Taunton Deane Borough Council

Corporate Governance Committee – 8 December 2014

Regulation of Investigatory Powers Act – Update following Inspection

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

1. Executive Summary

In accordance with normal procedure the Office of Surveillance Commissioners undertook an inspection of the Council's management of covert activities in respect of the Regulation of Investigatory Powers Act (RIPA) 2000 on 29 July 2014.

This report outlines the outcome from the inspection and seeks endorsement of the action required to implement the recommendations emanating from the inspection.

2. Background

On 29 July 2014 Mr Neil Smart, an inspector acting on behalf of the Chief Surveillance Commissioner, visited the Council to undertake a review of the Council's management of covert activities under the powers conferred by RIPA.

A copy of the covering letter subsequently received from the Rt Hon Sir Christopher Rose, the Chief Surveillance Commissioner, is attached as Appendix A to the report.

It can be noted that the Commissioner recognised that the recommendations made following the previous inspection of the Council's activities three years ago had been largely discharged with good practice having been identified with the formal designation of authorising officers.

The reason why the recommendations of the previous inspection had been described as "largely" rather than completely discharged related to the need for ongoing training which was picked up as part of the formal recommendations arising from the Inspector's report.

The report was generally very positive and confirmed that the Inspector was satisfied that the Council takes its responsibilities under this legislation seriously and that there are appropriate systems and processes in place to use it effectively.

There were two recommendations from the report:

1. That RIPA training should continue to be formally delivered to Council staff who are likely to engage the legislation to ensure it can be applied to an appropriate standard; this should be considered as ongoing professional development; and

2. The policy/guidance document should be further amended in accordance with details set out in the inspection report to ensure it is fit for purpose and up-to-date with all the relevant legislation.

Arrangements have already therefore been made for specialist training to be held for relevant staff on 13 January 2015. In addition, further work has been done on the policy documents which is attached at Appendix B to this report with appropriate tracked changes clearly identified.

When the policy document was last considered by the Committee, the possibility of the Chairman and Vice-Chairman being kept advised of any potential surveillance request was raised and following discussion with the Inspector it is suggested that an appropriate local protocol be agreed in this regard.

3. Finance Comments

There are no financial implications in this report.

4. Legal Comments

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

5. Links to Corporate Aims

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

6. Environmental Implications

There are no environmental implications in this report.

7. Community Safety Implications

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 must be carried out if the report is 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.

The application of the policy must be undertaken in such a way to ensure that the human rights of individuals are taken into account.

9. Risk Management

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

There are no partnership implications within this report.

11. Recommendations

1. That the Committee note the outcome of the inspection by the Office of Surveillance Commissioners and support the ongoing provision of appriopriate training relating to the RIPA process.
2. That the Committee approve the updated Corporate Policies and Procedures on the Regulation of Investigatory Powers Act 2000 (RIPA) as set out in Appendix B to this report.
3. That a local protocol be followed whereby the Senior Responsible Officer for the RIPA process will ensure that the Chairman and Vice-Chairman of the Corporate Governance Committee be kept appropriately informed in regard to any potential and/or actual authorisations for the undertaking of authorised covert surveillance.

Contact: Bruce Lang,
Assistant Chief Executive and Monitoring Officer
01984 635200
bdlang@westsomerset.gov.uk

Appendix A – Letter from Office of Surveillance Commissioners

Appendix B – RIPA Policy and Procedure Guide

The Rt Hon. Sir Christopher Rose

APPENDIX A

Office of Surveillance Commissioners

Chief
Surveillance
Commissioner

14th August 2014

Official-Sensitive

Dear M/s James,

Covert Surveillance

On 29 August 2014, one of my Surveillance Inspectors, Mr Neil Smart, again visited your Council on my behalf to review your management of covert activities. I am grateful to you for the facilities afforded for the inspection.

I enclose a copy of Mr Smart's report which I endorse. I am pleased to see that the recommendations made following Mr Smart's last inspection in August 2011 have been largely discharged. Good practice is identified in your formal designation of authorising officers.

