Taunton Deane Borough Council

Corporate Governance Committee – 19 May 2014

Regulation of Investigatory Powers Act – Policy and Procedures updated

Report of the Assistant Chief Executive & Monitoring Officer
(This matter is the responsibility of the Leader Councillor John Williams**)**

1. Executive Summary

The Council's policy needs to be updated to reflect the amendments made to the Regulation of Investigatory Powers Act 2000 (RIPA) by the The Protection of Freedoms Act 2012. In addition changes also need to be made to reflect the Council's new management structure and the appropriate authorising officers.

2. Background

2.1 The council has had a corporate policy dealing with the Regulation of Investigatory Powers Act 2000 since July 2008.

2.2 The Policy details various aspects of the legislation and guides officers and the relevant processes and procedures that need to be followed. In addition, it also sets out details of the relevant authorising officers for the Council.

2.3 In 2012, the Protection of Freedoms Act made amendments to RIPA to provide that following authorisation by an authorised Council officer to use the Act no surveillance can be conducted until that authorisation is approved by a Justice of the Peace. Therefore the Council's policy needs to be updated to reflect this change in process.

2.4 In addition, following the changes to the Council's management structure new officers are required to be authorising officers and the policy has been updated to reflect these changes.

3. Finance Comments

3.1 There are no financial implications in this report.

4. Legal Comments

4.1 The Council must ensure that it follows the procedures set out in this policy. A failure to do so may lead to evidence being inadmissible or the Council being guilty of maladministration.

5. Links to Corporate Aims (Please refer to the current edition of the Corporate Strategy)

5.1 There are no direct links to the Council's corporate aims.

6. Environmental Implications (If appropriate, consider impact on: carbon emissions; gas / electricity / other fuel usage including transport; biodiversity; and water and air quality. If appropriate, also consider adaptation requirements to the longer term impacts and opportunities of climate change such as increased heat and water stress, more flooding and stronger, more damaging wind speeds)

6.1 There are no environmental implications in this report.

7. Community Safety Implications (if appropriate, such as measures to combat anti-social behaviour)

7.1 There are no community safety implications in this report, although there will be community safety implications in assessing any applications under this policy.

8. Equalities Impact (An Equalities Impact Assessment should be carried out in respect of:-

- New initiatives/projects with an impact on staff, service or non-service users;
- New services/changes to the way services are delivered;
- New or refreshed Strategies;
- Events – Consultation/Training; and
- Financial/budget decisions.

8.1 There are no equalities impacts in this report.

9. Risk Management (if appropriate, such as reputational and health and safety risks. If the item the subject of the report has been included in a Service Plan, the result of the risk assessment undertaken when the plan was prepared should be entered here.

9.1 If the policy is not followed then the Council may suffer a risk to its reputation. In addition health and safety must be assessed as part of any authorisation request.

10. Partnership Implications (if any)

10.1 There are no partnership implications within this report.

11. Recommendations

11.1 The Committee are recommended to approve the policy as set out in Appendix 1 of this report.

Contact: Bruce Lang,
Assistant Chief Executive & Monitoring Officer
01823 356391
BDLang@westsomerset.gov.uk

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

ISSUE DETAILS	
TITLE:	**RIPA Policy & Procedures Guide**
VERSION CONTROL	1.2 dated 3rd July 2008 1.3 dated 20 February 2009 1.4 dated March 2009 1.5 dated June 2010 (FINAL) 1.6 dated February 2014 (updated)
OWNER	Assistant Chief Executive and Monitoring Officer
APPROVED By:	Corporate Governance Committee 19 May 2014
REVIEW DATE	(1) March 2015 (2) March 2016

Contact: Bruce Lang
Assistant Chief Executive & Monitoring Officer
Taunton Deane Borough Council
The Deane House
Belvedere Road
Taunton TA1 1HE

Tel: 01823 356391 E-mail: BDLang@westsomerset.gov.uk

CONTENTS PAGE

A. Introduction and Key Messages

1. This Policy & Procedures Document is based upon the requirements of the Regulation of Investigatory Powers Act 2000 ('RIPA') and the Home Office's Code of Practices on Covert Surveillance and Covert Human Intelligence Sources (covert surveillance would be used only rarely and in exceptional circumstances).

2. The authoritative position on RIPA is, of course, the Act itself and any Officer who is unsure about any aspect of this document should contact, at the earliest possible opportunity, the Monitoring Officer, for advice and assistance.

3. Copies of this document and related forms will be placed on the intranet, once this Document has been approved by the Council and the Office of Surveillance Commissioners. This guide (but not the RIPA forms or the list of Authorising Officers) will be placed on the TDBC website.

4. The Monitoring Officer will maintain (and check) the Corporate Register of all RIPA authorisations, reviews, renewals, cancellations and rejections. However, it is the responsibility of the relevant Authorised Officer to ensure that the Monitoring Officer receives a copy of the relevant forms within 1 week of authorisation, review, renewal, cancellation or rejection.

5. RIPA and this document are important for the effective and efficient operation of the Council's actions with regard to covert surveillance and Covert Human Intelligence Sources. This document will, therefore, be kept under 12-monthly review by the Monitoring Officer. Authorised Officers must bring any suggestions for the improvement of this document to the attention of the Monitoring Officer at the earliest possible opportunity. The Council takes responsibility for ensuring that RIPA procedures are continuously improved.

6. The Monitoring Officer is the Council's nominated Single Point of Contact (SPOC) Officer who will be the normal point of contact for the Surveillance Commissioner and will field enquiries relating to RIPA.

7. If you are in any doubt on RIPA, this document or the related legislative provisions, please consult the Monitoring Officer or at the earliest possible opportunity.

8. This policy will be approved and monitored by the Corporate Governance Committee on a regular basis.

B. Council Policy Statement

1. The Council takes its statutory responsibilities seriously and it will at all times act in accordance with the law and take action that is both necessary and proportionate to the discharge of such statutory responsibilities. In that regard, the Monitoring Officer is duly authorised by the Council to keep this document up to date and to amend, delete, add or substitute relevant provisions, as necessary. For administrative and operational effectiveness, the Monitoring Officer is also authorised to add or substitute Officers authorised for the purposes of RIPA.

C. Effective Date of Operation : 1 March 2009 and Authorised Officer Responsibilities

1. The Corporate Policy, Procedures and the forms provided in this document will become operative with effect from the date of the Policy's approval.

2. Prior to the operative date, the Monitoring Officer will ensure that sufficient numbers of Authorised Officers are (after suitable training on RIPA and this document) duly certified to take action under this document.

3. Authorised Officers will also ensure that staff who report to them follow this Policy & Procedures Document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document.

4. Authorised Officers must also pay particular attention to Health and Safety issues that may be raised by any proposed surveillance activity. Under no circumstances should an Authorised Officer approve any RIPA form unless and until s/he is satisfied that the health and safety of Council employees has been suitably addressed, and/or risks minimised so far as is possible, and that those health and safety considerations and risks are proportionate to/with the surveillance being proposed. If an Authorised Officer is in any doubt, s/he should obtain prior guidance.

5. Authorised Officers must also ensure that when sending copies of any forms to the Monitoring Officer, (or any other relevant authority), the same are sent in SEALED envelopes and marked 'Strictly Private & Confidential'.

D. General Information on RIPA

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

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

    (a) in accordance with the law;

    (b) necessary (as defined in this document); and

    (c) proportionate (as defined in this document).

3. The Regulation of Investigatory Powers Act 2000 ('RIPA') provides a statutory mechanism (i.e. 'in accordance with the law') for authorising covert surveillance and the use of a 'covert human intelligence source' ('CHIS') - e.g. undercover agents, informers. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, RIPA seeks to ensure that both the public interest and the human rights of individuals are suitably balanced.

4. Directly employed Council staff and external agencies working for the Council are covered by RIPA during the time they are working for the Council. Therefore, all external agencies must comply with RIPA and work carried out by agencies on the Council's behalf must be properly authorised by one of the Council's designated Authorised Officers. Authorised Officers are those whose posts appear in Appendix (1) to this document (as added to or substituted by the Monitoring Officer).

