillance Commissioners following their routine inspections.

8.7 There is also now a requirement for elected members of the Council to review the use of RIPA and to set the policy on covert surveillance at least once a year. Therefore, the Cabinet will review the operation of this policy every 12 months and activity will be reported through the performance management arrangements.

8.8 The Committee should not, and will not, be involved in making decisions on specific authorisations.

8.9 The RCO will be the person named in Annex 1(c). The role of the RCO is as follows:

- Maintaining the Central Record of authorisations and collating the original applications/authorisations, reviews, renewals and cancellations.
- Oversight of submitted RIPA documentation.
- Organising and maintain a RIPA training programme.
- Raising RIPA awareness within the Council.
- Appointment of investigating officers as authorised applicants by their inclusion in annex 2.

AUTHORISATION PROCEDURE

9 STAGE 1 – Internal Authorisation

9.1 Any of the Council's authorised applicants (Annex 2) (who will invariably also be the investigating officer) may make an application for authorisation under RIPA to conduct a covert operation to an authorised officer (Annex 1). Any application for permission to conduct a covert operation must be in writing on the appropriate form. The forms listed below are standard forms for use by all public authorities that are listed in Schedule 1 of RIPA. The forms are an indication of the information required before an authorisation can be granted and are consistent with the requirements in the codes of practice. The Home Office recommends that all users of the form should add any information that is relevant to their organisation but avoid taking any information out of the forms.

9.2 Forms for the application, review, renewal or cancellation of authorisations are available on the Council's intranet.

Directed Surveillance

- DIRECT1 – Authorisation Directed Surveillance
- DIRECT2 – Review of a Directed Surveillance Authorisation
- DIRECT3 – Renewal of a Directed Surveillance Authorisation
- DIRECT4 – Cancellation of a Directed Surveillance Authorisation
- JUDICIAL1 – application for judicial approval for authorisation to conduct directed surveillance

Covert Human Intelligence Source

- CHIS1 – Application for Authorisation for the use or conduct of a Covert Human Intelligence Source
- CHIS2 – Review of a Covert Human Intelligence Source Authorisation
- CHIS3 – Application for Renewal of a Covert Human Intelligence Source Authorisation
- CHIS4 – Cancellation of a Covert Human Intelligence Source Authorisation
- JUDICIAL1 – application for judicial approval for authorisation to use CHIS

9.3 A written application for authorisation must record:

(a) The action to be authorised, including any premises or vehicles involved;
(b) The identities, where known, of those to be the subject of surveillance;
(c) A full account of the investigation or operation;
(d) Justifying that the authorisation is sought for investigating a crime which carries a custodial sentence of 6 months or more (see paragraph 10.1);
(e) How and why the investigation is both necessary and proportionate;
(f) Authorising Officer should state in his own words why the investigation is necessary and proportionate.

9.4 It is considered good practice for a simple sketch map of the immediate area of investigation, detailing specific observation points, location of monitoring equipment etc, to be appended to the application for authorisation. Further details on completing a written application for authorisation are contained in the Codes of Practice.

9.5 No authorising applicant or authorising officer is permitted to request or approve any surveillance identified in this policy unless they have been suitably trained. Furthermore, authorising officers are not permitted to authorise application from within their own Department.

10 CONSIDERATION

10.1 The investigating officer will keep notes during the initial stages of gathering intelligence. Such records will be held on the case file.

10.2 Requests to the authorising officer for authorisation to mount a covert operation will be subject to and based on, the intelligence gathered and recorded on the investigator's notes. The officer will consider if such an operation would assist in investigating crimes which carry a custodial sentence of 6 months or more (see paragraph 10.1)

10.3 Responsibility for authorisation for a covert operation will be considered on the grounds that any operation is likely to be of value in connection with;

- investigating crimes which carry a custodial sentence of 6 months or more (see paragraph 10.1)

- and that the proposed covert operation is a reasonable means of achieving the desired result. This must be balanced with the individual's rights under the Human Rights Act 1998.

10.4 Any authorisation must be on the basis that the activity is both necessary and proportionate. The Authorising Officer must also take into consideration the risk of intrusion into the privacy of persons other than those directly implicated in the operation or investigation (collateral intrusion)

10.5 Additional considerations with respect to the use of a CHIS are

- their likely value as a source of information
- assessment of any risks to them
- the use of vulnerable individuals
- juvenile sources i.e. under 18 years

10.6 For further guidance on these issues please see the Home Office code of practice on the use of Covert Human Intelligence Source. The use of CHIS will only be in exceptional circumstances (See paragraph 5.1 above), and prior advice should be sought from the SRO or RCO.