The recommendations are that RIPA training continue to be delivered, as ongoing professional development, to ensure its application to appropriate standards and that further amendments be made to your Policy / Guidance as indicated in para 7.5 of the report.

I shall be glad to learn that your Council accepts the recommendations and will see that they are implemented.

One of the main functions of review is to enable public authorities to improve their understanding and conduct of covert activities. I hope your Council finds this process constructive.

Please let this Office know if it can help at any time.

Yours sincerely,
Christopher Rose

M/s Penny James
Chief Executive
Taunton Deane Borough Council
Deane House
Belvedere Road
Taunton
Somerset
TA1 1HE

PO Box 29105 London SW1V 1ZU Tel 020 7035 8127 Fax 020 7035 3114
Web: www.surveillancecommissioners.gov.uk email:oscmailbox@osc.gsi.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) 1.7 dated September 2014
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 is the Senior Responsible Officer (SRO) who shall be responsible for ensuring the compliance of the Council with Part IItwo of RIPA 2000 and will maintain (and check) the ~~Corporate Register of~~Central Record of Authorisations which will include all RIPA authorisations, reviews, renewals, cancellations and rejections. However, it is the responsibility of the relevant Authoris~~ed~~ing Officer to ensure that the Monitoring Officer receives ~~a copy of the relevant forms within 1 week of authorisation, review, renewal, cancellation or rejection.~~the original form as soon as practical after completion for the completion of the central record, oversight and secure filing.

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. Authoris~~ed~~inged Officer~~s~~s (AO) 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 Chief Surveillance Commissioner or Surveillance Inspector 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.

Formatted: Justified

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 the designated SRO and 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.

2. The SRO shall be responsible for the following:-

   - The integrity of the process in place within ~~West Somerset District Council~~Taunton Deane Borough Council to authorise Directed Surveillance;
   - Compliance with Part II~~two~~ of RIPA 2000 and any associated Codes of Practice;
   - Acting as liaison with the Commissioners and inspectors and engaging with them as appropriate;
   - Overseeing the implementation of any post-inspection action and plans recommended or approved by a ~~Commissioners~~The Chief Surveillance Commissioner.

3. The SRO shall ensure that all AO's are provided with ~~copies~~a copy of current and updated Codes of Practice and OSC ~~Guidance and Procedure Notes~~Procedures and Guidance documents as they are released from time to time.

4. The SRO shall maintain a Central Record of Authorisations.

5. The Deputy Monitoring Officers will assist the SRO in undertaking the tasks as specified in 2.0 above.

Formatted: Justified, Indent: Left: 0 cm, First line: 0 cm

Formatted: Justified

C. Effective Date of Operation : 1 March 2009 and Authorised~~ed~~ing Officer (AO) 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~~AO are (after suitable training on RIPA and this document) duly certified to take action under this document.

3. ~~Authorised Officers~~AO 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~~AO 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~~AO 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~~AO is in any doubt, s/he should obtain prior guidance.

5. ~~Authorised Officers~~AO 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'.

Formatted: Justified

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~~AO. ~~Authorised Officers~~AO 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~~AO 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.

Formatted: Justified

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.

Formatted: Justified

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).

Formatted: Justified

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

6. Powers relating to directed surveillance were amended by the Protection of Freedoms Act 2012 and the RIPA (Directed Surveillance and CHIS) (Amendment) Order 2012

Formatted: Justified

G6. Directed Surveillance and Intrusive Surveillance

Formatted: Font: Bold

1. Directed Surveillance is surveillance which:-

Formatted: Justified, Indent: First line: 0 cm

Formatted: Justified

- 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).

Formatted: Justified

72 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.

83 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.

94 For the avoidance of doubt, only those Officers designated and certified to be ~~'Authorised Officers'~~AO 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~~AO 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~~AO for RIPA purposes cannot delegate his/her power of authorisation to another officer unless that officer is also an ~~Authorised Officer~~AO 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~~5 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~~6. Intrusive Surveillance is surveillance which ~~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.