5. If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration may be made to the Ombudsman, and/or the Council may be ordered to pay compensation. Were this to happen the good reputation of the Council will be damaged and it will undoubtedly be the subject of adverse press and media interest. Therefore, it is essential that all involved with RIPA comply with this document and any further guidance that may be issued from time to time by the Monitoring Officer.

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

E. What RIPA Does and Does Not Do

1. RIPA does:

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

2. RIPA does not:

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

3. If the Authorised Officer or any Applicant is in any doubt, s/he should ask the Monitoring Officer before any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

F. Types of Surveillance

1. 'Surveillance' includes

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

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

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

Surveillance can be overt or covert.

2. Overt Surveillance

Most of the surveillance carried out by the Council will be done overtly - there will be nothing secretive, clandestine or hidden about it. In many cases, Officers will be behaving in the same way as a normal member of the public and/or will be going about Council business openly.

3. Similarly, surveillance will be overt if the subject has been told it will happen.

4. Covert Surveillance

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

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

6. Directed Surveillance

Directed Surveillance is surveillance which:-

- is covert; and

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

- is not carried out in 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; and

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

7. Private information in relation to a person includes any information relating to his private and family life, his home and his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance 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.

8. Similarly, although overt town centre CCTV cameras do not normally require authorisation, authorisation will be required if the camera is tasked for a specific purpose which involves prolonged surveillance on a particular 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.

9. For the avoidance of doubt, only those Officers designated and certified to be 'Authorised Officers' for the purpose of RIPA can authorise 'Directed Surveillance' if, and only if, the RIPA authorisation procedures detailed in this document are followed. If an Authorised Officer has not been 'certified' for the purposes of RIPA, s/he cannot carry out or approve/reject any action set out in this Corporate Policy & Procedures Document.

   Further, an Authorised Office for RIPA purposes cannot delegate his/her power of authorisation to another officer unless that officer is also an Authorised Officer for RIPA purposes (and listed in Appendix 1), in which case that officer would be authorising in his own right. If in doubt, check with the Monitoring Officer. Officers will bear personal responsibility for ensuring correct RIPA authorisation procedures.

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

11. Intrusive Surveillance

This is 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.

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

13. Examples of different types of Surveillance

Type of Surveillance	Examples
Overt	- Police Officer or Parks Warden on patrol. - Signposted Town Centre CCTV cameras (in normal use). - Most test purchases (where the officer behaves no differently from a normal member of the public).
Covert but not requiring prior authorisation	- CCTV cameras providing general traffic, crime or public safety information.
Directed (must be RIPA authorised)	- Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit or genuinely on long term sick leave from employment. - Test purchases where the officer has a hidden camera or other recording device to record information which might include information about the private life of a shop-owner, e.g. where s/he is suspected of running his business in an unlawful manner.
Intrusive - (Council cannot do this)	- Planting a listening or other device (bug) in a person's home or in their private vehicle.
(See Appendix 6)	(Examples of different types of surveillance)

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

Who is a CHIS?

1. Someone who establishes or maintains a personal or other relationship for the covert purpose of covertly using or covertly disclosing information obtained by that relationship. In common parlance, an informer or 'under cover' Council Officer.

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

What must be authorised?

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

   - Conduct of a CHIS = Establishing or maintaining a personal or other relationship with a person for the covert purpose of (or incidental to the covert purpose of) obtaining and passing on information.

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

4. The Council can use CHIS's if, and only if, the RIPA procedures, detailed in this document are followed.

Juvenile Sources

5. 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.

Vulnerable Individuals

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

7. A Vulnerable Individual will only be authorised to act as a source in the most exceptional of circumstances.

Test Purchases

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

9. By contrast, developing a relationship with a person in the shop to obtain information about the seller's suppliers of an illegal product (e.g. illegally imported products) will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance. A combined authorisation can be given for a CHIS and also for directed surveillance.

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

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

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

    Noise recordings should only ever be made from a complainant’s property or land that is open to the pubic. Covert recording within the premises of the alleged noise-maker would constitute Intrusive Surveillance, and is not permitted for Council Staff.

H. Authorisation Procedures

1. Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised and in strict accordance with the terms of the authorisation. Appendix (2) provides a flow chart of the authorisation process from application consideration to recording of information.

2. The Regulation of Investigatory Powers (Directed Surveillance and Cover Human Intelligence Sources) (Amendment) Order 2012 (made on 11 June 2012) comes into force on 1st November 2012 and will further restrict the Council's powers to grant a RIPA authorisation.

3. From this date authorisations can only be granted where the authorisation is for the purpose of preventing or detecting crime and that crime constitutes one or more criminal offences. Additionally the criminal offences being contemplated must be ones which are punishable by a prison sentence of at least six months. There are exceptions to this requirement covering various offences under s146 and s147 Licensing Act 2003 (effectively selling alcohol to children).

4. On 1st May 2012, the Protection of Freedoms Bill received Royal Assent to become the Protection of Freedoms Act 2012.

5. The Protection of Freedoms Act 2012 (Commencement No.2) Order 2012 (SI 2012/2075) ('the Order') was made on 7th August 2012 bringing in various provisions of the Protections of Freedoms Act 2012 into force during 2012.

6. Article 4 of the Order commences amendments to the Regulation of Investigatory Powers Act 2000 ("RIPA") on 1st November 2012.

7. The amendment in respect of RIPA authorisations is that when an authorisation is granted it will not take effect until such time (if any) as a Justice of the Peace has made an order approving the grant of the authorisation.

Authorised Officers

8. Forms can only be signed by Authorised Officers who hold a Certificate of RIPA Eligibility from the Monitoring Officer as shown in Appendix (3). Authorised Officer posts are listed in Appendix (1). This Appendix will be kept up to date by the Monitoring Officer and added to as needs require. The Monitoring Officer has been duly authorised to add, delete or substitute posts listed in Appendix (1).

9. As already mentioned, RIPA authorisations are for specific investigations only, and they must be renewed or cancelled once the specific surveillance is complete or about to expire. The authorisations do not lapse with time!

Training Records

10. Proper training will be given or approved by the Monitoring Officer before Authorised Officers are issued with a Certificate of RIPA Eligibility enabling them

to sign any RIPA forms. The issue of a Certificate of RIPA Eligibility will also have the dual purpose of confirming that the Officer has been RIPA trained and a Corproate Register of all those individuals who have been issued with such Certificates will be kept by the Monitoring Officer.

11. If the Monitoring Officer feels at any time that an Authorised Officer has not complied fully with the requirements of this document, or the training provided to him, the Monitoring Officer is duly authorised to retract that Officer's Certificate of RIPA Eligibility until s/he has undertaken further approved training. Were this to happen the Officer could no longer authorise RIPA Procedures.

Application Forms

12. Only the approved RIPA forms set out in this document must be used.

For the most up to date forms see:-

http://www.homeoffice.gov.uk/government/collections/ripa-forms-2

Grounds for Authorisation

13. Directed Surveillance or the Conduct and Use of the CHIS can be authorised by the Council only for the prevention or detection of crime or preventing disorder.

Assessing the Application Form

14. Before an Authorised Officer signs a form, they must:

(a) Be mindful of this Policy & Procedures Document, the training provided or approved by the Monitoring Officer and any other guidance issued, from time to time, by the Monitoring Officer on such matters;

(b) Satisfy themselves that the RIPA authorisation is:

(i) in accordance with the law;
(ii) necessary in the circumstances of the particular case on one of the grounds mentioned in paragraph 13 above; 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. The least intrusive method will be considered proportionate by the courts.

(d) Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (Collateral Intrusion). Measures must be taken wherever practicable to avoid or minimise (so far as is possible) unnecessary collateral intrusion into the lives of those not directly connected with the investigation or operation. This matter may be an aspect of determining proportionality;

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

(f) Allocate a Unique Reference Number (URN) for the application as follows:
Year / Group / Number of Application

(g) Ensure that the RIPA Service Register is duly completed, and that a copy of the RIPA forms (and any review/cancellation of the same) is forwarded to the Monitoring Officer for inclusion in the Corporate Register within one week of the relevant authorisation, review, renewal, cancellation or rejection.