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

11 STAGE 2 - Judicial Oversight and Approval

11.1 The *Protection of Freedoms Act* brought into law the Judicial oversight of all RIPA approvals by Local Authorities. It inserts sections into the 2000 Act which mean that authorisations whilst still given by Council staff, do not take effect until a Magistrate has approved them. The Judicial oversight does not take the place of the current authorisation process – it is an oversight function and not an authorisation function. **The Authority may not undertake the regulated activity until *Judicial Approval* has been given.**

11.2 The Authority has appointed all investigation officers and managers to make applications under this part (Annex 2) (in accordance with s.223(1) of the Local Government Act 1972), subject to their inclusion in the approved list at annex 2 by the *RCO.* The Authority has authorised the *RCO* to appoint as many investigation officers and managers to make applications under this part as they see fit. Those officers must be listed at annex 2 and any decisions to or deletions from that list must be notified to Members as part of the regular reporting protocols.

11.3 Once the application has been approved by an officer listed in Annex 1, the Authority must apply to the Magistrates Court for an order confirming that:

a. The person who granted or renewed the authorisation, or the notice, was entitled to do so;
b. The grant or renewal met the relevant restrictions or conditions;
c. There were reasonable grounds for believing (at the time it was made or renewed) that obtaining the information described in the form was both necessary and proportionate; and
d. It is still (at the time the court considers it) reasonable to believe the grant/renewal to be both necessary and proportionate.

11.4 The oversight will be determined at a hearing in front of a single Magistrate or District Judge. An officer appointed to do so (and listed at Annex 2 i.e. also the authorised applicant) must approach the court office to arrange the hearing.

11.5 There is a form held on the intranet JUDICIAL1 that must accompany all applications. The authorised applicant (normally the *Officer in Charge* of the case) must complete this form electronically, once the *Authorising Officer* has approved the application. (This also applies to requests for renewals of authorisations.)

11.6 Once the form has been completed, the authorised applicant must submit this, along with electronic copies of any accompanying documents (set out below) to the *Authorising Officer for checking.* Once satisfied with the standard of the form

and any attachments, the *Authorising Officer* must submit the bundle electronically to the *RCO* for onward transmission to the courts.

11.7 The bundle for submission to the courts must include:

a. The application for the order approving the authorisation;
b. The authorised application or renewal form;
c. Any supporting information, that exceptionally, does not form part of the form;
d. Any information you have that might show a reason to refuse the application;
e. An extract from the relevant legislation showing the offence being investigated and that it carries the relevant maximum sentence (unless it is one of the offences provided for in 7A(3)(b) of the 2010 regulations (see 10.1 below) and
f. A copy of the Annexes 1 and 2 to this policy, showing that the *Authorising Officer* and the authorised applicant are both persons duly approved to carry out those functions by the Authority.

11.8 The form requires that the authorised applicant makes a declaration of truth and disclosure, as part of the application for Judicial approval. **It is important that this is not signed lightly;** check that all material facts have been disclosed within the bundle and that the contents are accurate and true.

11.9 The authorised applicant must attend the hearing and assert the accuracy of the application. They must also be prepared to answer any questions about the application and the investigation which the Magistrate may have. At the end of the application, the Magistrate will give the Court's decision.

11.10 Once the bundle has been submitted the *RCO* will note this in the central record. Within 24 hours of receiving the Court's decision, the applicant must notify the *RCO* and the *Authorising Officer* by sending them an email. Both parties must also be sent copies of any court order. The original must be retained on the investigation file. The *RCO* will note the record of the outcome.

11.11 In the event that the Court refuses the application, the authorised applicant, the *Authorising Officer* and the *RCO* will review the decision within 24 hours and decide if they wish to make representations to the Court before a *Quashing Order* is made.

11.12 If the Authority decides to make representations about a refused application, the *Authorising Officer* and *RCO* will immediately notify the court officer of this and request a hearing.

11.13 Grounds for the submission should be set out in writing and notified to the court before the hearing. It must be drafted by the applicant and approved by the *Authorising Officer and RCO.* It must contain the standard declaration as set out above.