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

8~~13~~. Council Officers must not authorise surveillance that contravenes Part III~~three~~ of the Police act 1997 relating to interference with property or wireless photography.

9~~14~~. If any "trespass" is being considered by Council staff during the course of surveillance, the matter should be referred to the Monitoring Officer as a matter of urgency.

Formatted: Font: 12 pt, Not Bold

Formatted: Justified

Formatted: Font: 12 pt

Formatted: Justified, Indent: Left: 0 cm, Hanging: 1.27 cm

Formatted: Font: 12 pt

Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm

10~~5~~. 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.

Property Interference (the Council cannot authorise this)	Attaching or placing an alarm on a vehicle without the consent of the owner.

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

Formatted: Indent: Left: 0.63 cm, No bullets or numbering

1. Introduction

Formatted: Indent: Left: 0 cm, Hanging: 0.75 cm, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 5.71 cm + Indent at: 6.35 cm

Formatted: Indent: Left: 0.75 cm

The Council do not propose to initiate involvement within this area of the Act. Nevertheless, the Council does have the power to do so and, in the unlikely event that such a source presents him/herself unexpectedly, the Council will manage the source in accordance with RIPA, the current Code of Practice and will comply with this Section G.

2. Definition of a CHIS

Formatted: Indent: Left: 0 cm, Hanging: 0.75 cm, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 5.71 cm + Indent at: 6.35 cm

Formatted: Indent: Left: 0.75 cm

Covert Human Intelligence Source (CHIS) is defined under Section 26(8)(a-c) of RIPA 2000, where information is obtained to assist in the investigation of a crime or to prevent a crime, by a CHIS who establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything, which is:

Formatted: List Paragraph, Left, Line spacing: single, No bullets or numbering, Widow/Orphan control, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Bulleted + Level: 1 + Aligned at: 1.39 cm + Indent at: 2.02 cm

- Covertly using a relationship to obtain information or provide access to any information to another person; or
- Covertly disclosing information obtained by the use of such a relationship, or as a consequence of the existence of a such a relationship
- Where the relationship is conducted in a manner that is unaware of its purpose.

The provisions of RIPA relating to CHIS do not apply:

Formatted: Indent: Left: 0.75 cm

Formatted: Bulleted + Level: 1 + Aligned at: 1.39 cm + Indent at: 2.02 cm

- Where members of the public volunteer information to the Council as part of their normal civic duties;
- Where the public contact telephone numbers set up by the Council to receive information;
- Where test purchase are carried out in the normal course of business;
- Where members of the public are asked to keep diaries of incidents in relation to planning enforcement or anti-social behavior;

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

Formatted: Indent: Left: 0.75 cm

3. Authorisation

Formatted: Indent: Left: 0 cm, Hanging: 0.75 cm, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 5.71 cm + Indent at: 6.35 cm

Formatted: Indent: Left: 0.75 cm

The Council is only likely to use a CHIS under very exceptional circumstances, and advice should be sought from the SRO before any authorisation is applied for or granted.

Before the AO grants authorisation to use CHIS, in consultation with the SRO, the SRO should consult with the District Commander with the Police Force Area, which

is the Avon and Somerset Constabulary, to ensure that no conflict arises within the area of where the CHIS is deployed but this will not include disclosure of the identity of the CHIS.

Authorisations should noty be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked with an assignment. An authorisation can cover, in broard terms, the nature of the CHIS's task and only if this changes significantly would a new authorisations be needed.

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

- **Conduct** of a CHIS = Establishing or maintaining a personal or other relationship with a person for the covert purpose (or incidental to the coee vert purpose of) obtaining and passing on information.
- **Use** of a CHIS = Inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of a source.

In the event of the Council deploying a CHIS they must take into account the safety and welfare of that CHIS. Before authorising the use or conduct of a CHIS the SRO shall ensure that a risk assessment is carried out and consideration given to ongoing security, welfare and management of any requirement to disclose information (including that tending to reveal the existence of the CHIS) and should also include the risk to the CHIS from any tasking and the likely outcome should the role of the CHIS become known.