Additional Safeguards when Authorising a CHIS

15. When authorising the conduct or use of a CHIS, the Authorised 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 these arrangements 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; and

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

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

17. If an application is granted, the Authorising Officer must set a date for its review, and ensure that it is reviewed on that date. Records must be kept in relation to all RIPA applications and authorisations.

18. By law, an Authorising Officer must not grant authority for the use of a CHIS unless they believe that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the CHIS. Certain particulars must be included in the records relating to each CHIS, and the records must be kept confidential. Further advice should be sought from the Monitoring Officer or the Deputy Monitoring Officer on this point if authority is proposed to be granted for the use of a CHIS.

19. A ‘Surveillance Log Book’ should be completed by the investigating officer(s) to record all operational details of authorized covert surveillance or the use of a CHIS. Once completed, the Log Book should be passed to their relevant RIPA

co-ordinator for safe keeping in a secure place. Each group will also maintain a record of the issue and movement of all Surveillance Log Books.

Urgent Authorisations

20. Urgent authorisations should not be necessary. However, in exceptional circumstances, urgent authorisations may be given orally if the time that will elapse before a written authorisation can be granted will be likely to endanger life or jeopardise the investigation or operation for which the authorisation is being given.

21. It will not be urgent or an exceptional circumstance where the need for authorisation has been neglected or the situation is of the Officer's own making.

22. Urgent authorisations last for no more than 72 hours. They must be recorded in writing on the standard form as soon as practicable and the extra boxes on the form must be completed to explain why the authorisation is urgent.

Duration

23. The form must be reviewed in the time stated, and cancelled once it is no longer needed. The 'authorisation' to carry out/conduct the surveillance lasts for 3 months (from date of authorisation) for Directed Surveillance, and 12 months (from date of authorisation) for a CHIS. Any adjustments to the time period must be made by means of either a cancellation or a renewal.

24. However, whether or not the surveillance is carried out/conducted in the relevant period has no bearing on the authorisation becoming spent. In other words, the forms do not expire! The forms have to be reviewed and/or cancelled (once they are no longer required).

25. An urgent oral authorisation (if not already ratified in a written authorisation) will cease to have effect after 72 hours, beginning with the time when the authorisation was granted.

26. Authorisations shall be renewed in writing when the maximum period has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred.

27. The renewal will begin on the day when the authorisation would have expired. In exceptional circumstances, renewals may be granted orally in urgent cases (but see above) and they last for a period of 72 hours.

I. Working With / Through Other Agencies

1. When another agency has been instructed on behalf of the Council to undertake any action under RIPA, this document and its forms must be used by the Council Officers concerned (in accordance with the normal procedure), the agency advised and kept informed of the various RIPA requirements. They must be made explicitly aware of what they are authorised to do, preferably in writing (with a copy of the written instructions countersigned by the agency by way of acknowledgement of their instructions and returned to the instructing officer). If for reasons of urgency oral instructions are initially given, written confirmation must be sent and acknowledged within 4 working days. Officers must be satisfied that agencies are RIPA competent & RIPA trained before they are used.

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

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

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

3. With regard to 2(a) above, if the Police or other agency wish to use Council resources for general surveillance (as opposed to specific RIPA operations) an appropriate letter requesting the proposed use (and detailing the extent of remit, duration, who will be undertaking the general surveillance and the purpose of it) must be obtained from the Police or other agency before any Council resources are made available for the proposed use. The insurance/indemnity considerations mentioned above may still need to be addressed.

4. In addition should any officer wish to work in partnership with any other agency where the Council intend to share with that other agency any evidence obtained through surveillance activities then the advice of the Monitoring Officer or the Deputy Monitoring Officer should be first sought.

5. If in doubt, please consult with the Monitoring Officer at the earliest opportunity.

J. Records Management

1. The Council must keep a detailed record of all authorisations, renewals, cancellations and rejections generated by officers and a Corporate Register of all Authorisation forms will be maintained and monitored by the Monitoring Officer.

2. Records maintained by individual services

The following documents must be retained:

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

3. Each form will have a URN. The cross-referencing of each URN takes place within the forms for audit purposes. Rejected forms will also have URN's.

Corporate Register maintained by the Monitoring Officer

4. Authorised Officers must forward details of each form to the Monitoring Officer for the Corporate Register within 1 week of the authorisation, review, renewal, cancellation or rejection. The Monitoring Officer will monitor the same and give appropriate guidance from time to time or amend this document, as necessary.

5. 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.

K. Material obtained during investigations

1. Generally, all material (in whatever media) obtained or produced during the course of investigations subject to RIPA authorisations should be processed, stored and destroyed in accordance with the requirements of the Data Protection Act 1998, the Freedom of Information Act 2000, any other legal requirements including those of confidentiality. The following paragraphs give guidance on some specific situations, but advice should be sought from the Monitoring Officer or the Data Protection Officer where appropriate.

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

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

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

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

    - Confidential material should not be retained or copied unless it is necessary for a specified purpose;
    - Confidential material should only be disseminated in accordance with legal advice that it is necessary to do so for a specific purpose;
    - Confidential material which is retained should be marked with a warning of its confidential nature. Safeguards should be put in place to ensure that such material does not come into the possession of any person where to do so might prejudice the outcome of any civil or criminal proceedings;
    - Confidential material should be destroyed as soon possible after its use for the specified purpose.

If there is any doubt as to whether material is of a confidential nature, advice should be sought from the Monitoring Officer.

L. Amendments to this guidance document

1. The Monitoring Officer is duly authorised to keep this guidance document up to date, and to amend, delete, add or substitute any provisions as s/he deems necessary. For administrative and operational effectiveness, s/he is also authorised to amend the list of ‘Authorising Officer Posts” set out in Appendix 1, by adding, deleting or substituting any posts.

2. The RIPA Corporate Officers Working Group shall supplement any training requirements with exchanges of experiences in the operation of this document and any recommendations to improve this document will be considered by the Council’s Monitoring Officer.

M. Complaints Handling

1. Taunton Deane Borough Council's Surveillance Complaints Procedure

Complaints concerning breaches of the code may be made to the Council's Chief Executive, Taunton Deane Borough Council, The Deane House, Belvedere Road, Taunton, Somerset, TA1 1HE.

If a complaint is received from a member of the public or a person who has been subject to any form of surveillance the complaint will be referred to the Monitoring Officer for investigation.

Thereafter a decision will be taken, as to what action, if any, should be taken in line with the Council's Complaints Policy.

2. Independent Tribunal

The Regulation of Investigatory Powers Act 2000 also establishes an independent tribunal made up of Senior Members of the Judiciary and the Legal Profession and is independent of the government. The tribunal has full powers to investigate and decide any case within its jurisdiction. If a complaint is therefore received from an individual who has been subject to surveillance or by a member of the public then that person or persons should be referred immediately to the Investigatory Powers Tribunal.

The address for the Investigatory Powers Tribunal is PO Box 33220 London SW1H 9ZQ.

N. Useful contacts

6.1 Local Authorities Coordinators of Regulatory Services (LACORS) - www.lacors.gov.uk

6.2 Office of the Surveillance Commissioner – https://osc.independent.gov.uk/

6.3 RIPA forms- https://www.gov.uk/government/collections/ripa-forms--2

6.4 RIPA codes of practice- https://osc.independent.gov.uk/

6.5 RIPA home office guidance – https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa

O. Concluding Remarks of the Monitoring Officer

1. Where there is an interference with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority for the interference, or if it is held not to be necessary or proportionate to the particular circumstances, the consequences of not obtaining or following the correct authorisation procedure set out in RIPA and this document may be that the action taken (and the evidence obtained) will be held to be unlawful by the Courts pursuant to Section 6 of the Human Rights Act 1998. This could result in the Council losing a case and having costs (and possibly damages) awarded against it.

2. Obtaining an authorisation under RIPA and following the procedures set out in this document will ensure that the particular action taken is carried out in accordance with the law and subject to stringent safeguards against abuse of anyone's human rights.

3. Authorised Officers will be suitably trained and they must exercise their minds every time they are asked to sign a form. They must never sign or rubber stamp form(s) without thinking about both their personal responsibilities and the Council's responsibilities under RIPA and the European Convention.

