Epping Forest District Council

POLICY & PROCEDURE

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

CONTENTS

Section A

Introduction

1. HUMAN RIGHTS ACT 1998 – ARTICLE 8 – RIGHT TO RESPECT FOR PRIVATE & FAMILY LIFE, HOME AND CORRESPONDENCE

1.1 The Human Rights Act 1998 brought into UK domestic law much of the European Convention on Human Rights and Fundamental Freedoms 1950. Article 8 of the European Convention requires the Council to respect the private and family life of its citizens, their homes and their correspondence.

1.2 Article 8 does, however, recognise that there may be circumstances in a democratic society where it is necessary for the state to interfere with this right.

2. USE OF COVERT SURVEILLANCE TECHNIQUES AND HUMAN INTELLIGENCE SOURCES

2.1 The Council has various functions which involve observing or investigating the conduct of others, for example, investigating anti-social behaviour, fly tipping, noise nuisance control, planning (contraventions), benefit fraud, licensing and food safety legislation. In most cases, Council officers carry out these functions openly. However, there are rare cases where it is necessary for officers to use covert surveillance techniques to undertake a specific investigation.

2.2 The use of covert surveillance techniques is regulated by the Regulation of Investigatory Powers Act 2000 (RIPA), which seeks to ensure that the public interest and human rights of individuals are appropriately balanced. This document sets out the Council's policy and procedures on the use of covert surveillance techniques and the conduct and use of a Covert Human Intelligence Source.

2.3 You should also refer to the two Codes of Practice published by the Government. These Codes, which were revised in 2010, are on the Home Office website and supplement the procedures in this document. The Codes are admissible as evidence in Criminal and Civil Proceedings. If a provision of these Codes appear relevant to any court or tribunal, it must be taken into account:

(a) Covert Surveillance and Property Interference Code of Practice:

http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/covert-surveil-prop-inter-COP

(b) Covert Human Intelligence Sources Code of Practice:

http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/covert-human-intel-source-COP

2.4 There are also two other guidance documents relating the procedural changes regarding the authorisation process requiring Justice of the Peace approval from the 1st November 2012. These have been issued by the Home Office to both Local Authorities and Magistrates.

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/

3. ACQUISITION OF COMMUNICATIONS DATA

3.1 RIPA also regulates the acquisition of communications data. Communications data is data held by telecommunications companies and internet service providers.

3.2 Examples of communications data which may be acquired with authorisation include names, addresses, telephone numbers, internet provider addresses. Communications data surveillance does not monitor the content of telephone calls or emails. This document sets out the procedures for the acquisition of communications data. You should also refer to the Code of Practice which is available on the Home Office website:

(a) Acquisition and Disclosure of Communications Data Revised Draft Code of Practice:

http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/acquisition-disclosure-cop

Acronyms and Designations explained

OSC Office of Surveillance Commissioners
SRO Senior Responsible Officer : Director of Corporate Support Services / Solicitor to the Council
Authorising Officers: Director of Corporate Support Services/ Solicitor to the Council and the Assistant to the Chief Executive

Applicant Officer seeking RIPA authorisation or renewal

Section B

4. EFFECTIVE DATE OF OPERATION AND AUTHORISING OFFICER RESPONSIBILITIES

4.1 The Policy and Procedures in this document reflect the two revised Codes of Practice which came into force in April 2010, and the recent legislative amendments which now require Justice of the Peace (JP) approval for all Local Authority RIPA applications and renewals, which came in effect on 1 November 2012, changes in website addresses and application forms, as well as to reflect recommendations arising out of inspection by the Office of Surveillance Commissioners. Authorising Officers, take personal responsibility for the effective and efficient observance of this document and the Office of Surveillance Commissioners (OSC) guidance documents.

4.2 Authorising Officers will undertake training on RIPA and will facilitate where necessary training for relevant members of staff who may make RIPA applications.

4.3 Applicants are required to follow this Policy and Procedures Document and must not undertake or carry out surveillance activity that meets the criteria as set out by RIPA without first obtaining the relevant authorisations in compliance with this document.

4.4 Authorising Officers will pay particular attention to health and safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should an Authorising Officer approve any RIPA form unless, and until they are satisfied that

- the health and safety of Council employees/agents are suitably addressed
- risks minimised so far as is possible, and
- risks are proportionate to the surveillance being proposed.

4.5 Applications to Authorising Officers must be made in **sealed** envelopes and marked '**Strictly Private & Confidential**'.

4.6 In accordance with the Codes of Practice, the Senior Responsible Officer (SRO) is the Director of Corporate Support Services / Solicitor to the Council.

4.7 The SRO shall have delegated authority to appoint additional Authorising Officers for the purposes of RIPA should either or both of the Authorising Officers be absent.