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

- Be satisfied that the conduct and/or use if the CHIS is proportionate to the objective sought to be achieved;
- Consider the likely degree of intrusion for all those potentially affected;
- Consider any adverse impact on community confidence of the CHIS or the information obtained; and
- Ensure that records contain the required particulars set out in section 5 and that these are not available except on a 'need to know' basis.

If a juvenile or vulnerable individual is contemplated as a CHIS the Chief Executive or SRO must be the AO for the purposes of the authorisation.

4. Management of a CHIS

There are specific legal rules, which must be followed in relation to the management of sources. Officers to act as Designated Handlers and controllers (as set out in s.29(5) RIPA 2000) should be appointed. Officers who undertaken these roles must have undergone the specific training required by the legislation. Details are given in the relevant Home Office Code of Practice, and further advice can be obtained from the SRO.

Formatted: Bulleted + Level: 1 + Aligned at: 1.39 cm + Indent at: 2.02 cm

Formatted: Indent: Left: 2.02 cm

Formatted: Bulleted + Level: 1 + Aligned at: 1.39 cm + Indent at: 2.02 cm

Formatted: Indent: Left: 0.75 cm

Formatted: Bulleted + Level: 1 + Aligned at: 1.39 cm + Indent at: 2.02 cm

Formatted: Indent: Left: 0.75 cm

Formatted: Font: Bold

Formatted: Indent: Left: 0 cm, Hanging: 0.75 cm, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 5.71 cm + Indent at: 6.35 cm

Formatted: Indent: Left: 0.75 cm

A controller will have responsibility for the management and supervision of the Designated Handler and general oversight of the use of the CHIS.
Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 years of age). On no account can a child under 16 years of age be authorised to give information against his or her parents. Similar safeguards also apply to the use of vulnerable individuals as sources. (A vulnerable individual is a person who is a person or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.) Further advice must be sought from the SRO before using juveniles or vulnerable individual's source, to ensure that all necessary legal requirements are compiled with.

A CHIS will have his/her identify protected under the relevant legal procedures.

5. Specific CHIS Records

In addition to records kept in accordance with section 11 below the following matters will be recorded and maintained in relation to every CHIS.

- The identity of the CHIS and the identity, where known, used by the CHIS;
- The date when and the circumstances in which the CHIS was recruited;
- Any significant information connected with the security and welfare of the CHIS;
- Confirmation that annay person granting or renewing an authorisation for the conduct or use of a CHIS that the information referred to in **9.13.3** has been considered and that anay identified risks have, where appropriate, been explained to and understood by the CHIS.
- The identifies of the persons who in relation to the CHIS are acting as a Designated Handler or controller and the periods during which those persons have so acted;
- All contact or communications between the CHIS and the person acting on behalf of the Investigating Officer, including all tasks given to and demands made of the CHIS; information received by the conduct or use of the CHIS and the dissemination of any information so obtained;
- In situations where the relevant investigating authority is different to the Council, the details of that investigation authority and the means by which the CHIS is referred to within each relevant investigating authority.

6. Corporate Manager Records

The following information should be maintained by the relevant member of the Joint Management Team for the Service Team where the authorisation application originated from in relation to the source:

Formatted: Font: Bold

Formatted: Indent: Left: 0 cm, Hanging: 0.75 cm, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 5.71 cm + Indent at: 6.35 cm

