Appendix 1

TEWKESBURY BOROUGH COUNCIL

PROCEDURAL GUIDE

REGULATION OF INVESTIGATORY POWERS ACT 2000

Forward

The purpose of this Procedural Guide ("the Guide") is to ensure that Tewkesbury Borough Council ("the Council") complies with the Regulation of Investigatory Powers Act 2000 (RIPA).

The introduction of the Human Rights Act 1998 means that the Council by law has to respect the rights of everyone. In particular Article 8 guarantees everyone the right to respect for their private and family life, their home and correspondence. This right can only be interfered with when the interference is in accordance with the law and necessary. RIPA provides the framework for public authorities to carry out surveillance and the lawful means whereby rights can be infringed by the Council. If the correct procedures are put in place and followed by officers the Council will earn the protection of RIPA and our actions will be lawful.

1. INTRODUCTION

1.1 This document sets out the policies and procedures adopted by Tewkesbury Borough Council ("the Council") in relation to the Regulation of Investigatory Powers Act 2000 ("RIPA").

1.2 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 individual's 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.

1.3 This guide shall be readily available at the Council Offices. A copy can be obtained from the RIPA co-ordinator, One Legal, Tewkesbury Borough Council, Council Offices, Gloucester Road, Tewkesbury GL20 5TT. It is also available on the Council's website at www.tewkesbury.gov.uk.

1.4 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.

1.5 The Council may need, where it is deemed necessary and proportionate, to make use of covert surveillance or CHIS. The use of any covert surveillance should only be used as a last resort and any covert surveillance will have to be authorised and conducted in accordance with RIPA, the statutory codes of practice and this Guide and shall only be for one of the purposes set out in this Guide and for a purpose which the Council is legally required or empowered to investigate as part of its functions.

1.6 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 an Authorising Officer ("AO")(Appendix A) on the appropriate form (see Appendix B).

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.

1.7 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.

1.8 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 B contain relevant guidance notes; however, officers are encouraged to contact One Legal for advice or assistance if required. Useful guidance can also be found via the web-sites of the Office of Surveillance Commissioners at www.surveillancecommisioners.gov.uk and the Home Office RIPA web-site at www.homeoffice.gov.uk

1.9 Appropriate training will be arranged at regular intervals for all officers likely to make applications or authorise them. The Council's Senior Responsible Officer (SRO)(see section 7) will ensure that they and all relevant members of their staff undertake this training and that appropriate records are kept.

1.10 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 REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

2.1 THE BACKGROUND TO RIPA

2.1.1 RIPA provides a legal framework for the control and regulation of surveillance and information techniques which public authorities undertake as part of their duties. As was highlighted in the introduction to the Guide the need for such control arose as a result of the Human Rights Act 1998. Article 8 of the European Convention on Human Rights states that:

Everyone has the right of respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals or for the protection of the rights and freedoms of others.

2.1.2 The right under Article 8 is a qualified right and authorities can interfere with this right for the reasons given in paragraph 2 of Article 8. RIPA provides the legal framework for lawful interference.

3. THE SCOPE OF THIS GUIDE

3.1 SURVEILLANCE

3.1.1 This Guide intends to cover the surveillance and information gathering techniques which are most likely to be carried out by the Council.

3.1.2 Local Authorities can only approve authorisations under RIPA when performing its core functions. Those are the specific public functions undertaken by the Local Authority as opposed to its ordinary functions which are undertaken by all public authorities. For example, an authorisation under RIPA cannot be used when the principal purpose of an investigation is for taking disciplinary action against an employee, as the disciplining of an employee is not a core function. It may, however, be appropriate to seek an authorisation under RIPA if there are associated criminal investigations. If you are unsure about whether you can seek RIPA authorisation please contact the RIPA co-ordinator before you seek approval or undertake surveillance.

3.2 OVERT SURVEILLANCE

3.2.1 Neither RIPA nor this Guide covers the use of overt surveillance, any general observation that forms part of the normal day to day duties of officers (for example, where a planning officer drives past a site to check whether planning conditions are being complied with), the use of equipment to merely reinforce normal sensory perception such as binoculars or circumstances where members of the public who volunteer information to the Council. Surveillance is also overt if the subject has been told it will happen i.e. a noisemaker is warned that noise may be recorded if a noise nuisance continues.