4.8 The SRO is responsible for;

- the integrity of the process in place within this authority to authorise surveillance with the Act.
- compliance with Part II of the 2000 Act, relevant codes and this policy;
- 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.

4.9 The SRO will review the policy every year and report on performance of the policy to Council.

4.10 Annual reports on the use of RIPA will be considered by the Corporate Governance Group and will published in the Council Bulletin.

5. GENERAL INFORMATION ON RIPA

5.1 The Human Rights Act 1998 requires the Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, their homes and their correspondence.

5.2 The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council may interfere in the citizen's right mentioned above, if such interference is:-

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

(b) **necessary** ; **and**

(c) **proportionate**.

5.3 The Regulation of Investigatory Powers Act 2000 ('RIPA') provides a statutory mechanism (ie. 'in accordance with the law') for authorising **covert surveillance** and the use of a **'covert human intelligence source' ('CHIS')** – RIPA and this Policy and Procedure document seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

5.4 Directly-employed Council staff and external agencies working for the Council are covered by the Act for the time they are working for the Council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on the Council's behalf, must be properly authorised by one of the Council's designated Authorising Officers prior to seeking judicial approval

5.5 If the correct procedures are not followed, evidence may be inadmissible in court proceedings, a complaint of maladministration could be made to the Ombudsman and/or the Council could be ordered to pay compensation.

6. WHAT RIPA DOES AND DOES NOT DO

6.1 RIPA:

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

6.2 RIPA does not:

- prejudice or affect any existing powers available to the Council to obtain information by any means not involving conduct that may be authorised under this Act. For example, the Council's current powers to obtain information from the DVLA or from the Land Registry as to the ownership of a property.

6.3 If any Applicant is in any doubt, s/he should ask the SRO BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

7. TYPES OF SURVEILLANCE

7.1 **'Surveillance'** includes:

- monitoring, observing and listening to persons, watching or following their movements, listening to their conversations and other such activities or communications. It may be conducted with or without the assistance of a surveillance device.

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

- surveillance, by or with, the assistance of appropriate surveillance device(s).

7.2 Surveillance can be overt or covert**.**

Overt Surveillance

7.3 Most of the surveillance carried out by the Council will be done overtly. Surveillance will be overt if the subject has been told it will happen (eg. where a noisemaker is warned (preferably in writing) that noise will be recorded.

Covert Surveillance

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

7.5 There are two types of covert surveillance which local authorities may undertake. Directed Surveillance and the use of Covert Human Intelligence Sources (CHIS).

Directed Surveillance

7.6 Under Section 26(2) of RIPA ,Directed Surveillance is surveillance which is covert, but not intrusive, and undertaken

- for 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); and

- not as an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable e.g. spotting something suspicious and continuing to observe it.

7.7 Private Information in relation to a person includes any information relating to his private and family life, his home or his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others with whom s/he comes into contact.

7.8 Private information may include personal data such as names, addresses or telephone numbers. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate.

7.9 Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific purpose, which involves prolonged surveillance on a particular person, authorisation will be required. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others. Privacy considerations are likely to arise if several records are examined together to establish a pattern of behaviour.

NOTE: For the avoidance of doubt, only those Officers appointed as 'Authorising Officers' for the purpose of RIPA can authorise 'Directed Surveillance' IF, AND ONLY IF, the RIPA authorisation procedures detailed in this Document, are followed.

Intrusive Surveillance

7.10 This is when surveillance:

- is covert;
- relates to residential premises and private vehicles, even if used on a temporary basis; 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.

NOTE: For the avoidance of doubt, this authority cannot authorise intrusive surveillance.

"Proportionality"

7.11 This term contains three concepts:

- the surveillance should not be excessive in relation to the gravity of the matter being investigated;

- the least intrusive method of surveillance should be chosen; and

- collateral intrusion involving invasion of third parties' privacy and should, so far as possible, be minimised.

7.12 Proportionality involves balancing the intrusiveness of the activity on the subject 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. The interference with the person's right should be no greater than that which is required to meet the aim and objectives.

7.13 The onus is on the Authorising Officer to ensure that the surveillance meets the tests of **necessity and proportionality**.

7.14 The codes provide guidance relating to proportionality which should be considered by both applicants and Authorising Officers :

- 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;

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

7.15 When considering the intrusion, it is important that the Authorising Officer is fully aware of the technical capabilities of any proposed equipment to be used, and that any images are managed in line with the Data Protection Act and Home Office Guidance. These issues have a direct bearing on determining proportionality.

8 Surveillance outside of RIPA

8.1 Surveillance which is not covered by the RIPA must still be in accordance with the Council's obligations under the Human Rights Act and Data Protection Act. It must still be necessary and proportionate having taken account of the intrusion issues. The decision making process and the management of such surveillance must be well documented.