Formatted: Indent: Left: 0.75 cm

Formatted: Font: Not Bold

Formatted: Bulleted + Level: 1 + Aligned at: 1.39 cm + Indent at: 2.02 cm

Formatted: Font: Not Bold

Formatted: Indent: Left: 2.02 cm

Formatted: Bulleted + Level: 1 + Aligned at: 1.39 cm + Indent at: 2.02 cm

Formatted: Bulleted + Level: 1 + Aligned at: 1.39 cm + Indent at: 2.02 cm

Formatted: Bulleted + Level: 1 + Aligned at: 1.39 cm + Indent at: 2.02 cm

Formatted: Bulleted + Level: 1 + Aligned at: 1.39 cm + Indent at: 2.02 cm

Formatted: Bulleted + Level: 1 + Aligned at: 1.39 cm + Indent at: 2.02 cm

Formatted: Indent: Left: 2.02 cm

Formatted: Bulleted + Level: 1 + Aligned at: 1.39 cm + Indent at: 2.02 cm

Formatted: Font: Bold

Formatted: Indent: Left: 0 cm, Hanging: 0.75 cm, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 5.71 cm + Indent at: 6.35 cm

- Any risk assessment in relation to the source;
- The Circumstances in which tasks were given to the source;
- The value of the source of the investigating authority;

Formatted: Indent: Left: 1.25 cm, Hanging: 0.5 cm, Bulleted + Level: 1 + Aligned at: 1.39 cm + Indent at: 2.02 cm

A 'Surveillance Log Book' should be completed by the Investigating Officer(s) to record all operational details of authorised covert surveillance or the use of a CHIS. Once completed, the Log Book will be passed to the relevant member of the Joint Management Team or to their designated RIPA coordinatedor for safe keeping in a secure secure place. Each service will also maintain a record of the issue and movement ***** of all Surveillance Log Books

~~H~~I. 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.

Authoris~~inged~~ Officers (AO's)

8. Forms can only be ~~signed~~ authorised by ~~Authorised Officers~~AO 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!

Formatted: Justified

Formatted: Justified

Training Records

10. Proper training will be given or approved by the Monitoring Officer before ~~Authorised Officers~~AO 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~~AO 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. Powers relating to directed surveillance were amended by the Protection of Freedoms Act 2012 to limit usage of the prevention of disorder element to the purpose of preventing or detecting a criminal offence where the potential punishment for a person over 21 years on a first offence is a term of at least six months imprisonment, or involving potential offences involving underage sales of alcohol or tobacco. This in relation to the prevention of disorder is unlikely within a Council to be achieved.

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

Formatted: Justified

Formatted: Justified

Formatted: Indent: Left: 0 cm, Hanging: 1.25 cm, Tab stops: Not at 0. cm

Formatted: Indent: Left: 0 cm, Hanging: 1.25 cm

Formatted: Justified

Formatted: Justified, Indent: Left: cm, Hanging: 0.75 cm

Formatted: Justified, Indent: Hanging: 0. 1 cm

(iii) Proportionate to what it seeks to achieve.

Formatted: Justified, Indent: Left: cm, Hanging: 0.75 cm

Formatted: Justified

(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. It is important to balance the seriousness of the intrusion into the privacy of the subject of the operation (/or any other person who may be affected) against the need for the activity in iInvestigative or operational terms.

(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~~Central Record of Authorisations 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~~AO must also:

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

Formatted: Justified

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

17. If an application is granted, the ~~Authorising Officer~~ AO 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~~AO 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 coordinator for safe keeping in a secure place. Each group will also maintain a record of the issue and movement of all Surveillance Log Books.

Formatted: Justified

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.~~The Protection of Freedoms Act 2012 Schedule 9 (9)(2) removed the possibility of oral authorisation. Now authorisations must be in writing and have judicial approval before they are effective.

Formatted: Justified

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.~~In cases where emergency approval is required the AO must be visited by the applicant officer with two completed RIPA application forms. The AO will then assess proportionality and necessity and the legality of the application. If approved, the applicant officer must contact the out of hours HM Courts and Tribunal Service (HMCTS) representative to seek approval from a Magistrate.

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, expiring at 23.59 hours the preceeding day for operational purposes 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.

Formatted: Justified

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.~~

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

276 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.~~

Reviewing Authorisations

287. Regular review of the all authorisations should be undertaken to assess the need for the surveillance or property interference activity to continue. The result of a review should be retained for at least three years. Particular attention is drawn to the need to review authorisations frequently where the surveillance or property interference involves a high level of intrusion into private life or significant collateral intrusion, or confidential information is likely to be obtained.