11.14 If the Authority elects to seek a hearing, the applicant, *Authorising Officer* and *RCO* will attend the hearing.

11.15 At the conclusion of the hearing, the *RCO* will note the outcome in the central record.

12 SERIOUSNESS THRESHOLD

12.1 No officer may make an authorisation under this policy for directed surveillance unless it concerns conduct which constitutes one or more criminal offences (or would do if it all took place in England and Wales) and either the criminal offence (or one of the criminal offences):

- Is or would be an offence which is punishable by a maximum term of at least 6 months of imprisonment; or
- Is an offence under:
  i. Section 146 of the Licencing Act 2003(3) (sale of alcohol to children);
  ii. Section 147 of the Licencing Act 2003 (allowing the sale of alcohol to children);
  iii. Section 147A of the Licencing Act 2003(4) (persistently selling alcohol to children);
  iv. Section 7 of the Children and Young Persons Act 1933(5) (sale of tobacco, etc., to persons under eighteen).

12.2 In exceptional circumstances, where no named authorising officer is available, any Service Manager or more senior appointment is prescribed within legislation as an authorising officer. They would not however be permitted to authorise unless they have previously received relevant RIPA training.

13 DURATION OF AUTHORISATIONS

13.1 Authorisations for directed surveillance will cease to have effect three months from the day of issue and for the use of covert human intelligence sources, twelve months. The expiry date and time on the authorisation form will therefore always be three/twelve months from the date of authorisation, controlled by review and cancellation. Bear in mind that, for example, a directed surveillance authorisation granted on 1st January expires on 31st March. Authorisations should be reviewed on a regular basis, using the appropriate form, to ensure that they are still necessary and proportionate.

13.2 Authorisations can be renewed prior to their expiry providing the criteria in paragraph 3.9 and the Code of Conduct is met. Applications for renewal must

be in writing and the application and the decision, detailing the grounds for the renewal or refusal to renew or withdrawal of the authorisation.

13.3 When the case is closed prior to the authorisation expiring or covert surveillance is no longer required or meets the criteria for authorisation, which ever is the sooner, the authorisation must be cancelled by the authorising officer using the appropriate form.

13.4 In any case, the authorisation must be cancelled as soon as it has served its purpose.

14 CENTRAL RECORD OF ALL AUTHORISATIONS

14.1 The RCO, Legal Services Manager will maintain a central record of all authorisations granted, renewed or cancelled by the council. These records to be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners, upon request.

14.2 The central record will contain the following information:-

- the type of authorisation;
- the date the authorisation was given;
- name and rank/grade of the authorising officer;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and
- date or dates for review;
- the date JP approval was received;
- if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer;
- whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
- the date the authorisation was cancelled.

14.3 Within one week of the relevant date, the original of the application, review, renewal, court order and cancellation form is to be placed in the RIPA Records File kept secure by the Legal Services Manager. Departments should keep a copy for their own records.

14.4 All records shall be retained for a minimum of three years to ensure that they are available for inspection by the Commissioner. Where there is a belief that the material relating to an investigation could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with the Criminal Procedure and Investigations Act 1996 and kept a period of at least five years.

14.5 Legal Services will be responsible for maintaining the central record and monitoring compliance.

15 CONFIDENTIAL INFORMATION

15.1 There are no special provisions under RIPA for the protection of “confidential information”. Nevertheless, special care needs to be taken where the subject of the investigation or operation might reasonably expect a high degree of privacy or where confidential information is involved.

15.2 Confidential Information can include matters that are subject to legal privilege, confidential personal information or confidential journalistic material.

15.3 In practice, it is likely that most of the surveillance authorised and carried out by the Council would not involve confidential information. However, where there is a possibility that the use of surveillance will enable knowledge of confidential information to be acquired e.g. conversations between a doctor and patient, a higher level of authority for such surveillance is required.

15.4 In cases where it is likely that knowledge of confidential information will be acquired, the use of covert surveillance is subject to a higher level of authorisation, namely by the Head of Paid Service (Chief Executive) or, in his absence, the Corporate Director (Corporate Services).

15.5 The authorised applicant should complete the application for authorisation of directed surveillance in the usual way, but with sufficient indication of the likelihood that confidential information will be acquired.

15.6 At all times during any operation officers are to conduct themselves in a manner that will not breach:

- The Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Data Protection Act 1998
- The Council’s Enforcement Concordat
- This Guidance & Working Code of Practice
- Any code of practice issued by the Home Office

16 COMPLAINTS

16..1 There is provision under RIPA for the establishment of an independent Tribunal. This Tribunal will be made up of senior members of the legal profession or judiciary and will be independent of the Government.