8.2 The Office of Surveillance Commissioners(OSC) have stated that it should be the responsibility of the SRO to monitor this type of activity. Therefore, before any such surveillance takes place advice must be sought from the SRO.

9. Covert Human Intelligence Source (CHIS)

9.1 As a starting point, this Council will only use this form of surveillance as a last resort. However if it appears that use of a CHIS may be required, Authorising Officers must seek legal advice from the Solicitor to the Council.

9.2 A CHIS could be an informant or an undercover officer carrying out covert enquiries on behalf of the Council. However, the provisions of the 2000 Act are not intended to apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information such as the Benefit Fraud Hot Line. Members of the public acting in this way would not generally be regarded as sources.

9.3 Under section 26(8) of the 2000 Act a person is a source if:

a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);

b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or

c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

9.4 By virtue of section 26(9)(b) of the 2000 Act a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship if, and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

9.5 By virtue of section 26(9)(c) of the 2000 Act a relationship is used covertly, and information obtained as above is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

10. Conduct and Use of a Source

10.1 The **use of a source** involves inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source.

10.2 The **conduct of a source** is any conduct falling within section 29(4) of the 2000 Act, or which is incidental to anything falling within section 29(4) of the 2000 Act.

10.3 The **use of a source** is what the Authority does in connection with the source and the **conduct** is what a source does to fulfill whatever tasks are given to them or

which is incidental to it. **The Use and Conduct require separate consideration before authorisation.**

10.4 When completing applications for the use of a CHIS, the applicant must state who the CHIS is, what they can do and for which purpose.

10.5 When determining whether a CHIS authorisation is required, consideration should be given to the covert relationship between the parties and the purposes mentioned in 9.3 (a), (b), and (c) above.

Management of Sources

10.6 Within the provisions there has to be;

(a) a person who has the day to day responsibility for dealing with the source and for the source's security and welfare **(Handler)**

(b) at all times there will be another person who will have general oversight of the use made of the source **(Controller)**

(c) at all times there will be a person who will have responsibility for maintaining a record of the use made of the source

NOTE If, exceptionally, a CHIS authority is required, all of the staff involved in the process should make themselves fully aware of the CHIS Codes of Practice

Management Responsibility

10.8 The Council will ensure that arrangements are in place for the proper oversight and management of sources including appointing a Handler and Controller for each source prior to a CHIS authorisation.

10.9 It is envisaged that the use of a CHIS will be infrequent. Should a CHIS application be made, the CHIS Codes of Practice should be consulted to ensure that the Council can meet its management responsibilities.

Security and Welfare

10.10 The Council has a responsibility for the safety and welfare of the source and for the consequences to others of any tasks given to the source. Before permitting the use or conduct of a source, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorisation, should also be considered at the outset.

Record Management for CHIS

10.11 Proper records must be kept of the authorisation and use of a source. The particulars to be contained within the records are;

(a) the identity of the source;

(b) the identity, where known, used by the source;

(c) any relevant investigating authority other than the authority maintaining the records;

(d) the means by which the source is referred to within each relevant investigating authority;

(e) any other significant information connected with the security and welfare of the source;

(f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;

(g) the date when, and the circumstances in which the source was recruited;

(h) the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);

(i) the periods during which those persons have discharged those responsibilities;

(j) the tasks given to the source and the demands made of him in relation to his activities as a source;

(k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

(l) the information obtained by each relevant investigating authority by the conduct or use of the source;

(m) any dissemination by that authority of information obtained in that way; and

(n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

Juvenile Sources

10.12 Special safeguards apply to the use or conduct of juvenile sources (i.e. those under the age of 18). On no occasion can a child under 16 years of age be authorised to give information against his or her parents or any person with parental responsibility for him or her. Only the Chief Executive can authorise a juvenile source.

10.13 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

Test Purchases

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

10.15 Authorising Officers should consider the likelihood that the test purchase will lead to a relationship being formed with a person in the shop. If the particular circumstances of a particular test purchase are likely to involve the development of a relationship Authorising Officers must seek legal advice from the SRO.

Anti-Social Behaviour Activities

10.16 As from 1 November 2012 there is no provision for a Local Authority to use RIPA to grant lawful authority for he conduct of covert surveillance for disorder such as anti-social behaviour, unless there are criminal offences involved which attract a maximum custodial sentence of six months. Should it be necessary to conduct covert surveillance for disorder which does not meet the serious crime criteria of a custodial sentence of a maximum of six months, this surveillance would be classed as surveillance outside of RIPA, and would still have to meet the Human Rights Act provisions of Necessity and Proportionality?

10.17 Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (eg. the decibel level) so long as it does not record private information is unlikely to require authorisation.