3.2.2 Most investigations carried out by the Council will not involve covert surveillance as other investigative means will be used. For example the evidence will be collected overtly i.e. there will be nothing secretive, clandestine or hidden about it i.e. an officer of the Council in a council uniform walking around a car park or visiting a site to collect evidence where you make your presence known to the owner of the land or you will have collected evidence such as a food sample brought in good faith from a shop and you will take a witness statement from a person about the food sample.

3.2.3 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.

3.2.4 There may be occasions when officers come across events unfolding which were not pre planned which then requires them to carry out some form of observation. This will not amount to Directed Surveillance. However it will amount to surveillance outside of RIPA and must still be necessary and proportionate and take account of the intrusion issues. Officers must not abuse the process and be prepared to explain their decisions in court should it be necessary. It is important when conducting surveillance in these circumstances that officers still understand that they have obligations to ensure that their actions are HRA compliant and are therefore necessary and proportionate and take account of the intrusion issues. Investigating Officers (IO) should document their decisions, what took place, and what evidence or information was obtained.

3.3.5 IO should be careful if they start to undertake more specific and targeted investigations into a matter. Repeated visits may amount to systematic, and therefore, directed surveillance and require authorisation: If in doubt, legal advice should be sought in advance of any visit.

3.2.6 RIPA does not normally cover the use of overt CCTV surveillance systems since members of the public are aware that such systems are in place. There may however be times when the Council uses the CCTV for a specific investigation or operation. If the CCTV system is going to be used for this purpose the CCTV should only be used in accordance with the Council's policy on CCTV use.

3.3 COVERT SURVEILLANCE

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

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

3.4 DIRECTED SURVEILLANCE

3.4.1 Directed Surveillance (DS) is surveillance which:-

- is covert; and
- is not intrusive surveillance (see definition below and please also note that 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 authorisation 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).

3.4.2 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 may 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.

3.4.3 Surveillance that is unforeseen and undertaken as an immediate response to a situation normally falls outside the definition of DS 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.

3.5 INTRUSIVE SURVEILLANCE

3.5.1 Intrusive surveillance can be carried out only by police and other law enforcement agencies. **Council officers must not carry out intrusive surveillance**. This information is only included in this guide as information and to inform Investigators of what is Intrusive Surveillance so it can be avoided.

3.5.2 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.

3.6 COVERT HUMAN INTELLIGENCE SOURCES

3.6.1 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 One Legal before any authorisation is applied for or granted.

3.6.2 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 means of that 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.

3.6.3 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 should be sought from One Legal before using professional witnesses.

3.6.4 Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 years of age). On no account can a child under 16 years of age be authorised to give information against his or her parents. Similar safeguards also apply to the use of vulnerable individuals as sources. (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 One Legal before using juveniles or vulnerable individuals as sources, to ensure that all necessary legal requirements are complied with.

3.6.5 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 One Legal.

4. AUTHORISATION PROCEDURES

4.1 BACKGROUND

4.1.1 Any DS 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. A flow chart of the procedures to be followed appears at Appendix D.

4.1.2 Officers are advised to discuss the need to undertake DS or the use of a CHIS with their 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. If it is intended that both DS and the use of a CHIS will take place on the same

surveillance subject, the respective applications forms and procedures should be followed and both activities should be considered separately on their own merits.

4.2 INVESTIGATING OFFICERS (IO) RESPONSIBILITIES

4.2.1 All the relevant sections on an application form (see Appendix B) must be completed with sufficient information for the AO to consider necessity, proportionality and the collateral intrusion issues. Risk assessments should take place prior to the completion of the application form. Each application should be completed on its own merits of the case. Cutting and pasting or using template entries should not take place as this would leave the process open to challenge.