298. In each case the frequency of reviews should be considered at the outset by the AO or, for those subject to authorisation by the Secretary of State, the member or officer who made the application within public authority concerned. This should be as frequently as is considered necessary and practicable.

3029. ~~In some cases it may be appropriate for an AO to delegate the responsibility for conducting any reviews to a subordinate officer. The AO must is, however usually best placed to~~ assess whether the facts upon which he based the original decision to grant an authorisation have changed sufficiently to cause the authorisation to be revoked. Support staff can do the necessary research and prepare the review process but the actual review is the responsibility of the original AO and should, as matter of good practice, be conducted by them or, failing that, by an officer who would be entitled to grant a bean authorisation in the same terms.

310. Any proposed or unforeseen changes to the nature or extent of the surveillance operation that may result in the further or greater intrusion into the private life of any person should also be brought to the attention of the AO by means of a review. The AO should consider whether the proposed changes are

Formatted: Normal

Formatted: Font: (Default) Arial, English (United States)

Formatted: Font: (Default) Arial, English (United States)

Formatted: Normal, Justified, Indent: Left: 0 cm, Hanging: 1.27 cm

proportionate (bearing in mind any extra intended intrusion privacy or collateral intrusion), before approving or rejecting them.

Any such changes must be highlighted at the next renewal if the authorisation is to be renewed.

~~**Example:** A directed surveillance authorisation is obtained by the police to authorise surveillance of "X and his associates" for the purposes of investigating their suspected involvement in a crime. X is seen meeting with A in a café and it is assessed that subsequent surveillance of A will assist the investigation. Surveillance of A may continue (he is an associate of X) but the directed surveillance authorisation should be amended at a review to include "X and his associates, including A".~~

Cancellations

331. During a review, the AO who granted or last renewed the authorisation may amend specific aspects of the authorisation, for example, to cease surveillance against one of a number of named subjects or to discontinue the use of a particular tactic. They must cancel the authorisation if satisfied that the directed surveillance as a whole no longer meets the criteria upon which it was authorised.

Where the original AO is no longer available, this duty will fall on the person who has taken over the role of AO or the person who is acting as AO (see Regulation of Investigatory Powers Act (Directed Surveillance and Covert Human Intelligence Sources) Order 2010).

342. As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date the authorisation was cancelled should be centrally recorded and documentation of any instruction to cease surveillance should be retained. The AO must make a direction in respect of the surveillance product.

There is no requirement for any further details to be recorded when cancelling a directed surveillance authorisation. However, effective practice suggests that a record should be retained detailing the product obtained from the surveillance and whether or not objectives were achieved.

353. AO should not normally be responsible for authorising operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently or for security reasons. Where an AO authorises such an investigation or operation the centrally retrievable record of authorisations should highlight this and the attention of a Commissioner or Inspector should be invited to it during his next inspection.

364. It is unlikely to be regarded as "not reasonably" (within the meaning of sections of the Acts specified above) for an AO to consider an application, unless he/she is too ill to give attention, on annual leave, is absent from his office and his/her home, or is for some reason not able within a reasonable time to obtain access to a secure telephone or fax machine.

Formatted: Font: (Default) Arial, 12 pt, Not old, English (United States)

Formatted: Font: 14 pt

Formatted: Justified

Formatted: Justified

Pressure of work is not to be regarded as rendering it impracticable for an AO to consider an application.

375. Where a designated deputy gives an authorisation the reason for the absence of the AO should be stated.

386. The absence of a collaboration agreement does not preclude the application seeking authorisation of actions by members of another organisation.

37. **Process for obtaining Judicial Approval**

Under S37 and S38 Protection of Freedoms Act 2012 a Local Authority who wishes to authorise the use of directed surveillance, and use of a CHIS under RIPA will need to obtain an Order approving grant/renewal of an authorisation from the Magistrates' Court before it can take effect.