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

5. Those carrying out surveillance must inform the Authorising Officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation.

6. For further advice and assistance on RIPA, please contact the Monitoring Officer. Details are provided on the front of this document.

APPENDIX 1

List of Authorised Officer Posts

OVERALL RESPONSIBILITY: BRUCE LANG, ASSISTANT CHIEF EXECUTIVE/MONITORING OFFICER.

Authorising Officer's Name	**Designation**
Penny James	Chief Executive
Bruce Lang	Assistant Chief Executive & Monitoring Officer
James Barrah	Director of Housing & Communities
Tim Burton	Assistant Director of Planning & Environment
Paul Fitzgerald	Assistant Director of Resources
Chris Hall	Assistant Director of Operational Development
Simon Lewis	Assistant Director of Housing & Communities
Heather Tiso	Head of Revenues and Benefits Service

IMPORTANT NOTES

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

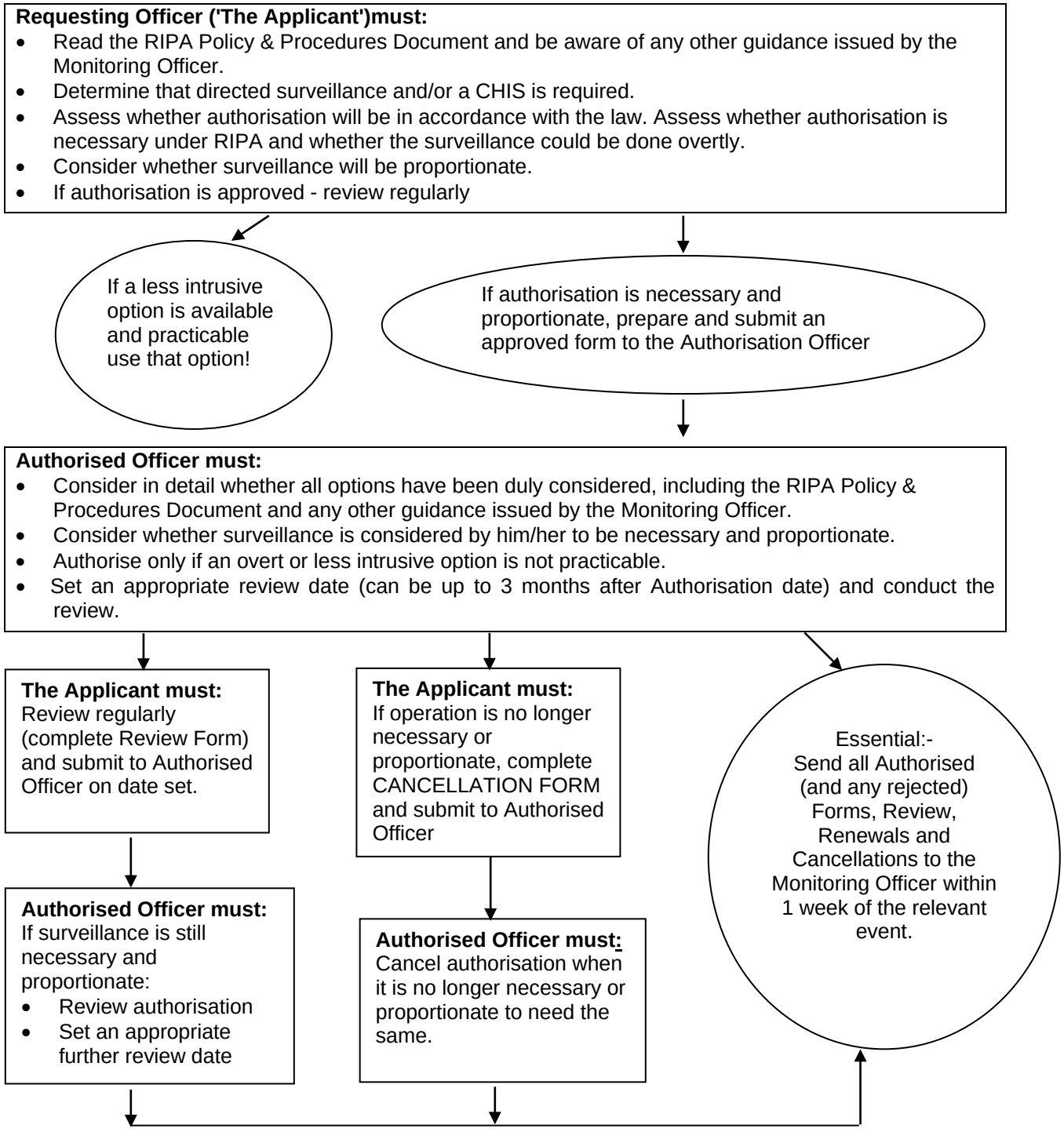
B. Only the Chief Executive and the Assistant Chief Executive & Monitoring Officer (Bruce Lang as of January 2014) are authorised to sign forms relating to Juvenile Sources and Vulnerable Individuals (see paragraph G of this document).

C. Particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material. In cases where through the use of surveillance it is likely that knowledge of confidential information will be acquired, the use of surveillance is subject to a higher level of authorisation; such authorisations will only be given by the CEO or by Bruce Lang.

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

APPENDIX 2

RIPA FLOW CHART



NB: If in doubt, ask the Monitoring Officer before any directed surveillance and/or CHIS is authorised, renewed, cancelled, or rejected.

PROCEDURE FOR MAGISTRATES COURT

Once authorisation has been granted, an application must be made to the Magistrates Court for a hearing.

The Investigating Officers must be authorized to appear in order to give evidence.

The Magistrates will need a copy of the original authorisation/notice and two copies of the judicial application/order.

The hearing will be held in private by one Justice of the Peace and the application must stand on its own.

If granted the Justice of the Peace will sign the order and a copy must be retained.

Advice and assistance can be sought from the Monitoring Officer or the Deputy Monitoring Officer and reference should be made to the Home Office guidance before making the application.

APPENDIX 3

TAUNTON DEANE BOROUGH COUNCIL

RIPA AUTHORISING OFFICER CERTIFICATE
No. [ ] / 200-

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

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

Certificate issued to:
[Full name of Officer] _____

Job Title: _____

Service: _____

Location: _____

Certificate date: _____

(signed) _____

Bruce Lang
Monitoring Officer
(Taunton Deane Borough Council)

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

APPENDIX 4

For the latest forms please go to this link

https://www.gov.uk/government/collections/ripa-forms--2

APPENDIX 5

EXAMPLES OF COVERT SURVEILLANCE

The following are examples of covert surveillance operations that may be conducted by Council staff, with indications as to whether RIPA authorisation may be needed.

If there are any special circumstances to an operation which, in general terms, matches one of the examples below, then the need for authorisation should be re-assessed by the Case Officer.

Example 1 -

Use of fixed CCTV cameras to record fly-tipping in the area around Recycling Centres in Council Car Parks.

Points to consider:

a) The cameras are in plain view and are therefore not covert, even if they are being used as part of a defined and pre-planned Operation.

b) By definition, these are well-used public areas and any expectation as to privacy would be minimal.

c) Collateral intrusion and the opportunity to obtain private information is unlikely.

Recommendation:

Unless there are additional and unusual features to the Operation, RIPA Authorisation would not be required.

Example 2 –

Use of temporary surveillance cameras to record fly-tipping in a public area such as a layby or a wooded area close to a road.

Points to consider:

a) Cameras and recording equipment would be deliberately concealed from view.

b) Although the area is accessible to the public, it is likely to be less frequented than, for example, a Council car park. There would therefore be a heightened expectation as to privacy.

c) The fact that fly-tipping is an illegal act does not reduce the perpetrators' rights to be protected.

d) Collateral intrusion and the opportunity to obtain private information, are more likely than in Example 1, above.

Recommendation:

On balance, RIPA authorisation for Directed Surveillance should be obtained.

This could be avoided by the publication in the local press beforehand of an article explaining that a given area would be placed under surveillance for a given period of time. However, this would largely negate the usefulness of the Operation.

Example 3 –

Use of noise recording equipment, in a complainant's property, with the tape recorder being operated by the complainant when noise events occur.