4.3 PRE AUTHORISATION STEPS

4.3.1 Before submitting an application for authorisation, an Investigating Officer must firstly contact One Legal, 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. The RIPA Coordinator 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 appropriate) (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

4.3.2 When issuing the URN, the RIPA Coordinator can provide advice to the Investigating Officer in relation to the activity to be authorised including any issues of necessity, proportionality and collateral intrusion.

4.4 AUTHORISING OFFICERS

4.4.1 Only those officers employed in the designated "Authorised Officer" posts (AOs) set out in Appendix A can authorise DS or the conduct or use of a CHIS. AOs may not sub-delegate their powers in relation to RIPA to other officers. AOs should also not authorise investigations in which they are directly involved. If however this is unavoidable the reasons for this should be recorded.

4.4.2 Before giving authorisation an AO must be satisfied that the reason for the request is for the prevention and detection of crime and that the crime attracts a custodial sentence of a maximum of 6 months or more or is an offence relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

4.4.3 An AO must also be satisfied the surveillance in each case is necessary and proportionate in those particular circumstances. Obtaining an authorisation under the 2000 Act, the 1997 Act and 1994 Act 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.

4.4.4 When considering an application, AOs must:-

(a) be satisfied that the desired result of the covert surveillance cannot reasonably be achieved by other means;

(b) have regard to the contents of this document, the training provided on RIPA and any other guidance or advice given by the RIPA co-ordinator;

(c) 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 paragraph 4.4.8 below; and
(iii) proportionate to what it seeks to achieve

(d) assess whether or not the proposed surveillance is proportionate, consider other appropriate means of gathering the information, and particularly whether any other means would be less intrusive (the least intrusive means of obtaining the necessary information should always be preferred);

(e) 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);

(f) consider whether there is the possibility of collecting confidential personal information. If there is a possibility of collecting personal information the matter should be passed to the Chief Officer for consideration

(g) 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.

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

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

(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.

4.4.6 In all cases the AO must record a clear description of what the 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.

4.4.7 When the AO has considered if the surveillance is necessary and proportionate they must complete the relevant section of the form explaining why in his/her opinion the surveillance is necessary and proportionate.

Necessity - RIPA first requires that the person granting an authorisation believes that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds in section 28(3) of the 2000 Act for DS. The applicant and AO must also be able to demonstrate that there were no other means of obtaining the same information in a less intrusive method.

Proportionality - Then, if the activities are necessary, the person granting the authorisation must believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

4.4.8 The codes provide guidance relating to proportionality which should be considered by both applicants and AOs:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; and
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

4.4.9 The AO will provide the details of when reviews will take place. The review periods will be decided by the AO based on the circumstances contained within the application.

4.5 COLLATERAL INTRUSION

4.5.1 Before authorising applications for DS an AO must also take into account the risk of obtaining private information about persons who are not the subject/s of the surveillance. Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance activity. Where collateral intrusion is unavoidable, activities may still be authorised, provided the intrusion is proportionate to what is sought to be achieved.

4.5.2 All applications should include an assessment of the risk of collateral intrusion and the details of any measures taken to limit the intrusion. An AO must consider these risks and the proportionality of proposed actions.

4.6 CONFIDENTIAL INFORMATION

4.6.1 If an IO or AO believes that confidential information may be obtained as a result of surveillance, the advice of One Legal should be sought in advance of any authorisation or surveillance. In any case where it is likely that confidential information may be acquired by

the use of a CHIS , 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, "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 counseling or other assistance given or to be given to them or
- confidential journalistic material (this includes related communications), that is, material obtained or acquired for the purposes of journalism and subject to an undertaking to hold in confidence

4.7 COURT APPROVAL

4.7.1 After the AO has authorised the surveillance the IO must seek judicial approval before they conduct any surveillance. Any application to the Court must be made in consultation with One Legal. The IO (applicant) will complete the relevant forms and seek advice from One Legal. A copy of the application form/order form is attached at Appendix C. The applicant must complete the required sections of the application/order form.

4.7.2 Any application to a JP must be made in consultation with One Legal. Unless otherwise agreed One Legal will contact Her Majesty's Courts & Tribunals Service (HMCTS) to arrange a hearing. The hearing will be in private and heard by a single JP. The IO and an officer from One Legal will attend the Magistrates' Court to seek a Justice of the Peace's (JP) approval before commencing any surveillance.