If the JP (District Judge or lay magistrate) 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.

The process to be followed to obtain Judicial approval is set out in Appendix 2.

38. Authorised Activity

Formatted: Font: Not old

Before surveillance commences, officers involved in the surveillance must read the authorisation and certify in writing that they have done so.

~~I~~J. Working With / Through Other Agencies

Formatted: Justified

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~~ certified by the officers as having been read 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):

Formatted: Justified

(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~~) Central Record of Authorisations or relevant extracts from the agencies RIPA form which are sufficient for the purposes of protecting the Council and use of its resources. The Council must only allow its equipment to be used in accordance with the authorisation.;

(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.

K. Covert use of the Internet and Social Networking Sites (SNS)

Formatted: Justified

Even if digital investigation can be routine or easy to conduct, this does not reduce the need for authorisation.

The AO must consider each service provider and services provided on an individual basis.

If Access Controls are applied to data by the author, there is a reasonable expectation of privacy. Where privacy settings are available but not applied, data may be considered open source and authorisation is not normally required.

If there is no warrant authorising interception, in accordance with S48(4) 2000 Act, if it is necessary and proportionate to breach covertly access controls, an authorisation for directed surveillance will be needed as a minimum.

An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of the public or by a person acting on its behalf.

If an officer wishes to set up a false identity for a covert purpose, authorisation must be obtained.

Use of photographs of third parties to support the false identity without the third party's permission is not permitted.

An officer should not adopt the identity of a person known or likely to be known by the subject of interest or users of the site, without authorisation and also the consent in writing of the person whose identity is to be used and details of what is agreed can be done and not done. The Officer must also consider the protection of that party.

~~J~~L. 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~~ Original documents should go to the SRO/RIPA co-ordinator for central filing within the Central Record of Authorisations. Practitioners should work from copy documents at all times.

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~~AO;
   - 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~~AO;
   - 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~~Central Record of Authorisation maintained by the Monitoring Officer

4. ~~Authorised Officer~~AOs 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

Formatted: Justified

Formatted: Justified

Formatted: Justified

audit/review the Council's policies and procedures, and individual authorisations.

~~K~~M. 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.

Formatted: Justified

Formatted: Justified, Indent: Hanging: 0.55 cm

Formatted: Justified, Indent: Left: 1.51 cm, First line: 0.74 cm

Formatted: Justified, Indent: Hanging: 0.55 cm

Formatted: Justified, Indent: Left: 1.51 cm, First line: 0.7 cm

Formatted: Justified

Formatted: Justified, Indent: Hanging: 0.55 cm

Formatted: Justified, Indent: Left: 1.4 cm, First line: 0. cm

Formatted: Justified

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

Formatted: Justified, Indent: Left: 1.02 cm

~~N~~L. Amendments to this guidance document

Formatted: Justified

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~~O. Complaints Handling

1. Taunton Deane Borough Council's Surveillance Complaints Procedure

Formatted: Justified

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.

PN. 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.~~ Q.Concluding Remarks of the Monitoring Officer

Formatted: No bullets or numbering

Formatted: Justified

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~~AO will be suitably trained and they must exercise their minds every time they are asked to ~~sign a form~~authorise a course of action. 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~~AO 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 Authorising 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 formspermitted to authorise any RIPA application 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.

Formatted: Justified

B. Only the Chief Executive and the Assistant Chief Executive & Monitoring Officer (Bruce Lang as of January 2014) are authorised to sign formsdetermine RIPA applications relating to Juvenile Sources and Vulnerable Individuals (see paragraph GHof 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