Points to consider:

a) The equipment is concealed from the occupants of the premises under surveillance (the Object). It is therefore a covert operation, unless the occupants of the premises under audio surveillance had been warned, in writing, that surveillance may be carried out within a given period of time.

b) The premises under surveillance are not public in any sense, and the expectation as to privacy would be very high.

c) Noise events coming from the premises under surveillance and affecting the complainant's premises might be regarded as no longer being private, as boundaries into other areas had been crossed by the time the noise was recorded.

However, there may well be instances (for example between poorly insulated flats or rooms within bedsits) where this consideration does not apply.

d) The possibility of collateral intrusion and the opportunity to obtain private information, are likely.

e) As the tape recording is operated by the complainant, it is possible (s)he is acting as a Covert Human Intelligence Source (CHIS).

Recommendation:

a) RIPA authorisation for Directed Surveillance should be sought by the Case Officer when the premises under surveillance are residential, unless:

i) The occupants of the premises under surveillance had been warned, in writing and in advance, that audio surveillance may be used, and/or

ii) There is such separation between the complainant's property and the property under surveillance that it could not be claimed that noise events passing from one to the other were of a private nature.

b) RIPA authorisation of the complainant as a CHIS should be considered if there was any form of relationship between the complainant and the occupants of the premises under surveillance. A relationship may include, for example, long-term neighbours who regularly speak to each other and who may, generally, be on good terms.

However, the need for Authorisation would only seem to apply if it is the clear intention to use this relationship, covertly, for the express purpose of obtaining confidential information. Clearly, in practically every case, this would not be the intention.

However, if the complainant may be able to influence the onset of a noise event from the object premises by using their relationship with the object, then the use of monitoring equipment, with or without RIPA Authorisation(s) would be inappropriate. To give an extreme example, the complainant may say to the object "…we are going out tonight, so you can play your music as loud as you like!".

Note: If the complainant, including any member of their household who may operate noise recording equipment, is judged to be acting as a CHIS, then it is immaterial whether or not the object has been informed of the likelihood of audio surveillance. Authorisation as a CHIS would still be required.

As part of the CHIS Authorisation, careful consideration must be given to the conditions to be imposed to prevent misuse of the relationship between complainant and object.

Example 4 –

Covert observation of a Night Club entrance to determine the number of patrons in the premises.

Points to consider:

a) No image or sound recording equipment is in use, so the opportunities for either collateral intrusion or of obtaining private information do not apply.

b) No individual person is under surveillance.

c) The queue that forms outside a Night Club is, by its nature, in a public place and is likely to be one that is well used.

Expectations as to privacy by any person outside the Club premises would therefore be very low.

Recommendation:

Unless there are additional and unusual features to the Operation, RIPA Authorisation would not be required.

Example 5 –

Asking a disabled person to book a taxi and complete a journey to determine whether the taxi driver was discriminatory and to report back to Licensing for possible enforcement action.

Points to consider:

a) The purpose of the journey would be to gather information.

b) It would be pre-planned.

c) It would be designed to be covert.

d) The nature and duration of the exercise make it likely that that a relationship, in legal terms, would be formed.

e) The expectation as to privacy would be high.

f) It is likely that, whether planned or not, confidential information would be obtained.

Recommendation:

a) It is considered that an Authorisation for Directed Surveillance would be required.

b) It is also considered that the disabled person would qualify as a CHIS, so that additional Authorisation would be required specifically for that aspect.

c) If it were intended to record conversation between the parties, this would constitute Intrusive Surveillance. Authorisation would not be possible and the surveillance itself would be unlawful.

END

March 2014

Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA)

Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance

Home Office

October 2012

Contents

1. INTRODUCTION: HOW THE LAW HAS CHANGED

1. On 1 November 2012 two significant changes will take effect governing 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[1] will mean that local authority authorisations and notices under RIPA for the use of particular covert techniques can only be given effect once an order approving the authorisation or notice has been granted by a Justice of the Peace (JP).
   - **Directed surveillance crime threshold**: Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order")[2] 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 particular types of criminal offences. These are 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.

2. This guidance is non-statutory but provides advice on how local authorities can best approach these changes in law and the new arrangements that need to be put in place to implement them effectively. It is supplementary to the legislation and to the statutory Codes of Practice. If a local authority has any doubts about the new regime they should consult their legal advisers. This guidance is intended for local authority investigation teams that may use covert techniques, including Trading Standards, Environmental Health and Benefit Fraud Officers. However, it will also be of use to authorising officers and designated persons and to those who oversee the use of investigatory techniques in local authorities including elected members.

3. Separate guidance is available for Magistrates' Courts in England and Wales and local authorities in Scotland.

1 Sections 37 and 38 of the Protection of Freedoms Act 2012 amend RIPA and will come into force on 1 November 2012.
2 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 [SI 2010/521] will be amended by the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 [SI 2012/1500] on 1 November 2012. See Section 5 for links.

2. LOCAL AUTHORITY USE OF RIPA

THE EXISTING REGULATORY FRAMEWORK

4. RIPA sets out a regulatory framework for the use of covert investigatory techniques by public authorities. RIPA does not provide any powers to carry out covert activities. If such activities are conducted by council officers, then RIPA regulates them in a manner that is compatible with the European Convention on Human Rights (ECHR), particularly Article 8, the right to respect for private and family life.

5. RIPA limits local authorities to using three covert techniques (details set out below) for the purpose of preventing or detecting crime or preventing disorder.

6. Use of these techniques has to be authorised internally by an authorising officer or a designated person. They can only be used where it is considered necessary (e.g. to investigate a suspected crime or disorder) and proportionate (e.g. balancing the seriousness of the intrusion into privacy against the seriousness of the offence and whether the information can be obtained by other means). The relevant Codes of Practice should be referred to for further information on the scope of powers, necessity and proportionality.[3]

THE TECHNIQUES WHICH LOCAL AUTHORITIES MAY USE

7. **Directed surveillance** is essentially covert surveillance in places other than residential premises or private vehicles[4].

8. Local authorities cannot conduct 'intrusive' surveillance (i.e. covert surveillance carried out in residential premises or private vehicles[5]) under the RIPA framework.

9. A **covert human intelligence source (CHIS) includes** undercover officers, public informants and people who make test purchases.

10. **Communications data** (CD) is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written). RIPA groups CD into three types:

    - 'traffic data' (which includes information about where the communications are made or received);
    - 'service use information' (such as the type of communication, time sent and its duration); and
    - 'subscriber information' (which includes billing information such as the name, address and bank details of the subscriber of telephone or internet services).

11. Under RIPA a local authority can only authorise the acquisition of the less intrusive types of CD: service use and subscriber information. Under **no circumstances** can local authorities be authorised to obtain traffic data under RIPA.

12. Local authorities are **not** permitted to intercept the content of any person's communications and it is an offence to do so without lawful authority.

3 See section 5 for links to the relevant legislation and codes of practice.
4 Further information on directed surveillance can be found in the Covert Surveillance and Property Interference Code of Practice.
5 Places where legal consultations are likely to take place will also be treated as intrusive surveillance.

RANK OF LOCAL AUTHORITY AUTHORISING OFFICERS/DESIGNATED PERSONS

13. Local authority authorising officers/designated persons will remain as designated by RIPA consolidating orders SI 2010 Nos.480 and 521:

- Director, Head of Service, Service Manager[6] or equivalent.

14. The authorisation of directed surveillance or use of a CHIS likely to obtain confidential information or the deployment of a juvenile or vulnerable person (by virtue of mental or other condition) as a CHIS requires authorisation by the most senior local authority officer – Head of Paid Service or, in his/her absence, the acting Head of Paid Service.

15. If there is any doubt regarding sufficiency of rank you should contact your Local Authority Monitoring Officer who will be able to advise you.

TIME LIMITS

16. The current time limits for an authorisation or notice will continue[7]. That is: 3 months for directed surveillance and 12 months for a CHIS (1 month if the CHIS is 18). Authorisations and notices for CD will be valid for a maximum of one month from the date the JP has approved the grant. This means that the conduct authorised should have been commenced or the notice served within that month.