11. THE ROLE OF THE RIPA CO-ORDINATOR

11.1 Key Responsibilities of the RIPA Co-ordinator

- In this document the RIPA Co-ordinator is the Director of Corporate Support Services/Solicitor to the Council. The key responsibilities of the RIPA Co-ordinator are to:

- Retain all applications for authorisation (including those that have been refused), renewals and cancellations for a period of at least **three years** together with any supplementary documentation;

- Provide a unique reference number and maintain the central register of all applications for authorisations whether finally granted or refused (see section below);

- Create and maintain a spreadsheet for the purpose of identifying and monitoring expiry dates and renewal dates although the responsibility for this is primarily that of the officer in charge and the Authorising Officer;

- Monitor types of activities being authorised to ensure consistency and quality throughout the Council;

- Ensure sections identify and fulfil training needs;

- Periodically review Council procedures to ensure that they are up to date;

- Assist Council employees to keep abreast of RIPA developments;

- Provide a link to the Surveillance Commissioner and disseminate information on changes on the law, good practice etc. Officers becoming aware of such information should, conversely, send it to the RIPA Co-ordinator for this purpose;

- Check that Authorising Officers carry out reviews and cancellations on a timely basis.

Central Record of Authorisations

11.2 A centrally retrievable record of all authorisations will be held by the RIPA Co-ordinator which must be up-dated whenever an authorisation is granted, renewed or cancelled. These records will be retained for a period of **three years** from the ending of the authorisation and will contain the following information:

- the type of authorisation;
- the date the authorisation was given;
- the name and title of the Authorising Officer;
- the unique reference number of the investigation (URN);

- the title of the investigation or operation, including a brief description and the names of the subjects, if known;
- whether the urgency provisions were used and if so why;
- whether the investigation will obtain confidential information;
- whether the authorisation was granted by an individual directly involved in the investigation;
- the dates the authorisation is reviewed and the name and title of the Authorising Officer;
- if the authorisation is renewed, when it was renewed and the name and title of the Authorising Officer;
- the date the authorisation was cancelled.
- joint surveillance activity where Council staff have been authorised on another agencies authorisation will also be recorded.

11.2 Access to the data will be restricted to the RIPA Co-ordinator and Authorising Officers to maintain the confidentiality of the information.

12. AUTHORISATION PROCEDURES

12.1 Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation.

Authorising Officers

12.2 Forms can only be signed by Authorising Officers. The Authorising Officers are:

Director of Corporate Services/Solicitor to the Council	Colleen O'Boyle
Assistant to the Chief Executive	Ian Willett

12.3 Authorisations under RIPA are separate from delegated authority to act under the Council's Scheme of Delegation and any internal departmental Schemes of Management.

12.4 RIPA authorisations are for specific investigations only, and must be renewed or cancelled once the specific surveillance is complete or about to expire. **The authorisations do not lapse with time.**

12.5 Authorisations are for 1, 3 or 12 months but should be cancelled promptly if completed within that timescale.

12.6 Authorising Officers should not normally be responsible for authorising operations in which they are directly involved. In such a case the centrally retrievable record of authorisations should highlight this and the attention of a Commissioner or Inspector should be drawn to it during the next inspection.

Training

12.7 The SRO will maintain a Register of Authorising Officers and details of training undertaken by them.

12.8 The SRO will maintain records of RIPA training to staff either internally or externally sourced

.

Grounds for Authorisation

12.9 On 1 November 2012 two significant changes came into force that effects how local authorities use RIPA.

- **Approval of Local Authority Authorisations under RIPA by a Justice of the Peace**: The amendments in the Protection of Freedoms Act 2012 mean

that local authority authorisations under RIPA for the use of Directed Surveillance or use of Covert Human Intelligence sources (CHIS) can only be given effect once an order approving the authorisation has been granted by a Justice of the Peace (JP). **This applies to applications and renewals only, not reviews and cancellations.**

- **Directed surveillance crime threshold**: Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that a local authority can now only grant an authorisation under RIPA for the use of **Directed Surveillance** where the local authority is investigating criminal offences which attract a maximum custodial sentence of six months or more or criminal offences 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.

NOTE: The crime threshold, as mentioned is only for Directed Surveillance.

12.10 Also, the **only** lawful reason is for granting a RIPA authorisation available to local authorities is the **prevention and detection of crime** in respect of its Core Functions.

13. APPLICATION PROCESS

13.1 No covert activity covered by RIPA or the use of a CHIS should be undertaken at any time unless it meets the legal criteria (see above) and has been authorised by an Authorising Officer and approved by a JP/Magistrate as mentioned above. The activity conducted must be in strict accordance with the terms of the authorisation.

13.2 The applicant will complete the current application form for Directed surveillance or CHIS and the required section of the judicial application/order form.
The applicant will submit them in an envelope marked Private & Confidential to an Authorising Officer.