4.7.3 Officers who may present the application at these proceedings may need to be formally designated by the Council under section 223 of the Local Government Act 1972 to appear, be sworn in and present evidence or provide information as required by the JP.

4.7.4 Upon attending the hearing, the officer must present to the Court the partially completed judicial application/order form, a copy of the RIPA application/authorisation form, together with any supporting documents setting out the case, and the original application/authorisation form.

4.7.5 The original RIPA application/authorisation should be shown to the Court but will be retained by the Council so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT).

4.7.6 The Court will consider the RIPA application/ authorisation and the judicial application/order form (Appendix C). They may have questions to clarify points or require additional reassurance on particular matters. These questions are supplementary to the content of the application form**.** The forms and supporting papers however must by themselves make the case. It is not sufficient for the Applicant to provide oral evidence where this is not reflected or supported in the papers provided.

4.7.7 The Court will consider whether he or she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the Council and the authorisation was made in accordance with any applicable

legal restrictions, for example that the crime threshold for directed surveillance has been met.

4.7.8 The Court may decide to: (1) Approve the grant or renewal of an authorisation in which case the grant or renewal of the RIPA authorisation will then take effect and the Council may proceed to use the technique in that particular case. (2) Refuse to approve the grant or renewal of an authorisation in which case the RIPA authorisation will not take effect and the Council may not use the technique in that case.

4.7.9 Whatever the decision the Court will record their decision on the order section of the judicial application/order form. The court administration will retain a copy of the Council's RIPA application and authorisation form and the judicial application/order form. The Applicant will retain the original application/authorisation and a copy of the judicial application/order form.

4.7.10 If approved by the Court, the date of the approval becomes the commencement date and the three months duration will commence on this date, the officers are now allowed to undertake the activity. The original application and the copy of the judicial application/order form should be forwarded to the Central Register and a copy retained by the applicant and if necessary by the AO

4.8 REFUSALS

4.8.1 If the Court does not approve the grant or renewal the authorisation will not take effect and the IO must not use technique in the case.

4.8.2 Where an application has been refused the applicant may wish to consider the reasons for that refusal. An IO and/or AO may wish to discuss this matter with One Legal.

4.8.3 Where the Court does not approve the grant or renewal and decides to quash the original authorisation the Court must not exercise its power to quash the application/authorisation unless the applicant has had 2 business days from the date of refusal to make representations. Any further representations will be made to the Court in consultation with One Legal.

4.9. DURATION AND RENEWALS OF AUTHORISATIONS

4.9.1 Authorisations will have effect until the date for expiry specified on the relevant application form. If approved by a JP applications will last for 3 months from the approval date. 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 IO to ensure that any DS 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 SRO ("Senior Responsible Officer") will perform an auditing role in this respect but the primary responsibility rests with the IO and AO.

4.9.2 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 Appendix B. There is no requirement for a review form to be submitted to a JP.

4.9.3 Should it be necessary to renew a DS or CHIS application authorisations must be made to a JP. Authorisations shall be renewed in writing. Applications for renewal 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.

4.9.4 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 officer in charge of the investigation, who should submit a request for cancellation on the appropriate form as set out in Appendix B. If the AO who authorised any DS or the use or conduct of a CHIS (or any AO who has taken over their duties) however 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.

5. RECORD MANAGEMENT

5.1 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 One Legal 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 three years from the ending of each authorisation.

5.2 The RIPA co-ordinator 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.

5.3 Copies of all completed RIPA forms, including applications (whether granted or refused), authorisations, renewals, cancellations and reviews, must be forwarded by the AO to the RIPA co-ordinator within five working days of the date of the relevant decision. All documents should be sent in sealed envelopes marked “Confidential”.

5.4 The following information and documents must be maintained by relevant Group Manager in relation to each operation or investigation where RIPA authorisation is requested by officers within their team:

- the URN for the operation or investigation;
- the originals 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 record of the result of each review of the authorisation;

- the original 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 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

5.5 The following additional information should also be maintained by the relevant Group Manager and 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;

5.6. 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 One Legal on this point if authority is proposed to be granted for the use of a CHIS.