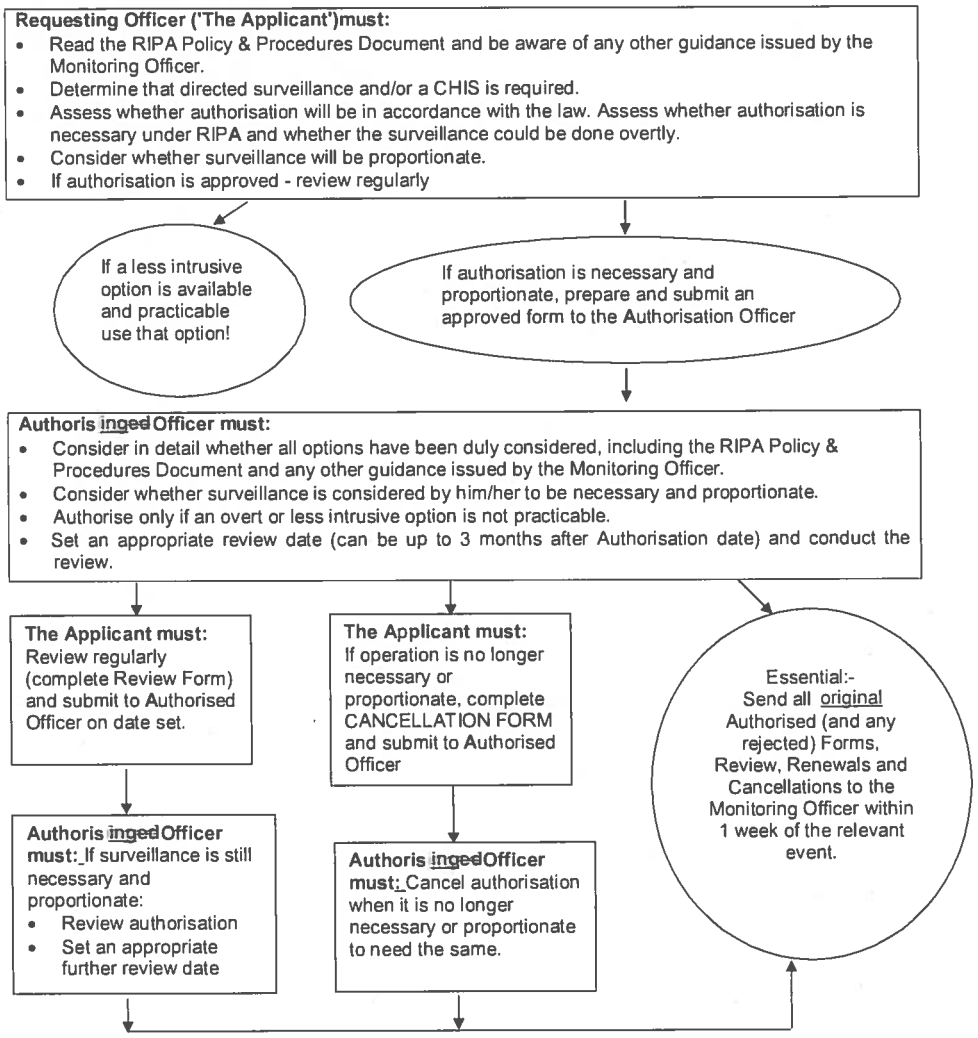
only be given by the CEO or by Bruce Lang.

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

Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm

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 contact HCTIMS HMCTS administration as soon as possible to request a hearing.

The Investigating Officers must be authorised to appear in order to give evidence, or provide information required by the JP.

The Magistrates will need a copy of the original authorisation/ notice and supporting documents and two copies of the partially completed judicial application/order. The original authorisation should be shown to the JP but retained by the Investigating Officer(s) so that it is available for inspection by the Commissioner's Officers and in the event of a legal challenge or investigations by the Investigatory Powers Tribunal.

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 complete and sign the order and this ~~a copy~~ must be retained as the official record of the JP's decision.

If out of hours access to a JP is required, the Investigating Officer(s) must make local arrangements with the relevant HMCTS legal staff.

Two partially completed judicial application forms will be needed, one will be retained by the JP. The Investigating Officer(s) will provide the Court with a copy of the signed judicial application form the next working day.

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

Formatted: Justified, Indent: Left: 0.25 cm, Line spacing: At least 12 pt, Tab stops: 0.22 cm, Left

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