17. A renewal must be authorised prior to the expiry of the original authorisation, but it runs from the expiry date and time of that original authorisation. Authorisations may be renewed more than once if still considered necessary and proportionate and approved by the JP.

18. Applications for renewals should not be made until shortly before the original authorisation period is due to expire but local authorities must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant local authority authorising officer and a JP to consider the application).

6 For CD RIPA applications, the Local Government Group and the Interception of Communications Commissioner's Office have advised that a Principal Trading Standards Officer is not considered to be of sufficient seniority to act as the Designated Person.

7 See section 43 RIPA.

3. DIRECTED SURVEILLANCE CRIME THRESHOLD

19. The crime threshold applies only to the authorisation of **directed surveillance** by local authorities under RIPA, not to the authorisation of local authority use of CHIS or their acquisition of CD. The threshold will come into effect on 1 November 2012.

20. The amendments to the 2010 Order have the following effect:

- Local authorities can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment **or** are related to the underage sale of alcohol and tobacco. The offences relating to the latter are in article 7A of the 2010 Order[8].
- Local authorities **cannot** authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment.
- Local authorities may therefore continue to authorise use of directed surveillance in more serious cases as long as the other tests are met – i.e. that it is necessary and proportionate and where prior approval from a JP has been granted. Examples of cases where the offence being investigated attracts a maximum custodial sentence of six months or more could include more serious criminal damage, dangerous waste dumping and serious or serial benefit fraud.
- Local authorities may also continue to authorise the use of directed surveillance for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco where the necessity and proportionality test is met and prior approval from a JP has been granted.
- A local authority **may not authorise** the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences or to investigate low-level offences which may include, for example, littering, dog control and fly-posting.

21. The change will affect authorisations or renewals which are granted on of after 1 November. It will not affect authorisations or renewals granted before that date.

IMPACT ON INVESTIGATIONS

22. At the start of an investigation, council officers will need to satisfy themselves that what they are investigating is a criminal offence. Directed surveillance is an invasive technique and at the point it is decided whether or not to authorise its use it must be clear that the threshold is met and that it is necessary and proportionate to use it.

23. During the course of an investigation the type and seriousness of offences may change. The option of authorising directed surveillance is dependent on the offence under investigation attracting a sentence of a maximum six months imprisonment or more or being related to the underage sale of alcohol and tobacco. Providing the offence under investigation is one which appears on the statute book with at least a maximum six months term of imprisonment or is related to the specific offences listed in the order concerning the underage sale of alcohol and tobacco an application can be made. However, if during the investigation it becomes clear that the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the threshold the use of directed surveillance should cease. If a directed surveillance authorisation is already in force it should be cancelled.

8 See section 5 for links to the relevant legislation

24. Directed surveillance will be authorised against a specific offence which meets the threshold, and the type and the timing of the deployment of the surveillance will always reflect this. There may be cases where it is possible, with the same evidence obtained by the same deployment, to substantiate a variety of different charges, some of which fall below the threshold, it will be for the courts to decide whether to admit – and what weight to attach to – the evidence obtained in the lesser charges.

25. Local authorities will no longer be able to use directed surveillance in some cases where it was previously authorised. But this does not mean that it will not be possible to investigate these areas with a view to stopping offending behaviour. The statutory RIPA Code of Practice on covert surveillance makes it clear that routine patrols, observation at trouble 'hotspots', immediate response to events and overt use of CCTV are all techniques which do not require RIPA authorisation.[9]

9 See paragraphs 2.21-2.29 of the Covert Surveillance and Property Interference Code of Practice.

4. JUDICIAL APPROVAL

WHAT THE CHANGES MEAN FOR LOCAL AUTHORITIES

26. From 1 November 2012, sections 37 and 38 of the Protection of Freedoms Act 2012 will commence. This will mean that a local authority who wishes to authorise the use of directed surveillance, acquisition of CD and use of a CHIS under RIPA will need to obtain an order approving the grant or renewal of an authorisation or notice from a JP (a District Judge or lay magistrate) before it can take effect. If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the grant or renewal for the use of the technique as described in the application.

27. The new judicial approval mechanism is in addition to the existing authorisation process under the relevant parts of RIPA as outlined in the Codes of Practice. The current local authority process of assessing necessity and proportionality, completing the RIPA authorisation/application form and seeking approval from an authorising officer/designated person will remain the same.

28. The inspection regimes of the independent RIPA oversight Commissioners will continue to apply to local authorities and the frequency and nature of their independent inspections of local authorities is not expected to change.

29. The judiciary is independent and it is not the role of the Commissioners to inspect the decision of the JP.[10] However the Commissioners will continue to have an important oversight role and will continue to inspect local authority use of RIPA. If the Commissioners identify an error in the authorisation process they will, as now, need to consider the best course of action. This may include asking the local authority to cancel the authorisation in question and, if appropriate, complete a new authorisation addressing their concerns which will need to be approved by the JP in the usual way. When an error is brought to the attention of a local authority they should cease the activity authorised.

30. The Commissioners will continue to advise local authorities of the procedures and training to adopt, on what is best practice and will continue to report to Parliament on relevant trends and findings.

PROCEDURE FOR APPLYING FOR JUDICIAL APPROVAL

Making the Application

31. The flowchart at Annex A outlines the procedure for applying for judicial approval. The application must be made by the public authority that has granted the authorisation[11]. Following approval by the authorising officer/designated person the first stage of the process is for the local authority to contact Her Majesty's Courts and Tribunals Service (HMCTS) administration team at the magistrates' court to arrange a hearing.

10 See section 62(2A) RIPA.

11 Some local authorities may enter into arrangements to form a regional group with other local authorities but the group cannot itself make the application. Only local authority officers in local authorities described in SIs 2010 Nos.480 and 521 are able to authorise under RIPA.

32. The local authority will provide the JP with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the JP and **should contain all information that is relied upon**. For communications data requests the RIPA authorisation or notice may seek to acquire consequential acquisition of specific subscriber information. The necessity and proportionality of acquiring consequential acquisition will be assessed by the JP as part of his consideration (see Annex C for considerations relating to CD authorisations and notices).

33. The original RIPA authorisation or notice 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). The court may wish to take a copy.

34. In addition, the local authority will provide the JP with a partially completed judicial application/order form (at Annex B).

35. Although the local authority is required to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well.

36. The order section of this form will be completed by the JP and will be the official record of the JP's decision. The local authority will need to obtain judicial approval for all initial RIPA authorisations/ applications **and renewals** and the local authority will need to retain a copy of the judicial application/ order form after it has been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

Arranging a Hearing

37. It will be important for each local authority to establish contact with HMCTS administration at the magistrates' court. HMCTS administration will be the first point of contact for the local authority when seeking a JP approval. The local authority will inform HMCTS administration as soon as possible to request a hearing.

38. On the rare occasions where out of hours access to a JP is required then it will be for the local authority to make local arrangements with the relevant HMCTS legal staff. In these cases the local authority will need to provide two partially completed judicial application/order forms so that one can be retained by the JP. The local authority should provide the court with a copy of the signed judicial application/order form the next working day.

39. In most emergency situations where the police have power to act, then they are able to authorise activity under RIPA without prior JP approval. No RIPA authority is required in immediate response to events or situations where it is not reasonably practicable to obtain it (for instance when criminal activity is observed during routine duties and officers conceal themselves to observe what is happening).

40. Where renewals are timetabled to fall outside of court hours, for example during a holiday period, it is the local authority's responsibility to ensure that the renewal is completed ahead of the deadline. Out of hours procedures are for emergencies and should not be used because a renewal has not been processed in time.

Attending a Hearing

41. The hearing is a 'legal proceeding' and therefore local authority officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the JP.

42. The hearing will be in private and heard by a single JP who will read and consider the RIPA authorisation or notice and the judicial application/order form. He/she may have questions to clarify points or require additional reassurance on particular matters.