13.3 If the Authorising Officer grants the application – with or without further information from the Applicant, the applicant will liaise with Legal Services to arrange with Her Majesty's Courts & Tribunals Service (HMCTS) a hearing.

13.4 The hearing will be in private and heard by a single JP.

13.5 The applicant will present to the JP the partially completed judicial application/order form, a copy of the RIPA application/authorisation form, together with any supporting documents setting out the case e.g. proof of the Authorising officer's designation, and the original application/authorisation form.

13.6 The original RIPA application/authorisation should be shown to the JP but will be retained by the local authority 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).

13.7 The JP may have questions to clarify points application **However the forms and supporting papers must by themselves make the case. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported in the papers provided**.

13.8 The JP 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 local authority and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

13.9 The JP may decide to

(a) Approve the Grant or renewal of an authorisation

The grant or renewal of the RIPA authorisation will then take effect and the local authority may proceed to use the technique in that particular case.

(b) Refuse to approve the grant or renewal of an authorisation

The RIPA authorisation will not take effect and the local authority may **not** use the technique in that case.

Where an application has been refused the applicant may wish to consider the reasons for that refusal and whether any defects can be remedied.

For, a technical error, the form may be remedied without going through the internal authorisation process again. The officer may then wish to reapply for judicial approval once those steps have been taken.

(c) Refuse to approve the grant or renewal and quash the authorisation or notice

This applies where the JP refuses to approve the application/authorisation or renew the application/authorisation and decides to quash the original authorisation or notice. However the court must not exercise its power to quash the application/authorisation unless the applicant has had at least 2 business days from the date of the refusal in which to make representations. If this is the case the officer will inform the Legal section who will consider whether there are grounds to make representations.

The JP will record any decision on the order section of the judicial application/order form. The court administration will retain a copy of the local authority RIPA application and authorisation form and the judicial application/order form. The officer will retain the original application/authorisation and a copy of the judicial application/order form.

If approved by the JP, the date of the approval becomes the commencement date and the three months duration will commence on this date.

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.

A local authority may only appeal a JP decision on a point of law by judical review. If such a concern arises Legal Services must be consulted.

If it is intended to undertake both directed surveillance and the use of a CHIS 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.

An application for an authorisation must include an assessment of the risk of any collateral intrusion or interference. The Authorising Officer will take this into account, particularly when considering the proportionality of the directed surveillance or the use of a CHIS.

Application, Review, Renewal and Cancellation Forms

13.10 Applications

All the relevant sections on an application form must be completed with sufficient information for the Authorising Officer 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.**

13.11 Duration of Applications

Directed Surveillance	3 Months
Renewal	3 Months
Covert Human Intelligence Source	12 Months
Juvenile Sources	1 Month
Renewal	12 months

NOTE: All Authorisations must be cancelled by completing a cancellation form. They must not be left to simply expire.

Reviews

13.12 An Authorising Officer conducts a review to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

13.13 In each case the Authorising Officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable and they will record when they are to take place on the application form. This decision will be based on the circumstances of each application

13.14 Applicants should submit a review form by the review date set by the Authorising Officer. They should also use a review form for changes in circumstances to the original application so that the need to continue the activity can be reassessed. However if the circumstances or the objectives have changed considerably, or the techniques to be used are now different a new application form should be submitted and will be required to follow the process again and be approved by a JP.

13.15 The applicant does not have to wait until the review date if it is being submitted for a change in circumstances.

Renewal

13.16 Should it be necessary to renew a Directed Surveillance or CHIS application/authorisation, this must be approved by a JP.

13.17 The applicant should complete all the sections within the renewal form and submit the form to the authorising officer.

13.18 Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusion issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

13.19 If the Authorising Officer refuses to renew the application the cancellation process should be completed. If the Authorising Officer authorises the renewal of the activity the JP process is to be followed as before**. A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.**

.

Cancellation

13.20 The cancellation form is to be submitted by the applicant or another investigator in their absence. The Authorising Officer who granted or last renewed the authorisation must cancel it if they are satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Where the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer

13.21 As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer.. . The date and time of cancellation should also be recorded in the central record of authorisations (see paragraph 5.18 in the Codes of Practice). **It will also be necessary to detail the amount of time spent on the surveillance as this is required to be retained by the Senior Responsible Officer.**

13.22 The officer submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and what if any images were obtained and any images containing third parties. The Authorising Officer should then take this into account and issue instructions regarding the management and disposal of the images etc.

13.23 The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what they stated was necessary in the application form. This check will form part of the oversight function. Where issues are identified they will be brought to the attention of the line manager and the Senior Responsible Officer (SRO). This will assist with future audits and oversight.