6. TELECOMMUNICATIONS DATA AND INTERCEPTION OF COMMUNICATIONS

6.1 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 One Legal.

6.2 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.

6.3 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.

6.4 The legislation referred to above is complex, and further advice should be sought from One Legal before any investigations are undertaken involving the interception of communications.

7 PROCEDURE FOR MONITORING RIPA AND OVERSIGHT

7.1 SENIOR RESPONSIBLE OFFICER (SRO)

7.1.2 The Council's Borough Solicitor is the designated SRO 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; and
- overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner.

7.1.3 The SRO 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.

7.1.4 The SRO shall maintain a Central Record of Authorisations.

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 Audit Committee as required under paragraph 7.3 below.

7.2.4 The SRO is the point of contact in respect of any covert activity that takes place that was not properly authorised. The SRO will report any such activity to the OSC in writing as soon as the error is recognised (See Appendix B for the correct form). This includes activity which should have been authorised but wasn't or which was conducted beyond the directions provided by the AO.

7.3 MEMBER REVIEW

7.3.1 The members of the Council's Audit Committee shall review the use of RIPA and this policy. In order to facilitate this, the SRO shall provide yearly reports to Audit Committee on how RIPA has been used in the previous year and whether there are any concerns as to the policy.

7.4 AMENDMENTS TO THIS POLICY AND PROCEDURES

7.4.1 The Council's SRO 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 A, by adding, deleting or substituting any posts.

Appendix A

Role	Designated Officer
Senior Responsible Officer	Borough Solicitor
Authorising Officers	Chief Executive
	Deputy Chief Executive
	Group Manager Environment and Housing
	Group Manager Development Services
	Group Manager Business Transformation
	Group Manager Finance and Asset Management
	Group Manager Revenues and Benefits
	Group Manager Policy and Performance
RIPA Co-ordinator	One Legal

Appendix B

AUTHORISATION FORMS

All of the forms necessary for RIPA are available from the Home Office website these forms are a mandatory part of the process and must be used in line with the guidance.

All decisions about using regulated investigatory powers must be recorded as they are taken on the required form.

This is the case for applicants seeking authority to undertake regulated conduct and for Authorising Officers and designated persons who consider and decide whether to grant authority or give notice for that conduct. Select the form that you require from the hyperlinked lists below:-

Directed Surveillance
Application for the use of directed surveillance
Renewal of directed surveillance
Review of the use of directed surveillance
Cancellation of the use of directed surveillance

Covert Human Intelligence Sources
Application for the use of covert human intelligence sources
Renewal of authorisation to use covert human intelligence sources
Reviewing the use of covert human intelligence sources
Cancellation of covert human intelligence sources

Reporting errors to the IOCCO
Reporting an error by a CSP to the IOCCO
Reporting an error by a public authority to the IOCCO

Appendix C

Application for judicial approval for authorisation to obtain or disclose communications data, to use a Covert Human Intelligence Source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local authority:.....

Local authority department:.....

Offence under investigation:.....

.....

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

.....

.....

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

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

Investigating Officer:.....

Authorising Officer/Designated Person:.....

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

Address of applicant department:.....

.....

Contact telephone number:.....

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

Local authority reference:.....

Number of pages:.....

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

Magistrates' Court:

Having considered the application,

I (tick one):

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

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

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

Notes

.....

.....

.....

.....

.....

.....

.....

Reasons

.....

.....

.....

.....

.....

.....

.....