43. Local authorities will want to consider who is best able to answer the JP's questions on the policy and practice of conducting covert operations and detail of the case itself. It is envisaged that the case investigator will be able to fulfil this role. The investigator will know the most about the investigation and will have determined that use of a covert technique is required in order to progress a particular case. The local authority may consider it appropriate for the SPoC (single point of contact) to attend for applications for CD RIPA authorisations or notices (see Annex C for considerations relating to CD authorisations and notices). This does not, however, remove or reduce in any way the duty of the authorising officer to determine whether the tests of necessity and proportionality have been met. Similarly, it does not remove or reduce the need for the forms and supporting papers that the authorising officer has considered and which are provided to the JP to make the case (see paragraphs 47-48).

44. The usual procedure would be for local authority Standing Orders to designate certain officers, including SPoCs, for the purpose of presenting RIPA cases to JPs under section 223 of the Local Government Act 1972. A pool of suitable officers could be designated at the start of the year when the Orders are examined and adjusted as appropriate throughout the year.

45. It is not envisaged that the skills of legally trained personnel will be required to make the case to the JP and this would be likely to, unnecessarily, increase the costs of local authority applications.

Decision

46. The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed or the notice was given or renewed, there were reasonable grounds for believing that the authorisation or notice 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.[12]

12 Further information on these restrictions can be found in the Regulation of Investigatory Powers Act 2000: Consolidating Orders and Codes of Practice, SI 2012 No.1500 (The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment), SI 2000 No.2793 (The Regulation of Investigatory Powers (Juveniles) Order 2000) and the OSC Procedures and guidance manual, available to public authorities on request from the Office of Surveillance Commissioners.

47. **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**. The JP may note on the form any additional information he or she has received during the course of the hearing but information fundamental to the case should not be submitted in this manner.

48. If more information is required to determine whether the authorisation or notice has met the tests then the JP will refuse the authorisation. If an application is refused the local authority should consider whether they can reapply, for example, if there was information to support the application which was available to the local authority, but not included in the papers provided at the hearing.

49. The JP will record his/her decision on the order section of the judicial application/order form. HMCTS administration will retain a copy of the local authority RIPA authorisation or notice and the judicial application/order form. This information will be retained securely. Magistrates' courts are not public authorities for the purposes of the Freedom of Information Act 2000.

50. The local authority will need to provide a copy of the order to the communications the SPoC (Single Point of Contact) for all CD requests. SPoCs must not acquire the CD requested, either via the CSP or automated systems until the JP has signed the order approving the grant.

Outcomes

51. Following their consideration of the case the JP will complete the order section of the judicial application/order form (see form at Annex B) recording their decision. The various outcomes are detailed below and reflected on the flowchart at Annex A.

52. The JP may decide to[13] –

- **Approve the Grant or renewal of an authorisation or notice**

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

  In relation to CD, the local authority will be responsible for providing a copy of the order to the SPoC.

- **Refuse to approve the grant or renewal of an authorisation or notice**

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

  Where an application has been refused the local authority may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without the local authority going through the internal authorisation process again. The local authority may then wish to reapply for judicial approval once those steps have been taken.

13 See sections 23B(3) and 32B(3) of the Regulation of Investigatory Powers Act 2000.

- **Refuse to approve the grant or renewal and quash the authorisation or notice**

  This applies where a magistrates' court refuses to approve the grant, giving or renewal of an authorisation or notice and decides to quash the original authorisation or notice.

  The court must not exercise its power to quash that authorisation or notice unless the applicant has had at least 2 business days from the date of the refusal in which to make representations.

Complaints/Judicial Review

53. There is no complaint route for a judicial decision unless it was made in bad faith. Any complaints should be addressed to the Magistrates' Advisory Committee.

54. A local authority may only appeal a JP decision on a point of law by juidical review. If such a concern arises, the local authority should consult their legal advisers.

55. The IPT will continue to investigate complaints by individuals about the use of RIPA techniques by public bodies, including local authorities. If, following a complaint to them, the IPT does find fault with a RIPA authorisation or notice it has the power to quash the JP's order which approved the grant or renewal of the authorisation or notice.

5. OTHER SOURCES OF REFERENCE

- The Regulation of Investigatory Powers Act 2000
  http://www.legislation.gov.uk/ukpga/2000/23/contents

- RIPA Explanatory Notes
  http://www.legislation.gov.uk/ukpga/2000/23/notes/contents

- RIPA statutory codes of practice

  – Covert Surveillance and Property Interference
  http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-covert
  – Covert Human Intelligence Sources
  http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-human-intel
  – Acquisition & Disclosure of Communications Data
  http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-acquisition

- SI 2000 No.2793 (The Regulation of Investigatory Powers (Juveniles) Order 2000
  http://www.legislation.gov.uk/uksi/2000/2793/made

- SI 2010 No.480 – Regulation of Investigatory Powers (Communications Data) Order 2010
  http://www.legislation.gov.uk/uksi/2010/480/contents/made

- SI 2010 N0.521 – Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010
  http://www.legislation.gov.uk/uksi/2010/9780111490365/contents

- SI 2010 No.461 (The Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010
  http://www.legislation.gov.uk/uksi/2010/461/contents/made

- SI 2012 No.1500 (The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012)
  http://www.legislation.gov.uk/uksi/1500/contents

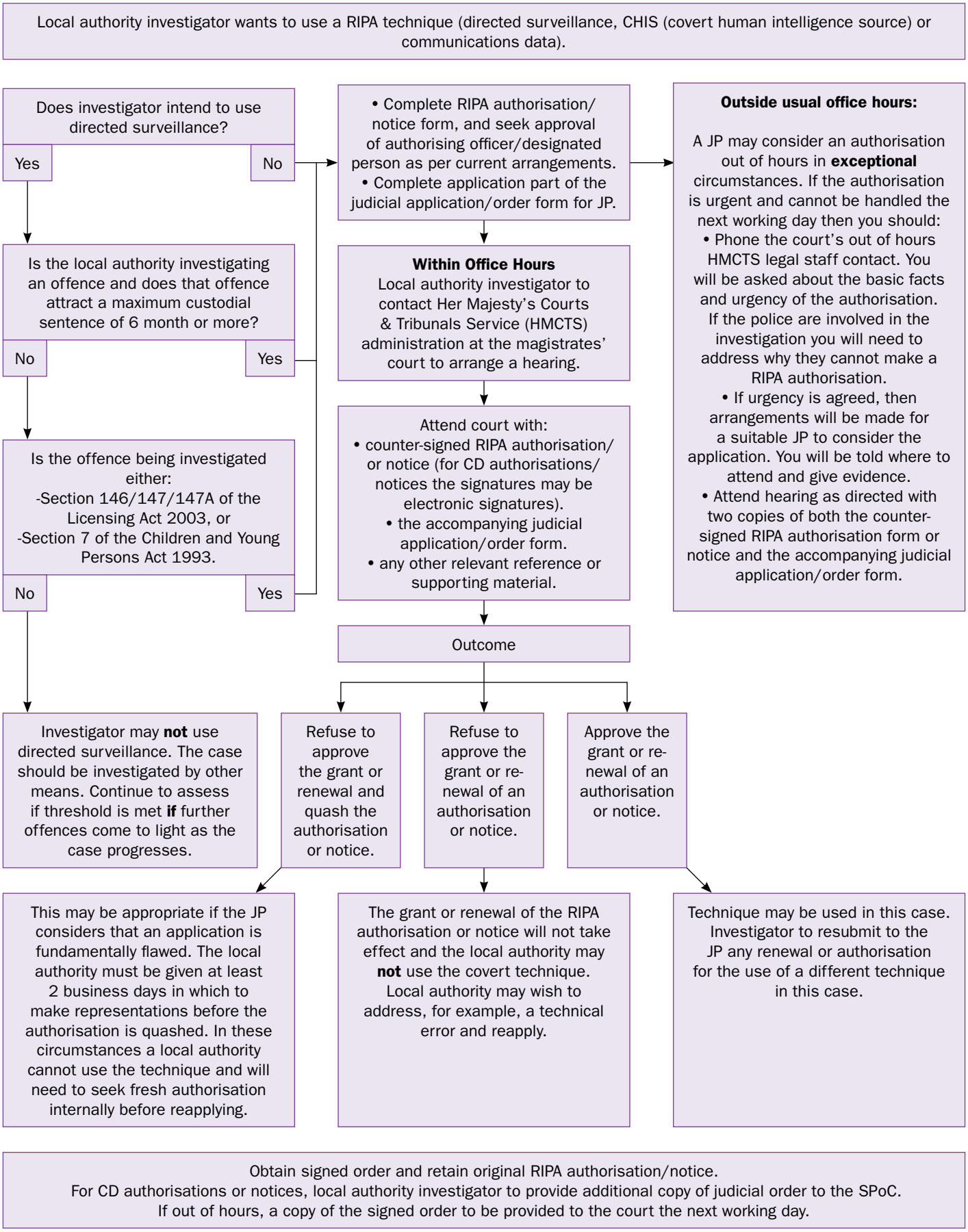
6. HOME OFFICE POINT OF CONTACT

Further information is available on request from:

RIPA Team
Home Office
5th Floor Peel Building
2 Marsham Street
London SW1P 4DF
Email: commsdata@homeoffice.x.gsi.gov.uk

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



ANNEX B

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:

ANNEX C

COMMUNICATIONS DATA (CD) RIPA AUTHORISATIONS OR NOTICES

Single Point of Contact (SPoC)

1. For CD requests, a Single Point of Contact (SPoC) undertakes the practical facilitation with the communications service provider (CSP) in order to obtain the CD requested. They will have received training specifically to facilitate lawful acquisition of CD and effective co-operation between the local authority and communications service providers.

2. Local authorities unable to call upon the services of an accredited SPoC should not undertake the acquisition of CD.

3. For CD requests the Home Office envisages that the local authority may also choose to authorise, under section 223 of the Local Government Act, their SPoC in order that they may appear in front of the JP. In cases where the type of CD or its retrieval is technically complex and the JP wants to satisfy him/herself that the CD sought meets the test, then the SPoC may be best placed to explain the technical aspects.

4. Following the hearing the SPoC may aquire the data. SPoCs must not acquire the data via a CSP or using automated systems until after the JP has signed the order approving the grant. The one month time limit will commence from the date of the JPs signature giving approval.

The National Anti Fraud Network (NAFN)

5. The National Anti-Fraud Network provides a SPoC service to local authorities, precluding each authority from the requirement to maintain their own trained staff and allowing NAFN to act as a source of expertise. Local authorities using the NAFN SPoC service will still be responsible for submitting any applications to the JP and a designated person in the local authority is still required to scrutinise and approve any applications. The accredited SPoCs at NAFN will examine the applications independently and provide advice to applicants and designated persons to ensure the local authority acts in an informed and lawful manner.

6. The local authority investigator (i.e. the applicant) will then submit the relevant judicial application/order form, the RIPA application (authorisation or notice) and any supporting material to the JP. As above, following a private hearing, the JP will complete the order section of the judicial application/order form, reflecting their decision. The local authority investigator will then upload a copy of this order to the NAFN SPOC.

7. The NAFN SPoC will then acquire the CD on behalf of the local authority in an efficient and effective manner.

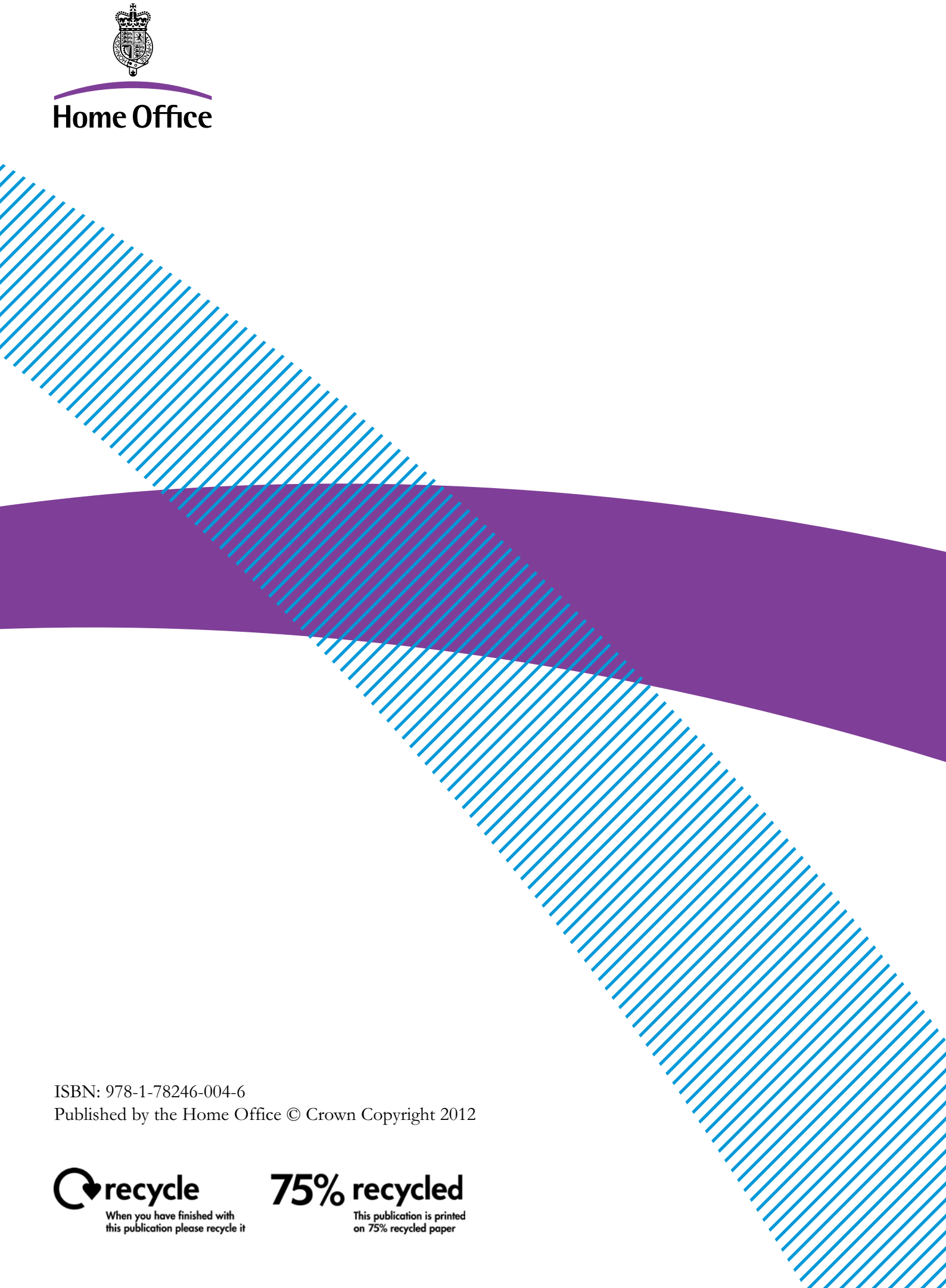
Consequential Acquisition

8. Section 3.31 of the Code of Practice for the Acquisition and Disclosure of CD outlines that a designated person may, at the time of granting an authorisation or notice for service usage data, also authorise the consequential acquisition of specific subscriber information. The designated person may only do so to the extent where it is necessary and proportionate. The consequential acquisition may only be for subscriber data, not traffic data, which local authorities may not acquire nor service usage data. Where a SPoC has been authorised to engage in conduct to obtain details of a person to whom a service has been provided and concludes that data is held by a CSP from which it cannot be acquired directly, the SPoC may provide the CSP with details of the authorisation granted by the designated person in order to seek disclosure of the required data[14].

9. In cases where an authorisation or notice seeks to acquire consequential acquisition of specific subscriber information the JP will assess this as part of his/her consideration. The local authority investigator should be prepared to explain to the JP the reasoning behind the request for consequential acquisition and be able to show how it meets the necessity and proportionality tests.

10. In cases where consequential acquisition is approved, but where a notice is required (which must specify the name of the CSP to whom it is given, and be signed by the designated person), a further grant of a notice will be required. This is a new legal instrument and therefore will require further approval to the designated person and the JP, despite authority for the human rights interference having already been given.

14 Acquisition and Disclosure of Communications Data Code of Practice, Paragraph 3.30.



ISBN: 978-1-78246-004-6