14 Notes for Authorising Officers

14.1 Before an Authorising Officer signs a Form, they must:-

(a) be mindful of this Policy & Procedures Document and the training undertaken;

(b) be satisfied that the RIPA authorisation is:-

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

(ii) **necessary** in the circumstances of the particular case on the ground mentioned; **and**

(iii) **proportionate** to what it seeks to achieve.

(c) In assessing whether or not the proposed surveillance is proportionate, consider other appropriate means of gathering the information.

14.2 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render actions proportionate. Similarly, an offence may be so minor that any covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

14.4 The following elements of proportionality should therefore be considered:

- balance the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explain how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- consider whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidence, what other methods have been considered and why they were not implemented.

NOTE: The least intrusive method will be considered proportionate by the courts.

14.5 Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (**collateral intrusion**). Measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion. This matter may be an aspect of determining proportionality;

14.6 Set a date for review of the authorisation and review on only that date;

14.7 Obtain a Unique Reference Number (URN) for the application from the SRO

14.8 Ensure that a copy of the RIPA Forms (and any review/cancellation of the same) is forwarded to the SRO for the Central Register, **within 5 working days of the relevant authorisation, review, renewal, cancellation or rejection.**

Additional Safeguards when Authorising a CHIS

14.9 When authorising the conduct or use of a CHIS, the Authorising Officer must also:-

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

(b) Be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS and this must address health and safety issues through a risk assessment;

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

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

(e) Ensure **records** contain particulars and are not available except on a need to know basis.

(f) Ensure that if the CHIS is under the age of 18 the Authorising Officer has the approval of the Chief Executive.

NOTE: It is strongly recommended that legal advice is obtained in relation seeking or granting the authorisation of a CHIS.

14. WORKING WITH / THROUGH OTHER AGENCIES

14.1 Anyone other than a Council officer instructed to undertake any action under RIPA, on our behalf must be advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do and be provided with a copy of the application form (redacted if necessary) or at the least the authorisation page containing the unique number.

14.2 Equally, if Council staff are authorised on another agencies RIPA authorisation, the staff will obtain a copy of the application form (redacted if necessary), or at the least the authorisation page containing the unique number, a copy of which should be forwarded for filing within the central register. They must ensure that they do not conduct activity outside of that authorisation.

14.3 The Council has a CCTV policy which covers its usage and this is separately inspected by the Commissioner/ Inspectors

15. RECORD MANAGEMENT

15.1 The Council must keep detailed records of all authorisations, renewals, cancellations and rejections in Departments and a Central Register of all Authorisation Forms will be maintained and monitored by the SRO. The following documents must be retained:

- a copy of the Forms together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the Authorising Officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction was given by the Authorising Officer;
- the Unique Reference Number for the authorisation (URN).
- Any JP decision Notice

15.2 Authorising Officers must forward a copy of the form to the SRO for the Central Register, within 5 working days of the authorisation, review, renewal, cancellation or rejection.

Retention and Destruction of Material

15.3 Arrangements are in place for the secure handling, storage and destruction of material obtained through the use of covert surveillance..

15.4 The Council will retain records for a period of at least three years from the ending of the authorisation. The Office of the Surveillance Commissioners (OSC) can audit/review the Council's policies and procedures, and individual authorisations.

15.5 The Office of the Surveillance Commissioners will also write to the Council from time to time, requesting information as to the numbers of authorisations made in a specific period. It will be the responsibility of the SRO to respond to such communications.

Errors

15.6 The Council has a responsibility to report to the Inspector at the commencement of an inspection all activity which should have been authorised but wasn't. This does not apply to covert activity which is deliberately not authorised because an Authorising Officer considers that it does not meet the legislative criteria, but allows it to continue. This would be surveillance outside of RIPA.

Acquisition of Communications Data

15.7 This Council does not access communications in a way that requires RIPA authorisation. For further information as to how evidence is gathered contact the Assistant Director (Finance). The link to the forms in Appendix C is reproduced for completeness.

16. CONCLUSION

16.1 RIPA authorisation gained through this policy/procedure document will protect human rights and protect the Council against challenges for breaches of Article 8 of the European Convention on Human Rights.

16.2 Authorising Officers will be suitably trained and they will never sign or rubber stamp Form(s) without thinking about their personal and the Council's responsibilities.

16.3 For further advice and assistance on RIPA, please contact the Director of Corporate Support Services/Solicitor to the Council or the Assistant to the Chief Executive.

APPENDIX 1

A FORMS

DIRECTED SURVEILLANCE

All forms can be obtained from:

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

The form has to be downloaded and completed in the applicant's handwriting. The Authorising Officer must also complete the relevant section of the form in handwriting. The original form has to be passed to the SRO.