16.2 The Tribunal has full powers to investigate and decide upon complaints made to them within its jurisdiction, including complaints made by a person who is aggrieved by any conduct to which Part II of RIPA applies, where he believes such conduct to have taken place in "challengeable circumstances" or to have been carried out by or on behalf of any of the intelligence services.

16.3 Conduct takes place in "challengeable circumstances" if it takes place:

(i) with the authority or purported authority of an authorisation under Part II of the Act; or

(ii) the circumstances are such that it would not have been appropriate for the conduct to take place without authority; or at least without proper consideration having been given to whether such authority should be sought.

16.4 Further information on the exercise of the Tribunal's functions and details of the relevant complaints procedure can be obtained from:

Investigatory Powers Tribunal

PO Box 33220
London
SW1H 9ZQ
020 7273 4514

16.5 Notwithstanding the above, members of the public will still be able to avail themselves of the Council's internal complaints procedure, where appropriate, which ultimately comes to the attention of the Local Government Ombudsman.

17 THE OFFICE OF SURVEILLANCE COMMISSIONERS

17.1 The Act also provides for the independent oversight and review of the use of the powers contained within Part II of RIPA, by a duly appointed Chief Surveillance Commissioner.

17.2 The Office for Surveillance Commissioners (OSC) was established to oversee covert surveillance carried out by public authorities and within this Office an Inspectorate has been formed, to assist the Chief Surveillance Commissioner in the discharge of his review responsibilities.

17.3 One of the duties of the OSC is to carry out planned inspections of those public authorities who carry out surveillance as specified in RIPA, to ensure compliance with the statutory authorisation procedures. At these inspections, policies and procedures in relation to directed surveillance and CHIS operations will be examined and there will be some random sampling of selected operations. The central record of authorisations will also be inspected. Chief Officers will be given at least two weeks notice of any such planned inspection.

17.4 An inspection report will be presented to the Chief Officer, which should highlight any significant issues, draw conclusions and make appropriate recommendations. The aim of inspections is to be helpful rather than to measure or assess operational performance.

17.5 In addition to routine inspections, spot checks may be carried out from time to time.

17.6 There is a duty on every person who uses the powers provided by Part II of RIPA, which governs the use of covert surveillance or covert human intelligence

sources, to disclose or provide to the Chief Commissioner (or his duly appointed Inspectors) all such documents and information that he may require for the purposes of enabling him to carry out his functions.

IMPORTANT NOTE

This Procedure Manual has been produced as a guide only and is primarily based on the revised Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources published by the Home Office.

For further information please contact Legal Services:

Martyn Knappett – Corporate Director (Corporate Services), RIPA Senior Responsible Officer – 01255 686501 mknappett@tendringdc.gov.uk

Lisa Hastings –Legal Services Manager, RIPA Co-Ordinating Officer– 01255 686561 lhastings@tendringdc.gov.uk

ANNEX 1

Appointment of Authorised Officers

1(a) Authorising Officers for the purposes of RIPA (Authorising Officers must **not** approve applications until they have been suitably trained and are **not** permitted to authorise applications within their own Department)

Richard Barrett (Finance and Procurement Manager)

John Fox (Environmental Services Manager)

Mark Westall (Commercial Manager)

Where it is likely that knowledge of confidential information will be acquired covert surveillance must be authorised by the **Chief Executive** or in his absence by the **Corporate Director (Corporate Services)**

1(b) Senior Responsible Officer

Martyn Knappett, Corporate Director (Corporate Services)

1(c) RIPA Co-Ordinating Officer

Lisa Hastings, Legal Services Manager and Monitoring Officer

ANNEX 2

Council's Authorised Applicants

In order for the Authority's RIPA authorisations to take effect, they must be approved by a Magistrate. That process requires applicants in person to appear for the Authority and the official court service guidance makes it clear that these should be investigators not lawyers.

Any person from this Authority wishing to make an application must be named in this annex and must take to court a copy of this annex and their official identification.

I certify that the following have been appointed under section 223(1) of the Local Government Act 1972 to appear for the Authority and are approved applicants in accordance with paragraph 9.2 of this policy:

Name	Section	Appointed from	Appointment terminated

Signed……

Lisa Hastings
RIPA Co-Ordinating Officer