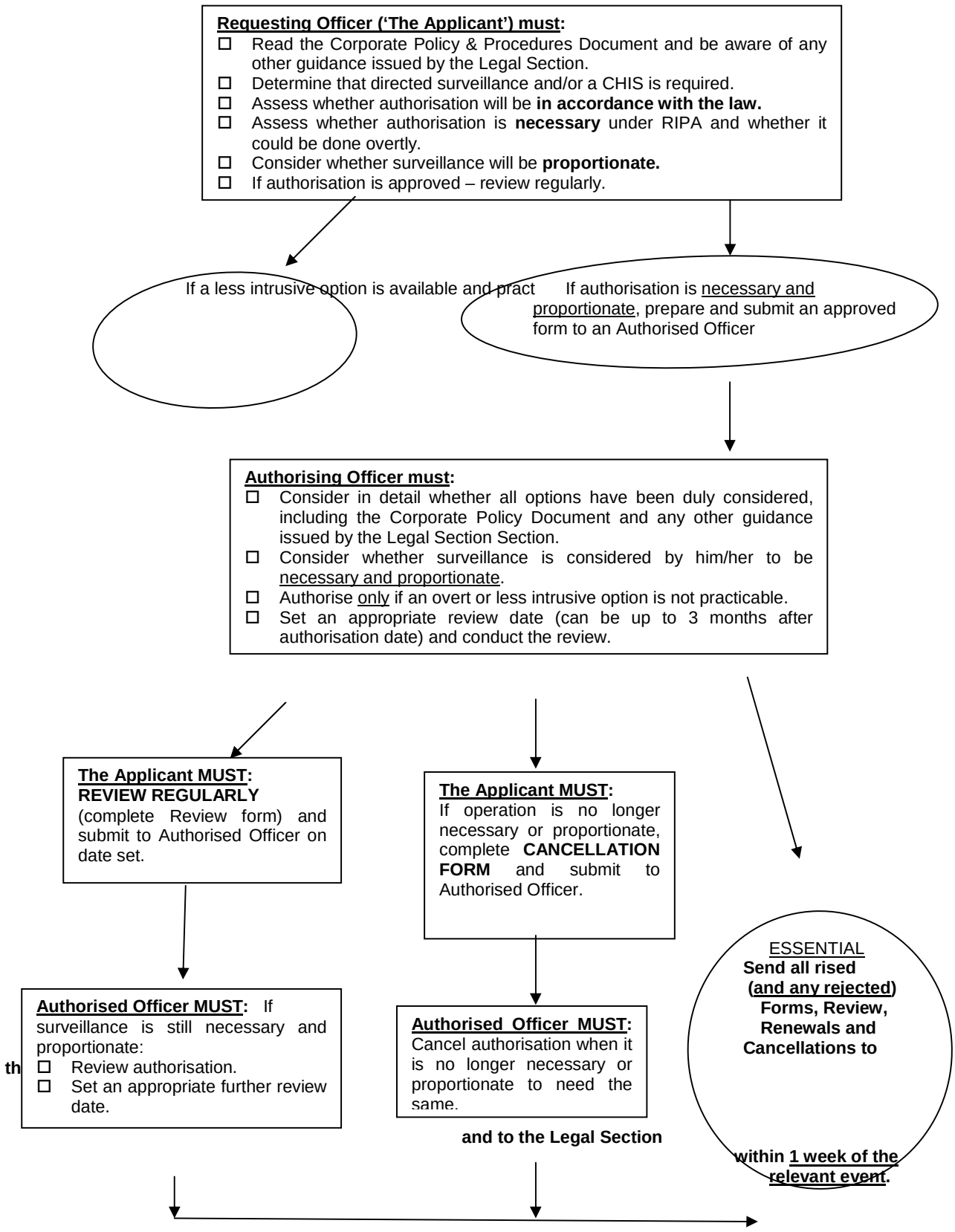
.....

Signed:

Date: Time:

Full name:

Address of Magistrates' Court:



NB: If in doubt, ask the Legal Section BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled, or rejected.

Requesting Officer ('The Applicant') must:

- ☐ Read the Corporate Policy & Procedures Document and be aware of any other guidance issued by the Legal Section.
- ☐ Determine that directed surveillance and/or a CHIS is required.
- ☐ Assess whether authorisation will be **in accordance with the law.**
- ☐ Assess whether authorisation is **necessary** under RIPA and whether it could be done overtly.
- ☐ Consider whether surveillance will be **proportionate.**
- ☐ If authorisation is approved – review regularly.