Application for Authorisation Directed Surveillance

Application for Review of a Directed Surveillance Authorisation

Application for Renewal of a Directed Surveillance Authorisation

Application for Cancellation of a Directed Surveillance Authorisation

APPENDIX 2

B FORMS

CONDUCT OF A COVERT HUMAN INTELLIGENCE SOURCE

All forms can be obtained from:

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

The form has to be downloaded and completed in the applicant's handwriting. The Authorising Officer must also complete the relevant section of the form in handwriting. The original form has to be passed to the SRO.

Application for Authorisation of the conduct or use of a Covert Human Intelligence Source (CHIS).

Application for Review of a Covert Human Intelligence Source (CHIS) Authorisation.

Application for renewal of a Covert Human Intelligence Source (CHIS) Authorisation.

Application for Cancellation of an authorisation for the use or Conduct of a Covert Human Intelligence Source.

APPENDIX 3

C FORMS

ACQUISITION OF COMMUNICATIONS DATA

All forms can be obtained from the Home Office: RIPA Codes of Conduct website: http://www.homeoffice.gov.uk/counter-terrorism/ripa-forms/

The form has to be downloaded and completed in the applicant's handwriting. The Authorising Officer must also complete the relevant section of the form in handwriting. The original form has to be passed to the SRO

Part I Chapter II request schedule for subscriber information

Specimen Part I Chapter II authorisation

Specimen Part I Chapter II Notice

Chapter II application for communications data

Guidance notes regarding chapter II application form

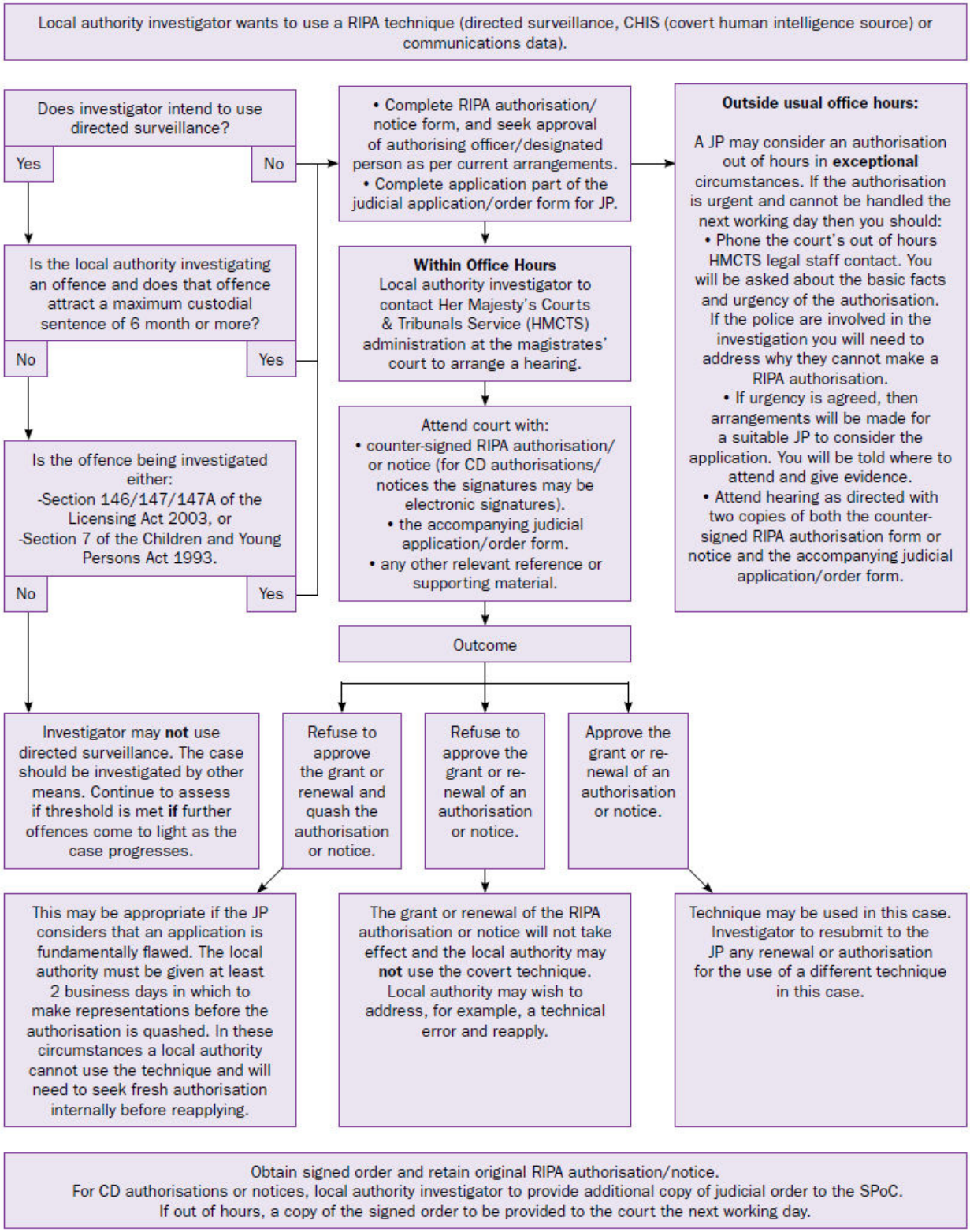
RIPA Section 22 notice to obtain communications data from communications service providers

Reporting an error by a CSP to the IOCCO

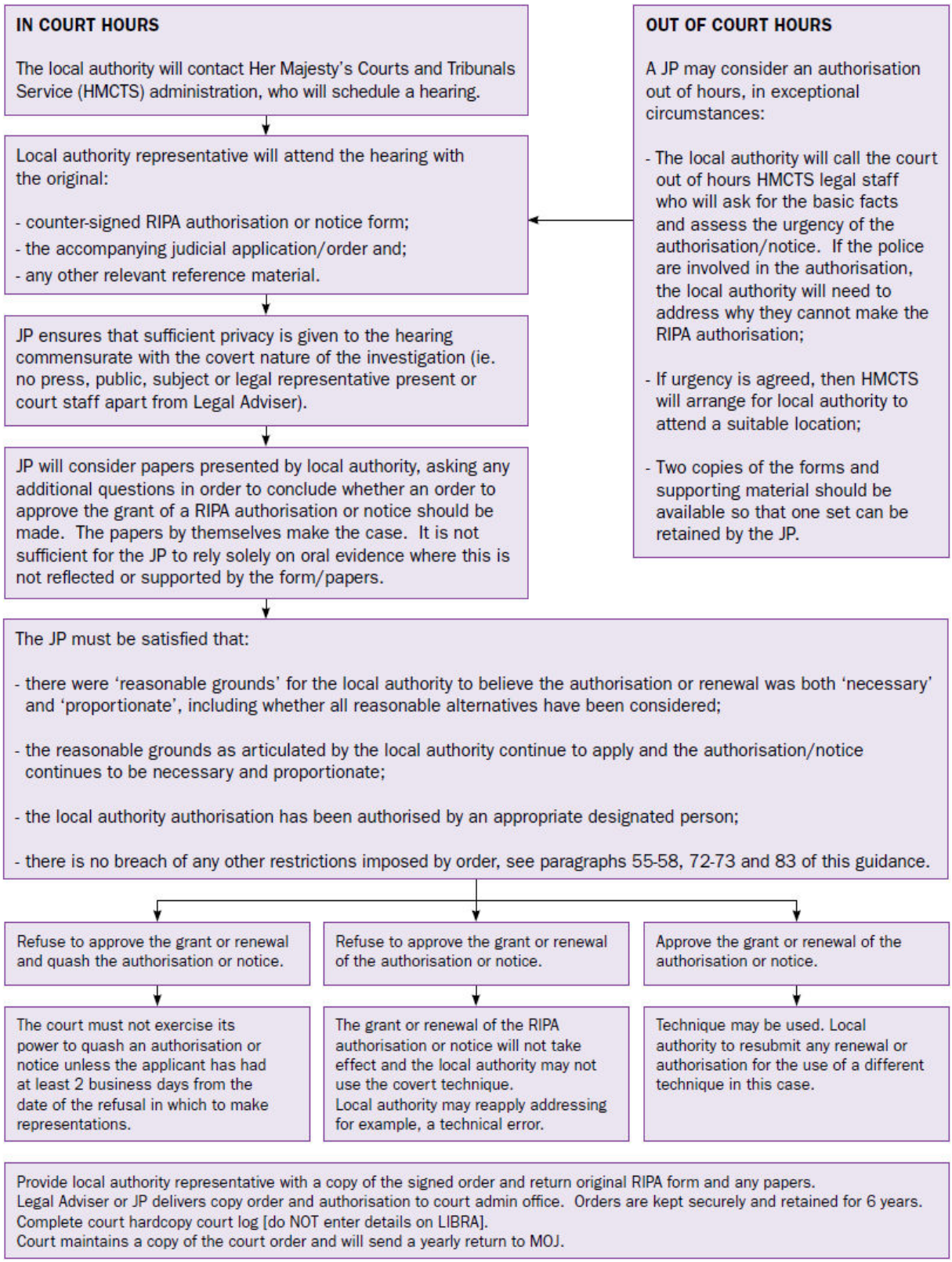
Reporting an error by a public authority to the IOCCO

Annex A

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



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



Annex B Application for Judicial Approval and Order Form

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

Local thority:.....

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: